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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction (Lecture 1)</td>
<td>4</td>
</tr>
<tr>
<td>0.1. Administrivia</td>
<td>4</td>
</tr>
<tr>
<td>0.2. Course plan (subject to revision)</td>
<td>4</td>
</tr>
<tr>
<td>0.3. Review of $\mathbb{Z}$</td>
<td>4</td>
</tr>
<tr>
<td>0.4. Motivating examples</td>
<td>5</td>
</tr>
<tr>
<td>0.5. Fermat’s Last Theorem (Lecture 2)</td>
<td>6</td>
</tr>
<tr>
<td>Chapter 1. Number Fields and Algebraic Integers</td>
<td>8</td>
</tr>
<tr>
<td>1.1. Algebraic Integers (Lecture 3)</td>
<td>8</td>
</tr>
<tr>
<td>1.2. The absolute discriminant (skipped)</td>
<td>9</td>
</tr>
<tr>
<td>1.3. Unique factorization (Lectures 4,5)</td>
<td>10</td>
</tr>
<tr>
<td>1.4. Primes in extensions (Lectures 6,7,8)</td>
<td>12</td>
</tr>
<tr>
<td>Chapter 2. Local fields</td>
<td>15</td>
</tr>
<tr>
<td>2.1. Valuations and absolute values</td>
<td>15</td>
</tr>
<tr>
<td>2.2. Complete fields (Lectures 11-13)</td>
<td>18</td>
</tr>
<tr>
<td>2.3. Ramification</td>
<td>22</td>
</tr>
<tr>
<td>2.4. Places of number fields</td>
<td>25</td>
</tr>
<tr>
<td>Chapter 3. Different, Discriminant and ramification</td>
<td>29</td>
</tr>
<tr>
<td>3.1. The trace form and duality (1 hour, 8/3/2013)</td>
<td>29</td>
</tr>
<tr>
<td>3.2. The different (2 hours, 8/3 + 11/3)</td>
<td>30</td>
</tr>
<tr>
<td>3.3. The Discriminant (15/3/2013)</td>
<td>33</td>
</tr>
<tr>
<td>3.4. Example: Cyclotomic fields</td>
<td>35</td>
</tr>
<tr>
<td>3.5. Everywhere unramified extensions</td>
<td>36</td>
</tr>
<tr>
<td>Chapter 4. Geometry of Numbers</td>
<td>37</td>
</tr>
<tr>
<td>4.1. Lattices in $\mathbb{R}^n$</td>
<td>37</td>
</tr>
<tr>
<td>4.2. Discriminant bounds</td>
<td>38</td>
</tr>
<tr>
<td>4.3. Finiteness of the class group</td>
<td>39</td>
</tr>
<tr>
<td>4.4. The Unit Theorem</td>
<td>39</td>
</tr>
<tr>
<td>Chapter 5. Analytic Theory: L-functions</td>
<td>42</td>
</tr>
<tr>
<td>5.1. Dirichlet Series</td>
<td>42</td>
</tr>
<tr>
<td>5.2. The Riemann zetafunction</td>
<td>46</td>
</tr>
<tr>
<td>5.3. The Dedekind Zetafunction</td>
<td>48</td>
</tr>
<tr>
<td>Bibliography</td>
<td>48</td>
</tr>
<tr>
<td>Bibliography</td>
<td>49</td>
</tr>
</tbody>
</table>
Introduction (Lecture 1)

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: $\pm 1$
  - 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 $z-x, z+x$ 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 $\mathbb{Z}[x,y,z,w]$:

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

so it is natural to understand prime $n$ first.

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

**Corollary 5.** If $n = \prod p^{e_p}$ is an integer such that $e_p$ is even whenever $p \equiv 3 \mod 4$ then $n = x^2 + y^2$ has solutions.

**Theorem 6.** The converse holds.

**Proof.** Consider the ring $O = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$. Let $z \mapsto \bar{z}$ be the non-trivial Galois automorphism of $\mathbb{Q}(i)$. Then $N z = z \bar{z}$ is a multiplicative map $O \to O$ (product of two multiplicative maps), which is the formula [0.4.1]. Now let $\pi \in O$ be a prime divisor of some rational prime $p$. Then $N\pi|Np = p^2$ so $N\pi \in \{1, p, p^2\}$. But $N\pi \neq 1$ (not a unit). If $N\pi = p^2$ then $N\left(\frac{\bar{\pi}}{\pi}\right) = 1$ 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. $p \equiv 3 \mod 4$. 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 $\mathbb{F}_p[x] \to O/pO$ given by mapping $\mathbb{F}_p$ to $\mathbb{Z}/p\mathbb{Z}$ and $x$ to $i + pO$ factors through the field $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(x^2 + 1)$, of the same cardinality, so $O/pO$ is a field. Thus $(p)$ is a prime ideal so $p$ is prime.

2. If $p \equiv 1 \mod 4$ then it is not prime in $O$, hence there is $\pi$ 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 $x^2 \equiv -1 \mod p$. If $a$ is the solution then $p|(1+ai)(1-ai)$ but it divides neither. It follows that $p$ isn’t prime in $O$.
   b. The ring $O/pO$ contains four solutions to $x^2 = -1$ (both $\pm a + pO$ and $\pm i + pO$) so it isn’t a field.

3. If $p = 2$ then $p = (1+i)(1-i) = -i(1+i)^2$ since $(1+i) \sim (1-i)$.
   a. Note that if $p \equiv 1 \mod 4$ 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 $x - iy = i^d(x + iy)$ 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 \( \pi \) is a prime then \( \pi \) 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

\[
z^p = (x - y) \prod_{j=1}^{p-1} (x - \zeta^j y)
\]

where \( \zeta \) is a primitive \( p \)th 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 \( \rho \) 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 \( j \neq k(p) \), \( \zeta^j - \zeta^k = \zeta^j (1 - \zeta^{k-j}) = \zeta^j \frac{1 - \zeta^{-j}}{1 - \zeta^{-1}} (1 - \zeta) \) so \( \rho \) 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 \( \Phi(x) = x^{p-1} - 1 \) is the \( p \)th 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 \( \tau \) denotes complex conjugation we then have

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

Now, for any \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \) we have \( |\sigma \tau(\varepsilon) / \varepsilon| = |\tau(\sigma(\varepsilon)) / \sigma(\varepsilon)| = 1 \) since the Galois group is commutative. It follows that \( \tau(\varepsilon) / \varepsilon \) is a root of unity, hence of the form \( \zeta^{-r} \) 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

\[
x - \zeta^{-1} y = \zeta^{-r} \epsilon \tau(t)^p \equiv \zeta^{-r}(x - \zeta y)(p).
\]

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 \( 1 \leq r \leq p - 1 \),

\[
\zeta^{r-1}(\zeta x - y) \equiv x - \zeta y(p),
\]
which we can rewrite as
\[(1 - \pi)r^{-1} (x - y - \pi x) - (x - y + \pi y) \equiv 0 \pmod{p}.
\]
Expanding in a power series in $\pi$, if $2 \leq r \leq p - 2$ 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 $\pi$ divides each of the $x - \zeta_j y$ (also $x - y$), and the $x - \zeta_j y$ 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 $\epsilon_j \in \mathcal{O}^\times$ and $t_j \in \mathcal{O}$,
\[
x - \zeta_j y = \epsilon_j \pi t_j^p
\]
furthermore, the $t_j$ are relatively prime. Now the $x - \zeta_j y$ where $j \neq 0$ are all divisible by $\pi$ 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 \( \mathbb{Z}[x] \). \( \square \)

EXAMPLE 10. \( K = \mathbb{Q} \). The minimal polynomial of \( \alpha \) 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 \( b \in \mathbb{Q} \), \( b \in \mathbb{Z} \) 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 \( 0, 1 \mod 4 \) which is impossible since \( (2a)^2 \equiv 1 \mod 4 \). 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 \( \mathbb{Z}[\beta] = \mathbb{Z} \oplus \mathbb{Z} \beta \oplus \cdots \oplus \mathbb{Z} \beta^{n-1} \) where \( \beta \) has degree \( n \). The last claim implies the first by Cayley–Hamilton.

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 \( \beta \) has degree \( n \). The last claim implies the first by Cayley–Hamilton. \( \square \)

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 \( \alpha, \beta \) hence by \( \mathbb{Z}[\alpha, \beta] \) which contains the requisite elements. \( \square \)

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

1. Every Galois conjugate of \( \alpha \) is integral over \( \mathbb{Q} \);
2. The minimal polynomial of \( \alpha \) over \( \mathbb{Q} \) is monic and belongs to \( \mathbb{Z}[x] \);
3. \( \text{Tr}_K^\mathbb{Q}(\alpha), N_K^\mathbb{Q}(\alpha) \in \mathbb{Z} \) and,
4. \( \alpha \in \mathcal{O}_K^\times \) iff \( N_K^\mathbb{Q} \alpha \in \mathbb{Z}^\times = \{\pm 1\} \).
PROOF. (1) Let $L$ be a normal extension containing $K$. Then $O_L \cap K = O_K$ by definition, and every conjugate of $\alpha$ satisfies the same polynomials that $\alpha$ does.

(2) The minimal polynomial of $\alpha$ is $\prod_{\mu \in \text{Hom}_Q(Q(\alpha), \overline{Q})} (x - \mu \alpha) = \prod_{\sigma \in \text{Hom}(Q(\alpha), L)} (x - \sigma \alpha) \in O_L [x] \cap Q[x] = \mathbb{Z}[x]$ since $O_L$ is a ring.

(3) now follows by taking specific coefficients.

(4) Exercise.

\begin{lemma}
\textbf{Lemma 16.} Let $\alpha \in K$. Then there is $m \in \mathbb{Z}$ so that $m \alpha \in O_K$.
\end{lemma}

\begin{proof}
Let $f = \sum_{i=0}^{d} a_i x^i \in Q[x]$ be the (monic) minimal polynomial of $\alpha$. 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 $0 \leq i < d$.
\end{proof}

\begin{corollary}
There exists a basis of $K$ consisting of elements of $O_K$.
\end{corollary}

\begin{lemma}
The quadratic form $(x, y) \mapsto \text{Tr}(xy)$ is non-degenerate.
\end{lemma}

\begin{proof}
$\text{Tr}(x \cdot x^{-1}) = n$.
\end{proof}

\begin{proposition}
There exist a $Q$-basis $\{\omega_i^*\}_{i=1}^{n} \subset K$ so that $O_K \subset \oplus_i Q \omega_i^*$.
\end{proposition}

\begin{proof}
Take $\{\omega_i^*\}$ to be the basis dual to a basis contained in $O_K$ w.r.t. the trace form.
\end{proof}

\begin{conclusion}
The $\mathbb{Z}$-module $O_K$ embeds in $\mathbb{Z}^n$ and contains a copy of $\mathbb{Z}^n$.
\end{conclusion}

\begin{theorem}
$O_K$ is a free $\mathbb{Z}$-module of rank $n$.
\end{theorem}

\begin{proof}
Classification of finitely generated Abelian groups.
\end{proof}

1.2. The absolute discriminant (skipped)

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

\begin{definition}
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 $\text{Hom}(K, \overline{Q})$.

\begin{lemma}
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 $B_{ij} = \text{Tr}_Q^K \omega_i \omega_j$ ("the Gram matrix of the quadratic space $(\oplus_{i=1}^{n} \mathbb{Z} \omega_i, \text{Tr}_Q^K)$"). Then $(\det A)^2 = \det B$.
\end{lemma}

\begin{proof}
$B = AA^t$ since $\text{Tr}_Q^K(x) = \sum_j \sigma_j(x)$.
\end{proof}

\begin{lemma}
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 $\alpha$.
\end{lemma}

\begin{proof}
$\det A = \prod_{i<j}(\omega_i - \omega_j)$ by the Vandermonde determinant, and $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.
\end{proof}

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

\begin{proof}
$B' = \gamma B \gamma^t$.
\end{proof}

\begin{corollary}
$\det B \neq 0$ iff $\{\omega_i\}$ is a $\mathbb{Q}$-basis.
\end{corollary}
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 \( \gamma \in \text{GL}_n(\mathbb{Q}) \) iff \( \det \gamma \neq 0 \). \( \square \)

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 \( \{ \omega_i \}, \{ \omega_j' \} \) generate the same lattice they are related by a matrix in \( \text{GL}_n(\mathbb{Z}) \) whose squared determinant is therefore 1. \( \square \)

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. \( \square \)

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. \( \square \)

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 \( d_{K/\mathbb{Q}}(L) = \det B = e^2 f \) with \( f \) squarefree. Since \( d_{K/\mathbb{Q}}(L) = d_K [\mathcal{O}_K : L]^2 \) it follows that \( [\mathcal{O}_K : L] \mid e \) 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 \( \frac{1}{e} L \) 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 \( d_{K/\mathbb{Q}}(\mathbb{Z} \oplus \mathbb{Z}[\sqrt{d}]) = \det \begin{pmatrix} \text{Tr}1 & \text{Tr}\sqrt{d} \\ \text{Tr}\sqrt{d} & \text{Tr}d \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d \). It follows that

\[
\begin{align*}
d_K = \begin{cases} 
d & d \equiv 1 \pmod{4} \\
4d & d \equiv 2, 3 \pmod{4} 
\end{cases}
\end{align*}
\]

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 \( \text{IJ} = \{ \sum_{i=1}^k a_i b_i \mid a_i \in I, b_j \in J \} \) 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 \( a \triangleleft \mathcal{O}_K \).

1. \( a \cap \mathbb{Z} \) is a non-zero proper ideal of \( \mathbb{Z} \).
2. \( [\mathcal{O}_K : a] < \infty \).
By construction \( n \) converse is not as easy – see Proposition 52. 

\textbf{DEFINITION 36.} The norm of an ideal is \( Na \triangleq [O_K : a] = \#(O_K/a) \).

\textbf{DEFINITION 37.} Say that a prime \( p \triangleleft O_K \) lies above \( (p) \triangleleft \mathbb{Z} \) if \( p \cap \mathbb{Z} = (p) \).

\textbf{REMARK 38.} Conversely, it is clear that for any rational prime \( p \), \( pO_K \) is a proper ideal of \( O_K \), hence that \( \exists \) 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 \( O_L \)) 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 \( O_K \). 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 \( a \), we replace \( p \) with a maximal ideal \( p \) containing \( a \). One issue now is constructing an ideal \( p^{-1}a \) such that \( p(p^{-1}a) = a \), but the real difficulty is in showing that \( p^{-1}a \) is “smaller” that \( a \) in the appropriate sense (its index in \( O_K \) is smaller) so that the inductive argument can run.

\textbf{DEFINITION 39.} An \( O_K \)-submodule \( a \subset K \) is a fractional ideal if there is \( \alpha \in K^* \) so that \( \alpha a \subset O_K \).

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

\textbf{LEMMA 40.} Every proper ideal of \( O_K \) contains a product of primes.

\textbf{PROOF.} Let \( a \) be a maximal counterexample. It is not prime so there are \( x, y \in O_K \setminus a \) with \( xy \in a \). Then \( (a,x)(a,y) = a \), a contradiction. \( \square \)

\textbf{PROPOSITION 41.} Let \( p \triangleleft O_K \) be prime. Then \( p^{-1} \triangleq \{ x \in K \mid xp \subset O_K \} \) is a fractional ideal properly containing \( O_K \). In particular, \( pp^{-1} = O_K \).

\textbf{PROOF.} Let \( p \in \mathbb{Z} \) be the prime lying below \( p \). Let \( x, y \in p^{-1} \) and \( \alpha \in O_K \). First, \( (\alpha x + y)p \subset xp + yp \subset O_K + O_K = O_K \). Second, if \( x \in p^{-1} \) then \( xp \in xp \subset O_K \) so \( pp^{-1} \subset O_K \). \( p^{-1} \supset O_K \) by definition of ideal, and the real issue (as noted above) is to see that \( p^{-1} \neq O_K \). For this note that the ideal \( pO_K \) contains a product of prime ideals. Let \( p_1 \cdots p_r \) be a minimal such product. Since \( p \) contains this product, it contains one factor, and hence equal to it (all primes are maximal). Let \( a \in p_2 \cdots p_r \setminus pO_K \) (this exists by minimality of \( r \)). Then \( ap \subset pO_K \) so \( \frac{a}{p}p \subset O_K \) but \( \frac{a}{p} \notin O_K \). Finally, \( p \subset pp^{-1} \subset O_K \). Since \( pp^{-1} \) is an \( O_K \)-submodule of \( O_K \) and \( p \) is a maximal ideal one side must be an equality. If \( pp^{-1} = p \) held then every \( y \in p^{-1} \) would preserve the finitely generated \( \mathbb{Z} \)-module \( p \) and hence be integral, a contradiction. \( \square \)
**Theorem 42.** All ideals of \( \mathcal{O}_K \) are invertible; every ideal can be uniquely written in the form \( \prod_{j=1}^r p_j^{e_j} \) with \( p_j \) prime and \( e_j \in \mathbb{Z}_{>0} \). \( a \mid b \) in the monoid of ideals iff \( b \subset a \).

**Proof.** First, let \( a \subset \mathcal{O}_K \) be a proper ideal and let \( a \subset p \triangleleft \mathcal{O}_K \) be a maximal ideal. Then \( p^{-1}a \subset p^{-1}p = \mathcal{O}_K \) and \( p^{-1}a \neq a \) since \( p^{-1} \not\subset \mathcal{O}_K \).

Now let \( a \triangleleft \mathcal{O}_K \) be maximal among the ideal without representation as a product of primes. Then \( p^{-1}a \) can be written as such a product, and hence so can \( a \). If \( a = \prod_i p_i \) then \( \prod_i p_i^{-1} = \mathcal{O}_K \) so \( a \) is invertible. For uniqueness let \( \prod_{j=1}^r p_j = \prod_{j=1}^s q_j \). Then \( p_r \) contains the product on the left, hence the product on the right, hence equal to one of the factors. Multiplying by \( p_r^{-1} \) the claim follows by induction on \( r \).

Finally, \( ac = b \) then certainly \( b \subset a \). Conversely, if \( b \subset a \) then \( a^{-1}b \subset a^{-1}a = \mathcal{O}_K \).

**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 \( \prod_{i=1}^r p_i^{e_i} \) 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 \( a, b \) are in the same class if \( ab^{-1} \) 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 \( Cl(K) \) of the group of ideals by the group of principal ideals. It measures the failure of unique factorization.

**Theorem 45 (Dedekind).** \( Cl(K) \) is a finite group. Its order is denoted \( h_K \) and called the class number of \( K \).

This is an immediate Corollary of Theorem 185 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).** \( \lim_{x \to \infty} \frac{\#\{p | Np \leq x, \text{p principal}\}}{\#\{p | Np \leq x\}} = \frac{1}{h_K} \).

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

Fix a finite extension \( L/K \) of number fields and a prime \( p \triangleleft \mathcal{O}_K \).

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

**Lemma 48.** Let \( \mathfrak{P} \) be a prime of \( L \). Then \( p = \mathfrak{P} \cap \mathcal{O}_K \) 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 \( p \) and write \( \mathfrak{P} \triangleright p \).

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

**Definition 50.** The number \( q_p = \#\mathcal{O}_K/p \) is called the residue field size. \( f(\mathfrak{P}/p) \) \( \overset{\text{def}}{=} [k_\mathfrak{P} : k_p] = \dim_{k_p} k_\mathfrak{P} \) is called the residue index or the inertial degree.
**Lemma 51.** Let $p$ be a prime of $K$. Then $\mathfrak{P}|p$ iff $\mathfrak{P}|pO_L$.

**Proof.** Exercise.

**Proposition 52.** $pO_L \neq O_L$. In particular, $\{\mathfrak{P} \triangleleft O_L \mid \mathfrak{P}|p\}$ is non-empty and finite.

**Proof.** Exercise.

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

**Lemma 54.** Let $\mathfrak{P} \triangleleft O_L$ be prime. Then for all $e \geq 1$, $O_L/\mathfrak{P}^e$ is a dvr – a local ring and a PID.

**Proof.** The ideals of $O_L/\mathfrak{P}^e$ correspond to the ideals of $O_L$ 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.** $n = \sum_{i=1}^{r} e_if_i$.

**Proof.** We calculate the dimension of the $k_p$-vector space $O_L/pO_L$ 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, $pO_L = \cap_{i=1}^{r} \mathfrak{P}_i^{e_i}$ (they have the same prime factorization). By the CRT, $O_L/pO_L \cong \oplus_{i=1}^{r} O_L/\mathfrak{P}_i^{e_i}$. Now $O_L/\mathfrak{P}_i^{e_i} \cong O_L/\mathfrak{P}_i \oplus \mathfrak{P}_i^{e_i}$ and by Lemma 54 multiplication by $\bar{\pi}^j$ gives a vector space isomorphism $O_L/\mathfrak{P}_i \to \mathfrak{P}_i^{j}/\mathfrak{P}_i^{j+1}$, so $\dim_{k_p} O_L/\mathfrak{P}_i^{e_i} = e_if_i$.

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

**1.4.2. Explicit factorization (Lecture 7).**

**Theorem 56.** Suppose $O_L = O_K[\alpha]$, and let $f \in O_K[x]$ be the minimal polynomial of $\alpha$ over $K$. For a prime $p \triangleleft O_K$ let $\bar{f} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ be the factorization of the image of $f$ in $k_p[x]$ into irreducibles. Then there are $r$ primes of $L$ lying above $p$, and $f(\mathfrak{P}_i/p) = \deg \bar{P}_i$ and $e(\mathfrak{P}_i/p) = e_i$.

**Proof.** We have

$$O_L/pO_L \cong O_K[x]/(f,x) \cong k_p[x]/(\bar{f}) \cong \bigoplus_{i=1}^{r} k_p[x]/(\bar{P}_i^{e_i}).$$

It follows that there are $r$ ideals of $O_L$ in the factorization of $p$, with $O_L/\mathfrak{P}_i \cong k_p[x]/(\bar{P}_i)$ hence $f(\mathfrak{P}_i/p) = \deg \bar{P}_i$. Also, $\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \subset pO_L$ (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 $O_K = \mathbb{Z}[\sqrt{-5}]$ 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 $(x + 1)/((x + 1)^2)$ in $\mathbb{F}_2[x]/((x + 1)^2)$, so the ideal will be $(2, 1 + \sqrt{-5})$.

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

13
Remark 58. In case where $O_L$ is not of this form localize at $p$ first.
Furthermore, if $[O_L : O_K[\alpha]]$ is prime to $p$ (the rational prime under $p$) 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 $G = \text{Gal}(L : K)$. It is clear that $G$ acts on the set of primes $\{p_i\}_{i=1}^g$ lying over $p$.


Proof. Suppose that $\mathfrak{P}^\prime$ is not in the $G$-orbit of $\mathfrak{P}$. By the CRT there exists $x \in O_L$ such that $x \in \mathfrak{P}^\prime$ but $x \not\in (\sigma \mathfrak{P})$ for all $\sigma \in G$. It follows that $\sigma x \not\in \mathfrak{P}$ for all $\sigma \in G$, and since $\mathfrak{P}$ is prime we have $N^K_L x \not\in \mathfrak{P}$. But $N^K_L x \in \mathfrak{P}^\prime \cap O_K = p \subset \mathfrak{P}$, a contradiction. □

Corollary 60. All primes above $p$ 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 $k_{\mathfrak{P}} = O_L/\mathfrak{P}$, fixing $k_p = O_K/\mathfrak{P}$. In other words, there is a natural homomorphism

\[ G_{\mathfrak{P}} \to \text{Gal}(k_{\mathfrak{P}} : k_p) . \]

Lemma 62. Let $K \subset E \subset L$ be the fixed field of $G_{\mathfrak{P}}$. Then $\mathfrak{P}$ is the unique ideal of $O_L$ lying above $\mathfrak{P} \cap O_E$, and the injection $O_K/p \to O_E/\mathfrak{P} \cap O_E$ is an isomorphism.

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

Proposition 63. This map $G_{\mathfrak{P}} \to \text{Gal}(k_{\mathfrak{P}} : k_p)$ is surjective.

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

Definition 64. The kernel of this map is called the inertia subgroup $I$. Any element of $G_{\mathfrak{P}}$ projecting to the generator of $\text{Gal}(k_{\mathfrak{P}} : k_p)$ (given by $x \mapsto x^{q^p}$) is called a Frobenius element and is denoted $\mathfrak{F}$.

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 $\sigma$ is a Frobenius element iff $\sigma x \equiv x^{q^p}(\mathfrak{P})$. 


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 \( v : F \to \mathbb{R} \cup \{\infty\} \) 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. \( F = \mathbb{Q}, v_p \left( \frac{p}{r} \right) = r \) where \( p \nmid ab \).
2. \( F = K(t) (K \text{ a field}), p \in K[t] \text{ irreducible}, v_p \left( \frac{p}{r} \right) = r \) where \( p \nmid ab \).
3. \( F = K(t), v_{\infty} \left( \frac{g}{h} \right) = \deg b - \deg a \).

**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 *discrete* 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 \( |p'|_p = \frac{1}{p'} \).

**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

\[
|x+y|^n = \left| \sum_{k+l=n} \binom{n}{k} x^k y^l \right| \leq \sum_{k+l=n} \binom{n}{k} (\max\{|x|,|y|\})^n \leq (n+1)M (\max\{|x|,|y|\})^n
\]

and the claim follows by taking \( n \)th 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-discrete 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 unique $\lambda$ 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 $|b|_2^n \leq |a|_1^m \leq |b|_2^n (1 + \varepsilon)$. Then $1 \leq \left| \frac{a^m}{b^n} \right|_2 \leq (1 + \varepsilon)$ while $\left| \frac{a^m}{b^n} \right|_1 = \left| \frac{a^m}{b^n} \right|_2^\lambda \left( \frac{|b|_2^n}{|a|_1^m} \right)^n \leq (1 + \varepsilon)^\lambda \left( \frac{|b|_2^n}{|a|_1^m} \right)^n$. 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-discrete absolute values of $F$.

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

**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-discrete absolute values on a field $F$. Let $x \in F^n$ and let $\varepsilon > 0$. Then there is $y \in F$ such that $|y - x|_i < \varepsilon$.

**PROOF.** We first construct for each $2 \leq k \leq n$ some $z_k \in F$ such that $|z_k|_1 > 1$ and $|z_k|_j < 1$ 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 $|z_k|_{k+1} < 1$ then we are done. If $|z_k|_{k+1} \geq 1$ choose $w$ such that $|w|_1 > 1$ and $|w|_{k+1} < 1$. If $|z_k|_{k+1} = 1$ 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 $|z_k|_{k+1} > 1$ 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 $|z_i|_1 > 1$ and $|z_i|_j < 1$ if $j \neq i$. Now let $w_i = \frac{z_i}{\sum_{j=1}^n z_j}$. Then $\sum_{i=1}^n w_i = 1$ and $\lim_{s \to \infty} |w_i|_j = \delta_{ij}$. It follows that for any $\varepsilon > 0$ there is $s$ large enough such
that $|w_i - \delta_{ij}| < \varepsilon$. Now given $\chi \in F$ let $y = \sum_{i=1}^{n} w_i \chi_i$. Then $|y - x|_j = |\sum_{i=1}^{n} (w_i - \delta_{ij}) \chi_i|_j \leq \varepsilon \sum_{i=1}^{n} |\chi_i|_j$.

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 $f : X^n \to Y$ be uniformly continuous on every ball. Then there is a unique continuous function $\hat{f} : \hat{X}^n \to Y$ 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 $\left( x_i^j \right)_{j=1}^{\infty} \subset X$ be a Cauchy sequence. Let $R$ be such that $d_X\left( x_i^j, x_i^k \right) \leq R$ for all $i, j$. Then since $f$ is uniformly continuous on $\{ x \in X^d \mid \max_i d_X(x_i, x_i^j) \leq R \}$, $(f(x_j^j))_{j=1}^{\infty}$ is a Cauchy sequence in $Y$. Letting $x_j$ be the join of two Cauchy sequences with the same limit shows that $\lim_{j \to \infty} f(x_j^i)$ only depends on the limit of the $x_j$, 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 $|p^k a/b - x|_p \leq p^{-r}$ for some $r \geq 0$. Then $p^{-k} = |p^k a|_p \leq \max \left\{ |p^k a/b - x|_p, |x|_p \right\} \leq 1$ so $k \geq 0$. Now let $b \in \mathbb{Z}$ be an inverse to $b$ mod $p^r$. Then $p^k ab \in \mathbb{Z}$ and

$$|p^k ab - x|_p \leq \max \left\{ |p^k ab - p^k a/b|_p, |p^k a - b|_p, |x|_p, |x|_p \right\} = \max \left\{ p^{-k} |1 - bb|_p, p^{-r} \right\} \leq \max \left\{ p^{-k-r}, p^{-r} \right\} = p^{-r}.$$

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 \( x \neq y(p^k \mathbb{Z}_p) \). Now \( y + p^k \mathbb{Z}_p \) and \( \bigcup_{a \neq x(p^k)} a + p^k \mathbb{Z}_p \) are disjoint and cover \( \mathbb{Z}_p \). 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 \( 3 \mathbb{Z}_3 = 9 \mathbb{Z}_3 \cup 3 + 9 \mathbb{Z}_3 \cup 6 + 9 \mathbb{Z}_3 \) and \( 2 + 3 \mathbb{Z}_3 = 2 + 9 \mathbb{Z}_3 \cup 5 + 9 \mathbb{Z}_3 \cup 8 + 9 \mathbb{Z}_3 \), \( 5 + 9 \mathbb{Z}_3 = 5 + 27 \mathbb{Z}_3 \cup 14 + 27 \mathbb{Z}_3 \cup 23 + 27 \mathbb{Z}_3 \). Get a \((p + 1)\)-regular rooted tree, rooted at \( \mathbb{Z}_p \). 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 \( A \subset Z \) be a set of representatives for \( Z / p^k \mathbb{Z} \) and let \( f : A^n \to \mathbb{Z}_p \) be the map \( f(a) = \sum_{j=0}^{\infty} a_j p^j \). We show the map is a homeomorphism. By Lemma 83 each such series converges in \( \mathbb{Z}_p \) (it is a closed subset of \( \mathbb{Q}_p \), 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 \( A^n \). For injectivity suppose that \((a'_j)_{j \geq 0} \) is a second sequence, and that \( j_0 \) is the first time they disagree. Then 
\[
\left( \sum_{j=0}^{\infty} a_j p^j \right) - \left( \sum_{j=0}^{\infty} a'_j p^j \right) = p^{j_0} (a_{j_0} - a'_{j_0}) + p^{j_0+1} \sum_{j > j_0} (a_j - a'_j) p^j.
\]
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) \( A^n \) is compact by Tychonoff so \( \mathbb{Z}_p \) is compact. In fact, the compactness shows that \( f \) is a closed map hence a homeomorphism. Concretely, 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 \( m, k \) 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-discrete 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-discrete). 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, \( U' = B_F(0,1)U_2 \cup \{x \mid |x| \leq 1 \} \) 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-discrete 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 \( W_1 = \text{Span}_F \{v_i\}_{i=1}^n \), \( W_2 = \text{Span}_F \{v_{n+1}\} \). Then by induction \( W_1, W_2 \) are linearly homeomorphic to \( F^n, F \) respectively hence complete and closed in \( V \). Let \( f : F^{n+1} \to V \) be the map \( f(x) = \sum_{i=1}^{n+1} x_i v_i \). 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-discrete. Then \( L_w \) is an algebraic extension of \( F_v \). In fact, \( [L_w : F_v] \leq [L : F] \).
\textbf{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 \( L_w = L \cdot F_v \). 

\textbf{2.2.2. Extension of valuations.} Let \( K \) be a field equipped with a (non-discrete) non-archimedean absolute value \(|\cdot|\).

\textbf{Lemma 93.} Let \( \mathcal{O} = \{ x \in K \mid |x| \leq 1 \}, \ p = \{ x \in K \mid |x| < 1 \} \).

(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) \( \mathcal{O} \) is a valuation ring.

(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 \( \mathcal{O} \).

\textbf{Proof.} PS3.

\textbf{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 \( \kappa \).

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 \( f \neq 0 \).

\textbf{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 \(|\alpha - \beta| \leq \left| \frac{f(\alpha)}{f'(\alpha)} \right| < 1 \).

(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 \( \deg g = \deg \bar{g} = \deg \bar{h} \) and \( f = gh \).

\textbf{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

\[ f(x) = f(\alpha) + f'(\alpha)(x - \alpha) + g(x)(x - \alpha)^2 \times \]

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 \(|f'(\alpha_n)| = |f'(\alpha)|, \left| \frac{f(\alpha_n)}{f'(\alpha_n)^2} \right| \leq c^{2n} \). Then \( \alpha_n, \alpha_{n+1} \in \mathcal{O} \). Using a Taylor expansion for \( f'(x) \), there is \( \gamma \in \mathcal{O} \) such that

\[ |f'(\alpha_{n+1})| = |f'(\alpha)| \times \]

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

\[ \left| \frac{f'(\alpha_{n+1})}{f'(\alpha_{n+1})^2} \right| \leq \left| \frac{f(\alpha_n) + f'(\alpha_n)(\alpha_{n+1} - \alpha_n) + \gamma(\alpha_{n+1} - \alpha_n)^2}{f'(\alpha_{n+1})^2} \right| \leq \left| \frac{f(\alpha_n)^2}{f'(\alpha_n)^4} \right| \leq \left( c^{2n} \right)^2 \times \]
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, $|\alpha_{n+1} - \alpha_n| = \left| \frac{f(\alpha_n)}{f(\alpha)} \right| \leq c^n \leq c$ so by induction $|\alpha_n - \alpha| \leq c$ and $|\beta - \alpha| \leq c$.

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

$$f - g_{n+1} h_{n+1} = (f - g_n h_n) - \pi^{n+1} (g_n q_{n+1} + h_{n+1} p_{n+1}) - \pi^{2n+2} p_{n+1} q_{n+1}$$

and thus

$$\pi^{-(n+1)} [f - g_{n+1} h_{n+1}] \equiv \pi^{-(n+1)} [f - g_n h_n] - (g_0 q_{n+1} + h_0 p_{n+1}) (\pi \mathcal{O}).$$

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

$$(g_0 q_{n+1} + h_0 p_{n+1}) \equiv \pi^{-(n+1)} [f - g_n h_n] (\pi \mathcal{O}).$$

Let $f_n = \pi^{-(n+1)} (f - g_n h_n) \in \mathcal{O}[x]$. Since $\bar{g}, \bar{h}$ are relatively prime, we could have fixed $a, b \in \mathcal{O}[x]$ such that $a \bar{g} + b \bar{h} = 1$. Now if $\pi$ divides the coefficients of $a g_0 + b h_0 - 1 \in p[x]$ 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 $p$) so we can divide with remainder $bf_n = g_0 p_n + r$ where $\deg r < \deg g_0 = k$. Then we also have

$$g_0 (af_n + h_0 q) + h_0 p_{n+1} \equiv f_n (\pi \mathcal{O}).$$

Define $q_{n+1}$ by omitting from $(af_n + h_0 q)$ any coefficient divisible by $\pi$. Then

$$g_0 q_{n+1} + h_0 p_{n+1} \equiv f_n (\pi \mathcal{O}).$$

Also, since the leading coefficient of $g_0$ is a unit, and since $\deg(h_0 p_{n+1}) < d$, $\deg f_n \leq d$ we must have $\deg q_{n+1} \leq d - k$. \qed

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

**Proof.** Multiply by a constant to make $f \in \mathcal{O}[x]$ and $|f| = 1$. If $a_0, a_d \in p$ write $\bar{f} = x^r \bar{h}$ for some $\bar{h}$ non-vanishing at $0 \in K$. Then $r > 0$ since $a_0 \in p$ 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. \qed

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

**Theorem 98.** Let $K$ be complete with respect to a non-discrete non-archimedean absolute value and let $L/K$ be an algebraic extension of degree $n$. Then $|\alpha| \overset{\text{def}}{=} |N_K^L(\alpha)|^{1/n}$ 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 $\alpha$. 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 $\alpha$ is integral over $\mathcal{O}_K$. Conversely, if $\alpha$ 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

$$\left| \frac{\alpha}{\beta} \right| \leq 1 \text{ so } \left| 1 + \frac{\alpha}{\beta} \right| \leq 1 \text{ so } |\alpha + \beta| \leq |\beta|.$$
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 \( \mathbb{R} \).
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 \( \mu \) 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 \( |a| \in \mathbb{R}_+^\times \) 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 \( |(1 + x)^N| \) 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 characteristics one shows that the field of constants is the residue field.

For details see \( \square \)

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, \( p_L \) the prime, \( \lambda \) 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 \( \lambda \) over \( \kappa \). Let \( \{\Pi_j\}_{j=0}^{e-1} \subset \mathcal{O}_L \) be such that \( |\Pi_j|_w \) 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 \( p \). Call the resulting sum \( s'_j \). Then \( s'_j \in \mathcal{O}_L \) but reducing mod \( p_L \) not all coefficients are zero in \( \kappa \), so \( s'_j \notin p_L \) by the choice of \( \omega_j \). It follows that \( s'_j \in \mathcal{O}_L^\times \) so \( |s'_j| = 1 \), at which point \( |s_j| \in |K^\times| \). 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 \( \Pi \) is a uniformizer. Then \( M = \bigoplus \lambda \mathcal{O}_K \omega_j \Pi_j \subset \mathcal{O}_L \). We will show equality. Let \( N = \bigoplus \lambda \mathcal{O}_K \omega_i \). Then \( N + \Pi \mathcal{O}_L = \mathcal{O}_L \) since \( \omega_i \) are a generating set for \( \mathcal{O}_L/\Pi \mathcal{O}_L \) as an \( \mathcal{O}_K \)-module. Iterating we find
\[
\mathcal{O}_L = N + \Pi(N + \Pi(\cdots)) = \sum_{j=0}^{e-1} \Pi^j N + \Pi^e \mathcal{O}_L = M + \Pi^e \mathcal{O}_L = M + \sigma \mathcal{O}_L.
\]
It now follows by induction that
\[
\mathcal{O}_L = M + \sigma^k \mathcal{O}_L
\]
for all \( k \geq 1 \). But then \( M \) is dense in \( \mathcal{O}_L \) (\( \sigma^k \mathcal{O}_L \) 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 \( M = \mathcal{O}_L \).

\begin{remark}
This gives an alternative proof of the claim from chapter 1.
\end{remark}

\subsection{Unramified extensions.}

\begin{definition} 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.
\end{definition}

\begin{lemma} 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.
\end{lemma}

\begin{proof}
First, \( \lambda / \kappa \) is separable iff \( \mu / \kappa \) and \( \lambda / \mu \) 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 \([\lambda : \kappa] = [L : K]\).
\end{proof}

\begin{proposition}
Inside a fixed algebraic closure \( \bar{K} \) let \( L/K \) be unramified, \( M/K \) any extension. Then \( LM/M \) is unramified.
\end{proposition}

\begin{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 \( \alpha \). Then \( \bar{f} \in \kappa[x] \) is monic, and \( \bar{f}(\bar{\alpha}) = 0 \) \([\lambda : \kappa] \leq \deg \bar{f} \leq [L : K] = [\lambda : \kappa]\). 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 \( \alpha \) 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.
\end{proof}

\begin{corollary}
Let \( L/M/K \) be a tower of algebraic extensions. Then \( L/K \) is unramified iff both of \( L/M, M/K \) are.
\end{corollary}

\begin{proof}
PS4
\end{proof}

\begin{theorem}
The compositum of unramified extensions is unramified.
\end{theorem}

\begin{definition}
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 \( K \).
\end{definition}

\begin{proposition}
Let \( T/K \) be the maximal unramified subextension of \( L/K \). Then \( \tau \) is the separable closure of \( \kappa \) in \( \lambda \), and \( T, K \) have the same value groups.
\end{proposition}
PROOF. We have $e = 1$ in every finite subextension of $T/K$, so the value groups are the same. Now let $\tilde{\alpha} \in \lambda$ be separable over $\kappa$, 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 $\bar{f}(\tilde{\alpha}) = 0$ while $\bar{f}'(\tilde{\alpha}) \neq 0$ since $\bar{f}$ is separable. It follows from Hensel’s Lemma again that $f$ has a root $\alpha \in L$ lifting $\tilde{\alpha}$. Then $K(\alpha)$ is unramified over $K$ since $[K(\alpha) : K] = \deg f = \deg \bar{f} = [\kappa(\tilde{\alpha}) : \kappa]$. $\square$

2.3.3. Ramification. Suppose now that $\kappa$ 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 $p = \text{char}(\kappa)$.

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 $\Pi$ 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 $\Pi^d$. But this coefficient is in $K^\times$, so its absolute value is an integer power of $\Pi^e$. It follows that $e|d$ so $e = d$ and the constant coefficient of the minimal polynomial is $\mathfrak{p}$ 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 $\Pi$ 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 $i < e$ $|a_i| < |\Pi|$. 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 $1 \leq i \leq e-1$, $|a_i \Pi^i| < |a_i| \leq |a_0|$. Since $f(\Pi) = 0$ it follows that $|\Pi|^e = |a_0|$, and since $|K^\times|$ is generated by $|a_0|$ this means that $e \deg(K(\Pi) : K) \geq e$. We thus have:

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

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

Then $|\Pi| = |N^L_K \Pi|^{1/e} = |\mathfrak{p}|^{1/e}$ by assumption, so $e(L/K) = e = [L : K]$. $\square$

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 $\alpha$ 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 $\left|\frac{g(\alpha)}{(g'(\alpha))}\right| < 1$. Then by Hensel’s Lemma $g$ has a root in $K$ so (since 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! $\square$
2.4. Places of number fields

2.4.1. On passing to the completion. Let $F$ be a field, $v$ a non-archimedean place of $F$.

**Lemma 115.** $R_v = \{x \in F \mid |x|_v \leq 1\}$ is a subring, $p_v = \{x \in F \mid |x|_v < 1\}$ is a maximal ideal of the subring, and $R_v, p_v$ are dense in the corresponding subring and idea of $F_v$.

**Corollary 116.** The residue field is the same on both sides.

2.4.2. Extension of absolute values.

**Lemma 117.** 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 $|a_i \alpha^i| = |\alpha|^i < |\alpha|^d$ and hence $|f(\alpha)| = |\alpha|^d > 0$. It follows that $\alpha$ is transcendental over $K$. 

**Definition 118.** 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 119.** There is a natural bijection between $\{w \in |L| \mid w|v\}$ and $\text{Hom}(L, \bar{K}_v)/\text{Gal}(K_v)$.

**Proof.** $v$ has a unique extension to $\bar{K}_v$, which is therefore Galois-invariant. This gives a map $\text{Hom}_K(L, \bar{K}_v)/\text{Gal}(K_v) \to \{w \in |L| \mid w|v\}$. 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 $\bar{K}$-homomorphism $\sigma : L \to L'$. Then $\sigma$ 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 120.** 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.** $\text{Hom}_K(L, \bar{K}_v)$ 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 121.** This is a new proof of 56, which now applies even to primes dividing the discriminant of $\alpha$.

**Example 122.** Let $K$ be a number field, $v$ an archimedean place, $L/K$ a finite extension. Suppose $L = K(\alpha)$. If $K_v \cong \mathbb{C}$ then $K_v \cong \mathbb{C}$ for all $w|v$; $\alpha$ has $n = [L:K]$ $K_v$-embeddings in $\mathbb{C}$ so there are $n$ places, all complex. If $K_v \cong \mathbb{R}$ 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 $\mathbb{R}$".
EXAMPLE 123. 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 $(x - \sqrt[3]{2}) (x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ 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 Eisenstein hence irreducible. Thus there is a unique place $w_2 | 2$ and the extension is totally (but tamely) ramified.
- 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 $f_1f_2$ 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 unramified extension: since $\bar{f}_2$ is irreducible, we have $f\left(L_{w_3} : \mathbb{Q}_5\right) \geq \deg \bar{f}_2 = 2 = \left[L_{w_3} : \mathbb{Q}_5\right]$.
- Over $\mathbb{Q}_p$, $p \geq 5$, $\bar{f}(x) = 3x^2$ is relatively prime to $\bar{f}$, so by Hensel’s Lemma $f$ factors as $f = \prod_i f_i$ where $\bar{f}_i = \prod_i \bar{f}_i$ and the $f_i$ are irreducible and distinct. It follows that the places over $p$ correspond to the $f_i$ and they are all unramified since again $f\left(L_{w_p} : \mathbb{Q}_p\right) \geq \deg \bar{f}_i = \deg f_i = \left[L_{w_p} : \mathbb{Q}_p\right]$.
- If $p \equiv 1 \pmod{3}$ 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 $p = \pi \mathfrak{p}$ in the Eisenstein integers $\mathbb{Z}[\omega]$. Then $f(\pi : p) = 1$ (since $\omega = 2$ and $\bar{g} = 2$) so $\mathbb{Z}[\omega]/\pi \mathbb{Z}[\omega] \simeq \mathbb{Z}/p\mathbb{Z}$ and thus we need to decide if $(\frac{2}{\pi})_3 = 1$ and by cubic reciprocity this is $(\frac{\pi}{2})_3$ if we choose $\pi$ 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 $(\frac{\pi}{2})_3 = 1$ iff $\pi \equiv 1 \pmod{2}$.
- Writing $p = a^2 + 3b^2$ where $a, b \in \mathbb{Z}$ (take the norm of $\pi$) $p$ is primary if

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

**Theorem 124.** If $L/K$ is separable, this is an isomorphism.

**Proof.** Say $L = K(\alpha)$ with minimal polynomial $f \in K[x]$. Let $f = \prod_v f_v$ be the factorization of $f$ in $K_v[x]$. Then by the CRT $\prod_v L_v = \prod_v \left(K_v[x]/(f_v)\right) = K_v[x]/fK_v[x] = K_v \otimes_K (K[x]/fK[x])$.

**Corollary 125.** If $L/K$ is separable we have $[L : K] = \sum_{v|v} [L_v : K_v] = \sum_{v|v} e(w|v) f(w|v)$.

**Remark 126.** Note that this is a new proof of Theorem 55.

**Corollary 127.** If $L/K$ is separable we have for all $v \in |K|$ and $\beta \in L$ that $\text{Tr}_{L/K}^v \beta = \sum_{w|v} \text{Tr}_{K_{v'}}^w \beta$ and $N_{L/K}^w \beta = \prod_{w|v} N_{K_w}^w \beta$.  

26
PROOF. \( \text{Tr}_K^L \beta \) let \( M_\beta \in \text{End}_{K, \text{vsp}}(L) \) and \( M'_\beta \in \text{End}_{K, \text{vsp}}(K_v \otimes L) \) be multiplication by \( \beta \). Then \( M'_\beta = 1 \otimes M_\beta \) so \( \text{Tr} M_\beta = \text{Tr} M'_\beta \). But under the decomposition \( K_v \otimes L \simeq \bigoplus_w L_w \) each \( L_w \) is \( M'_\beta \)-invariant, so

\[
\text{Tr} M'_\beta = \sum_{w|\nu} \text{Tr} (M'_\beta | L_w) = \sum_{w|\nu} \text{Tr}_{L_w} I_\nu \beta .
\]

\( \square \)

PROPOSITION 128. Suppose \( L/K \) is Galois. Then \( G = \text{Gal}(L/K) \) acts transitively on the places above \( \nu \).

PROOF. Suppose not. Then there are two disjoint orbits. By weak approximation (Theorem \ref{thm:78}) can find \( \alpha \in L \) such that \( |x|_\nu < 1 \) in one orbit, but \( |x|_\nu > 1 \) in the other orbit. Taking norms we get a contradiction. \( \square \)

DEFINITION 129. The decomposition group is \( G_w = \text{Stab}_G(w) \). If \( v \) is non-archimedean we also have the inertia subgroup \( I_w = \text{Ker}(G_w \to \text{Aut}(\lambda_w : \kappa_w)) = \{ \sigma \in G_w | \sigma x \equiv x (\mathcal{P}_w) \} \).

LEMMA 130. \( \lambda_w/\kappa_w \) is normal and the map \( G_w \to \text{Aut}(\lambda_w : \kappa_w) \) is surjective.

PROOF. Let \( f \in \kappa_w[x] \) be irreducible and have a root in \( \lambda_w \). Then \( \square \)

LEMMA 131. Let \( K \subset E \subset L \) be the fixed field of \( G_w \). Then \( w \) is the unique place lying above its restriction to \( E \), and \( f_w(E/K) = 1 \).

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

\( \square \)

2.4.3. Places of number fields.

DEFINITION 132. Let \( K \) be a number field. Call a place of \( K \) infinite if it is archimedean (equivalently, lies over the archimedean place of \( \mathbb{Q} \)), finite otherwise (it if lies over a non-archimedean place of \( \mathbb{Q} \)). Write \( |K|_\infty \), \( |K|_f \) for the two sets of places.

PROPOSITION 133. Let \( F \) be a number field. Then

1. \( |F|_\infty = \text{Hom}(F, \mathbb{C})/\text{Gal}(\mathbb{C}/\mathbb{R}) \).
2. \( |F|_f = \{ |\cdot|_p | p \leq \mathcal{O}_F \text{ prime} \} \).

PROOF. (1) This is Lemma \ref{lem:179}.

(2) Let \( p \leq \mathcal{O}_F \) be prime, and for \( x \in \mathcal{O}_F \) let \( v_p(x) = e \) where \( p^e || x \mathcal{O}_F \). 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-archimedean 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 \( |f(\alpha)|_v = |\alpha|^d_v > 0 \) so \( \alpha \notin \mathcal{O}_F \). It follows that \( |x|_v \leq 1 \) for all \( x \in \mathcal{O}_F \) and hence that \( p = \{ x \in \mathcal{O}_F | |x|_v < 1 \} \) is a prime ideal of \( \mathcal{O}_F \). Since \( |p|_v = |p|_p < 1 \) we have \( p \in p \) so \( p | p \). Let \( |\cdot|_p \) be the absolute value corresponding to this ideal, normalized the same way. Then the two absolute values agree on \( p \) and on \( \mathcal{O}_F \setminus p \), hence on the invertible elements of \( (\mathcal{O}_F)_p \). But that ring
is a local PID, so it is now enough to check that they agree on a uniformizer, which must be the case since they agree on $p$ which is associate to a power of the uniformizer.

We now introduce a new normalization of the absolute values.

**Definition 134.** Let $F$ be a number field, $v \in |F|$. We write $|\cdot|_v$ for an absolute value in the class of $v$ which restricts to the usual absolute values on $Q$. We write $\|\cdot\|_v$ for the absolute value of that class such that $\|p\|_v = p^{-1/e}$ if $v|p$ and $e = e(v/p)$, $\|z\|_v = |z|$ if $F_v \simeq \mathbb{R}$ and $\|z\|_v = z\bar{z}$ if $F_v \simeq \mathbb{C}$.

**Lemma 135.** Let $K$ be a number field, $v$ a finite place corresponding to the ideal $p$. Then $\mathcal{O}$ is dense in $\mathcal{O}_v$, and the map $\mathcal{O}/p^j \to \mathcal{O}_v/p_v^j$ is an isomorphism.

**Proof.** Same as in $\mathbb{Q}_p$.

**Lemma 136.** 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 $e(L_w/K_v) = e(\mathfrak{p}/p)$ and $f(L_w/K_v) = f(\mathfrak{p}/p)$.

**Proof.** Lemma 115 shows that $\mathcal{O}_K/v \simeq \mathcal{O}/p$ and $\mathcal{O}_L/w \simeq \mathcal{O}_L/w$ in compatible fashions. For the ramification indices localize at $p$, $\mathfrak{p}$ first. This does not change the ramification index, and now after localization we have $(\mathfrak{p})^e = p$ and that both ideals are principal, so there is nothing to prove.

**Proposition 137 (Product formula).** For all $x \in F^\times$,

$$\prod_{v \in |F|} \|x\|_v = 1.$$
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 \( \mathfrak{p} \mid \mathcal{O}_L \) divides the different iff \( e(\mathfrak{p} : \mathcal{O}_L) > 1 \), while \( \mathfrak{p} \mid \mathcal{O}_K \) divides the discriminant iff there is \( \mathfrak{p} \mid \mathfrak{P} \) 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)

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

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 \( K_\infty = \prod_{\nu|\infty} K_\nu \) is an \( \mathbb{R} \)-algebra with \( \dim_{\mathbb{R}} K_\infty = \sum_{\nu|\infty} f(K_\nu : \mathbb{R}) = n \) 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 \( N_{K_\infty}^{K_\nu} \) is continuous.

Example 138. \( \mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R} \times \mathbb{R} \). \( \sqrt{2} \) 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 \( K_\infty \). Since \( \text{rk}_\mathbb{Z} \mathcal{O}_K = n = [K : \mathbb{Q}] \) (see xxx), \( \mathcal{O}_K \) is cocompact.

Exercise. For \( k = (k_\nu)_{\nu|\infty}, x = (x_\nu)_{\nu|\infty} \in K_\infty \) define \( e_k(x) = \exp \left( 2\pi i \sum_{\nu|\infty} \text{Tr}_{\mathbb{Q}}^{K_\nu}(k_\nu x_\nu) \right) \). Now that if \( k, x \) are images of \( k, x \in K \) then \( e_k(x) = \exp(2\pi i \text{Tr}_Q^K(kx)) \) (see Corollary 127). It now follows (for general \( k \)) that \( e_k \) is \( K \)-periodic iff \( \text{Tr}_Q^K(kx) \in \mathbb{Z} \) for all \( x \in \mathcal{O}_K \). In other words, characters of \( K_\infty/\mathcal{O}_K \) are parametrised by the dual lattice \( \mathcal{O}_K^\vee \).

\[
L^2(K_\infty/\mathcal{O}_K) \simeq \bigoplus_{k \in \mathbb{Z}} \mathbb{C} e_k
\]
3.1.2. The trace form. The trace form \((x,y) = \text{Tr}_K^L(xy)\) is a non-degenerate bilinear form on \(L\), and so gives an identification of \(L\) with its dual \(K\)-vector space (for its first use in the course, see Proposition 19). From now on write simply \(\text{Tr}\) unless we need to specify the field.

**Definition 139.** Let \(\Lambda \subset L\) be an \(\mathcal{O}_K\)-submodule. We define the dual of \(\Lambda\) to be \(\Lambda^* = \{x \in L \mid \text{Tr}_K^L (x\Lambda) \subset \mathcal{O}_K\}\).

Note that \(\Lambda^*\) is always an \(\mathcal{O}_K\)-submodule of \(L\).

**Lemma 140.** 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 \(\text{Tr}_K^L (\omega_i \omega_j) \in \mathbb{Z}\) 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 \(a_j = \text{Tr}_K^L \left( \omega_i \sum_{j=1}^n a_j \omega_j^* \right) \in \mathcal{O}_K\).

**Corollary 141.** The dual of a fractional ideal is a fractional ideal.

**Proof.** First note that \(\mathcal{O}_L \subset \mathcal{O}_L^\prime\) and that if \(\alpha \in L^\times\) then \((\alpha L)^* = \alpha^{-1}L^*\) (so that we may freely replace \(\alpha\) with \(\alpha a\) without loss of generality). Now let \(a\) be a fractional ideal of \(L\). Then if \(x \in a^*\) and \(\alpha \in L\) we have \(\text{Tr}_K^L (\alpha \alpha^*) = \text{Tr}_K^L (\alpha \alpha^*) = \alpha^*\) so \(a^*\) is an \(\mathcal{O}_L\)-module. If \(a \subset \mathcal{O}_L\) then \(a^* \supset \mathcal{O}_L^\prime \supset \mathcal{O}_L\) so it is non-zero. Finally, let \(\alpha \in \text{abe non-zero and let } \{\omega_i\}_{i=1}^n\) be a \(K\)-basis of \(L\) contained in \(\mathcal{O}_K\). Then \(a \supset \alpha \mathcal{O}_L \supset \bigoplus_{i=1}^n \mathcal{O}_K (\alpha \omega_i)\). Then by the Lemma \(a^* \subset \bigoplus_{i=1}^n \mathcal{O}_K \alpha^{-1} \omega_i^*\). 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 \((m \alpha) a^* \subset \mathcal{O}_L\) so \(a^*\) is indeed a fractional ideal.

3.2. The different (2 hours, 8/3 + 11/3)

**Definition 142.** The complementary module (or inverse relative different) of \(L/K\) is the fractional ideal \(\mathcal{C}_{L/K} \overset{\text{def}}{=} \mathcal{O}_L^\prime\). The relative different of the extension is then the ideal \(\mathcal{D}_{L/K} \overset{\text{def}}{=} \mathcal{C}_{L/K}^{-1}\).

**Remark 143.** We saw in the proof of Corollary 141 that \(\mathcal{O}_L \subset \mathcal{C}_{L/K}\) so \(\mathcal{C}_{L/K}^{-1}\) is an ideal.

**Lemma 144 (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 \(\text{Tr}_K^M (\mathcal{C}_{L/K}^L \mathcal{C}_M/L \mathcal{O}_M) = \text{Tr}_K^L \text{Tr}_M^L (\mathcal{C}_{L/K}^L \mathcal{C}_M/L \mathcal{O}_M) = \text{Tr}_K^L (\mathcal{C}_{L/K}^L \mathcal{C}_M/L \mathcal{O}_M) \subset \text{Tr}_K^L (\mathcal{C}_{L/K}^L \mathcal{O}_L) \subset \mathcal{O}_K\) so \(\mathcal{C}_{L/K}^L \mathcal{C}_M/L \subset \mathcal{C}_{M/K}\).

Conversely, since \(\mathcal{O}_L \mathcal{O}_M = \mathcal{O}_M\), \(\text{Tr}_K^L (\mathcal{O}_L \text{Tr}_M^L (\mathcal{C}_M/K \mathcal{O}_M)) = \text{Tr}_K^M (\mathcal{C}_M/K \mathcal{O}_M) \subset \mathcal{O}_K\) so \(\text{Tr}_K^L (\mathcal{C}_M/K \mathcal{O}_M) \subset \mathcal{C}_{L/K}\). Thus \(\text{Tr}_L^M (\mathcal{C}_{L/K}^{-1} \mathcal{C}_M/K \mathcal{O}_M) \subset \mathcal{O}_L\) and hence \(\mathcal{C}_{L/K}^{-1} \mathcal{C}_M \subset \mathcal{C}_{M/L}\) 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 145.** 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 \(\alpha\). 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 \( \beta \) be a root of \( f \). Then \( g(\beta) = \begin{cases} \frac{f'(\beta)}{\beta - \alpha} & \beta = \alpha \\ 0 & \beta \neq \alpha \end{cases} \). Now let \( \{\alpha_i\}_{i=1}^{n} \) be the roots of \( f \) in a splitting field consider the polynomial

\[
h_{r}(X) = \sum_{i=1}^{n} \frac{f(X)}{X - \alpha_i} = \alpha_i.\]

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 \( h_{r}(X) = \text{Tr}_{K}^{L} \frac{f(X)}{X-\alpha} \alpha^r \) we see that \( \text{Tr}_{K}^{L} \frac{b_i}{f'(\alpha)} \alpha^r = \delta_{ir} \).

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 \( \alpha^i \in \text{Span}_{\mathcal{O}_K} \{b_j\}_{n-1-i \leq j \leq n-1} \). Since \( \alpha b_j = b_{j-1} - a_j b_{n-1} \) it follows that \( \alpha^{i+1} \in \text{Span}_{\mathcal{O}_K} \{b_j\}_{n-1-i \leq j \leq n-1} \) and we are done.

COROLLARY 146. Let \( L = K(\alpha) \) where \( \alpha \in \mathcal{O}_L \), and let \( f \in \mathcal{O}_K[x] \) be the minimal polynomial of \( \alpha \). Then \( \mathcal{O}_{L/K} \) divides \( f'(\alpha) \mathcal{O}_L \).

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

\[
\mathcal{O}_{L/K} \supset f'(\alpha) \mathcal{O}_L \text{ as claimed.} \]

FACT 147. \( \mathcal{O}_{L/K} \) is the GCD of all the ideals \( f' (\alpha) \) where \( \alpha \) ranges over all integral generators of \( L \).

COROLLARY 148. Let \( L/K \) be an unramified extension of local fields. Then \( \mathcal{O}_{L/K} = (1) \).

PROOF. Let \( \alpha \in \mathcal{O}_L \) be such that \( \lambda = \kappa(\alpha) \), 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 \( f'(\alpha) \in \mathcal{O}_L^* \).

### 3.2.2. Approximation Lemmas (skipped).

LEMMA 149. Let \( L \) be a number field, \( \mathfrak{P} \triangleleft \mathcal{O}_L \) a prime ideal, \( w \in |\mathfrak{P}| \) the corresponding place. Let \( \alpha \triangleleft \mathcal{O}_L \) be a non-zero fractional ideal and suppose that its order at \( \mathfrak{P} \) is \( e \). Then the closure of \( \alpha \) in \( L_w \) is exactly \( \mathfrak{P}_w^e \). Conversely, \( \mathfrak{P}_w^e \cap \mathcal{O}_L = \mathfrak{P}^e \).

PROOF. The closure of a \( \alpha \) in \( L_w \) is \( \mathcal{O} \)-invariant, hence \( \mathcal{O}_w \) invariant. Also, if \( \alpha \triangleleft \mathcal{O}_L \) then its closure is contained in \( \alpha \mathcal{O}_w \). It is therefore a fractional ideal. The claim is invariant under multiplication by elements of \( L^\times \), so we may assume \( \alpha \) is an ideal of \( \mathcal{O}_L \) prime to \( \mathfrak{P} \). But then its closure is an ideal of \( \mathcal{O}_w \) containing an element of \( \mathcal{O}_w^\times \) and hence all of \( \mathcal{O}_w \). The converse follows from the definition of the valuation. \( \square \)

DEFINITION 150. For a finite set \( S \subset |L| \) the set of \( S \)-integers is \( \mathcal{O}_L^S = \{x \in L \mid \forall w \in |L| \setminus S : |x|_w \leq 1\} \). Also set \( L_S = \prod_{w \in S} L_w \).

LEMMA 151. let \( S \) be as above. Then \( \mathcal{O}_L^S \) is dense in \( L_S = \prod_{w \in S} L_w \).
PROPOSITION 152. Let $K$ be a number field, and let $w$ be a finite place of $L$ corresponding to the prime ideal $\mathfrak{P} \triangleleft \mathcal{O}_L$ 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 $\mathcal{D}_{L_w/K_w}$.

PROOF. By Lemma [49] it is enough to show that the closure of $\mathcal{C}_{L/K}$ in $L_w$ (which is a fractional ideal) is $\mathcal{C}_{L_w/K_w}$. In one direction let $x \in \mathcal{C}_{L/K}$ and let $y \in \mathcal{O}_{L_w}$. By Lemma [151] there is $z \in \mathcal{O}_L$ such that $z$ is $w$-close to $y$ (see below) and $z$ is $w'$-close to 0 for all $w' \mid v$ other than $w$. Then $z$ is everywhere integral so $z \in \mathcal{O}_L$. We thus have $\text{Tr}_{K}^L(xz) \in \mathcal{O}_K \subset \mathcal{O}_{K_w}$. But

$$\text{Tr}_{K}^L(xz) = \text{Tr}_{K_w}^L(xz) + \sum_{w' \mid v, w' \neq v} \text{Tr}_{K_w}^L(xz).$$

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

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

3.2.3. The different and ramification.

PROPOSITION 153. 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 [148] we may assume that the extension is totally ramified, hence of the form $L_w = K_v([\Pi])$ where $\Pi$ satisfies an Eisenstein polynomial: $f(\Pi) = \Pi^e + \sum_{i=0}^{e-1} a_i \Pi^i = 0$ where $a_i \in \mathcal{O}_v$, $a_0$ a uniformizer of $K_v$. We first show that in this case $\mathcal{O}_{L_w} = \mathcal{O}_{K_v}[\Pi]$. Indeed, it is enough to show that $\mathcal{O}_{K_v} [\Pi]$ contains $\mathcal{O}_{L_w}^\times$. For this let $\alpha \in \mathcal{O}_{L_w}^\times$. Since $\mathcal{O}_{K_v}$ surjects on the residue field of $L_w$ (the extension is totally ramified), there is $c_1 \in \mathcal{O}_{K_v}^\times$ such that $w(\alpha - c_1) \geq 1$ where $w$ is the valuation, normalized such that $w(\Pi) = 1$. Then $\frac{\alpha - c_1}{\Pi^{w(\alpha - c_1)}} \in \mathcal{O}_{L_w}^\times$, so can be approximated by some $c_2 \in \mathcal{O}_{K_v}^\times$, at which point $\alpha$ is well-approximated by $c_1 + c_2 \Pi^{w(\alpha - c_1)}$. Continuing by induction we see that the compact subring $\mathcal{O}_{K_v}[\Pi]$ is dense in $\mathcal{O}_{L_w}$, hence equal to it.

Now by Proposition [145] we have $\mathcal{D}_{L_w/K_v} = (e \Pi^{e-1} + \sum_{i=1}^{e-1} ia_i \Pi^{i-1}) \mathcal{O}_{L_w}$. Since $\Pi^e | a_i$ we see see that $\mathcal{D}_{L_w/K} = (\Pi^{e-1})$ if $e$ is prime to $p$. If $p | e$ then $\Pi^e | \mathcal{D}_{L_w/K}$. □

We now summarize the discussion so far.

THEOREM 154. Let $L/K$ be a finite extension of number fields. For each prime $\mathfrak{P} \triangleleft \mathcal{O}_L$, say lying over $p \triangleleft \mathcal{O}_K$, we have $v_\mathfrak{P} \left( \mathcal{D}_{L/K} \right) \geq e (\mathfrak{P}/p) - 1$ with equality unless the extension is wildly ramified at $\mathfrak{P}$, at which point the inequality is strict. There are finitely many ramified primes.

PROOF. The first claim is the Proposition; the last claim follows from Corollary [146] □
3.3. The Discriminant (15/3/2013)

Returning to general separable $L/K$, for a $K$-basis $\Omega = \{\omega_i\}_{i=1}^n$ of $L$ let $\{\sigma_j\}_{i=1}^n = \text{Hom}_K(L, \bar{K})$, and set

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

Clearly this is independent of the ordering of the basis. If two bases $\Omega, \Omega'$ generate the same $\mathcal{O}_K$-module then the discriminants differ by the square of an element in $\mathcal{O}_K^\times$.

**Lemma 155.** Let $\Omega, \Omega'$ be two bases, and define matrices $A, B$ by $a_{ij} = \sigma_j \omega_i$, $b_{kj} = \sigma_j \omega'_k$. Then $(AB')_{ik} = \text{Tr}_K^L(\omega_i \omega'_k)$. In particular, taking $A = B$ we find

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

**Definition 156.** The discriminant of a fractional ideal in $L$ is the $\mathcal{O}_K$-module generated by the discriminants of bases contained in it. The relative discriminant of $L/K$ is the ideal $D_{L/K} = D_{L/K}(\mathcal{O}_L)$.

**Lemma 157.** The discriminant of a fractional ideal is a fractional ideal.

**Proof.** If $\Omega \subset \mathcal{O}_L$ then $\text{Tr}_K^L(\omega_i \omega_j) \in \mathcal{O}_K$. It follows that $D_{L/K}(a) \triangleleft \mathcal{O}_K$ for all $a \triangleleft \mathcal{O}L$. It remains to observe that $D_{L/K}(\beta a) = (N_{L/K}^L(\beta))^2 D_{L/K}(a)$. \hfill $\square$

**Theorem 158 (Different and discriminant).** $D_{L/K} = N_{L/K}^L D_{L/K}$.

**Proof.** Localizing and completing it is enough to consider the case where $L, K$ are complete wrt discrete valuations. Then $OK$ is a PID so

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

for a basis $\Omega$, and all bases are connected by a matrix in $\text{GL}_n(\mathcal{O}_K)$. It follows that $D_{L/K} = (D_{L/K}(\Omega))$ and that the complementary module $\mathcal{C}_{L/K}$ has the form $\bigoplus_{i=1}^n \mathcal{O}_K \omega_i^\ast$ for the dual basis $\Omega^\ast$. We now calculate the discriminant of $\mathcal{C}_{L/K}$ in two ways. First, by Lemma 155, $D_{L/K}(\Omega) D_{L/K}(\Omega^\ast) = 1$ (the relevant matrices are inverse!). Second, $\mathcal{C}_{L/K}$ is a principal fractional ideal, say of the form($\beta$). Then it also has the basis $\beta \Omega$, of discriminant $(N_{L/K}^L(\beta))^2 D_{L/K}(\Omega)$. It follows that

$$(N_{L/K}^L(\beta))^2 D_{L/K}(\Omega) = D_{L/K}(\Omega)^{-1}$$

and hence that $D_{L/K} = D_{L/K}(\Omega) = N_{L/K}^L(\beta)^{-1} = N_{L/K}^L(\beta^{-1})$

$\square$

**Corollary 159 (Properties).**

1. In a tower $M : L : K$, $D_{M/K} = D_{L/K}^{[M:L]} N_{L/K}^L D_{M/L}$.

2. $D_{L/K} = \prod_{w \in |L|} D_{L_w/K_w}$.

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

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 fewnomial explicit formulas can be written down. For example:

**Lemma 160.** Let $f(x) = x^n + b$. Then $D(f) = (-1)^{n(n-1)/2} n^n \cdot b^{n-1}$. 

33
PROOF. The roots are \((-b)^{1/n} \zeta_i\) so
\[
D(f) = \prod_{i<j} \left( (-b)^{1/n} \zeta_i - (-b)^{1/n} \zeta_j \right)^2
\]
\[
= (-b)^{n(n-1)} \left( -1 \right)^{\frac{n(n-1)}{2}} \prod_{i=0}^{n-1} \zeta_i \prod_{j=1}^{n} (1 - \zeta_j)
\]
\[
= (-b)^{n-1} \left( -1 \right)^{\frac{n(n-1)}{2}} \zeta_n \left( \frac{X^n - 1}{X - 1} \right)_{X=1}^n
\]
\[
= (-1)^{n-1} (-b)^{n-1} \left( -1 \right)^{\frac{n(n-1)}{2}} n^n.
\]
Indeed, \(\left( \frac{n(n-1)}{2} \right)^2 = 1\) and \(\zeta_n^{n(n-1)} = 1\) if \(n-1\) is even. \(\Box\)

**Remark 161.** But note that the only homogenous polynomial of degree \(n(n-1)\) in the roots is of the form \(c_n b^{n-1}\) so it remained to find \(c_n \in \mathbb{Z}\).

**Lemma 162.** Let \(f(x) = x^n + ax + b\). Then
\[
D(f) = (-1)^{\frac{n(n-1)}{2}} \left[ n^n b^{n-1} + (-1)^{n-1} (n-1) a^n \right].
\]

**Proof.** Where must be some universal \(c_{ij} \in \mathbb{Z}\) such that
\[
D(f) = \sum_{i(n-1) + jn = n(n-1)} c_{ij} a^i b^j.
\]
Now reducing mod \(n, n-1\) we see that \(n|i\) and that \((n-1)|j\). Since \(i, j \geq 0\) only two summands are possible, and
\[
D(f) = c_2 a^n + c_1 b^{n-1}.
\]
Setting \(a = 0\) we see that \(c_1 = (-1)^{\frac{n(n-1)}{2}} n^n\). Setting \(b = 0\) we have \(D(x^n + ax) = D(x^{n-1} + a) \prod_i (\alpha_i - 0)^2\) where \(\alpha_i\) are the roots of \(x^{n-1} + a\). But the product is \(a\) up to sign, so
\[
D(x^n + ax) = (-1)^{\frac{n-1}{2}} (n-1) a^{n-2} a^2
\]
\[
= (-1)^{\frac{n(n-1)}{2}} (n-1) a^n.
\]
It follows that \(c_2 = (-1)^{\frac{n-1}{2}} (n-1) a^n\) and the claim follows. \(\Box\)

**Corollary 163.** \(D(x^3 + ax + b) = -[4a^3 + 27b^2]\)

**Lemma 164.** Let \(f(x) = x^n + ax^2 + b\).

**Proof.** Need to classify \(i, j\) such that \(i(n-2) + jn = n(n-1)\). Reducing mod \(n-1\) we see \(i \equiv j(n-1)\). Reducing mod \(n\) we see \(2i \equiv 0(n)\). It follows that \(i \in \{0, \frac{n}{2}, n\} \cap \mathbb{Z}\), so \((i, j) \in \{(0, n-1), (\frac{n}{2}, \frac{n}{2}), (n, 1)\} \cap \mathbb{Z}^2\). Thus
\[
D(f) = c_1 b^{n-1} + c_2 (ab)^{n/2} + c_3 a^n b
\]
where \(c_1 = (-1)^{\frac{n(n-1)}{2}} n^n\) as before. \(\Box\)
3.4. Example: Cyclotomic fields

Let $\zeta_n$ 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 $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ 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 165. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = p^{r-1}(p - 1) = \phi(p^r)$, 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 $\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X - 1} = \sum_{j=0}^{p^r-1} X^{j(p^r - 1)}$. Then $\zeta_{p^r} - 1$ is a root of $\Phi_{p^r}(Y + 1)$ which is Eisenstein at $p$.

Approach 2: $1 - \frac{\zeta_k}{\zeta_{p^r}} = \sum_{j=0}^{k-1} \zeta_j^{p^r} \in \mathbb{Z}[\zeta_{p^r}]$. If $(p, k) = 1$ then $\zeta_{p^r}^k$ is also a primitive root of unity and therefore $1 - \frac{\zeta_k}{\zeta_{p^r}} \in \mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. It follows that these ratios are all units ("cyclotomic units") and hence that $1 - \zeta_k^r$ are all associate in $\mathbb{Z}[\zeta_{p^r}]$. In particular, $\pi^{\phi(p^r)} \sim \prod_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} (1 - \zeta_{p^r}^k) = \Phi_{p^r}(1) = p$. It follows that the ramification index of $(\pi)$ 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 $\pi$ over it.

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

□

LEMMA 166. 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 $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$. Multiplying by $\pi$ we see that $\pi\mathcal{O}_K = \pi\mathcal{O} + \pi^2\mathcal{O}_K$ so $\mathcal{O}_K = \mathcal{O} + \pi\mathcal{O} + \pi^2\mathcal{O}_K = \mathcal{O} + \pi\mathcal{O}_K$. Continuing by induction we see that $\mathcal{O}_K = \mathcal{O} + \pi^k\mathcal{O}_K$ for all $k$.

Approach 1: Since $D(\mathcal{O}_K)$ is a power of $p$, $[\mathcal{O}_K : \mathcal{O}]$ is a power of $p$. Therefore if we pass to the $\pi$-adic completion, this index will remain the same. But taking $k \to \infty$, shows that the $\pi$-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 $\pi$ up to a unit. Since $[\mathcal{O}_K : \mathcal{O}]$ is a power of $p$, for $k$ large enough we have $p^k\mathcal{O}_K \subset c\mathcal{O}$.

□

COROLLARY 167. The discriminant of $\mathbb{Q}(\zeta_n)$ is $\pm p^{r-1}(p-1)^r$.

PROOF. PS5

□

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 $K_i = \mathbb{Q}(\zeta_{p_1^{r_1}}, \ldots, \zeta_{p_i^{r_i}})$, $K_i = K_0 (0 = Q)$. Then for $1 \leq i \leq s$, $p_i$ is unramified in $K_{i-1}$, so the ramification index of $p$ in $K_i/K$ is the same as in $K_i/Q$ which is at least that of $\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$, 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 168. $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.
PROOF. Completing \( p \)-adically, it is enough to show that the ring of integers of \( \mathbb{Q}_p(\zeta_n) \) is \( \mathbb{Z}_p[\zeta_n] \) for all \( p \). If \( p \) does not divide \( n \) then the extension is unramified and the claim holds. Suppose now that \( p' \mid n \) and let \( n = p'm \). Then the ring of integers of \( \mathbb{Q}_p(\zeta_n) \) is \( \mathbb{Z}_p[\zeta_m] \), and we know that the extension \( \mathbb{Q}_p(\zeta_n) \) over this is totally ramified, with prime element \( \pi = \zeta_{p'} - 1 \). But then the ring of integers of \( \mathbb{Q}_p(\zeta_n) \) is \( \mathbb{Z}_p[\zeta_n][\zeta_{p'} - 1] = \mathbb{Z}_p[\zeta_n] \). \( \square \)

PROPOSITION 169. \(|D_K| = \left( \prod_{p \mid n} p^{\frac{rp-r-1}{p-1}} \right)^{\phi(n)} = n^{\frac{\phi(n)}{\phi(n)}} \prod_{p \mid n} p^{\frac{r-1}{p-1}} \). \( \square \)

PROOF. PS5

What about the sign?

LEMMA 170 (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 \( \{\sigma_j\}_{j=1}^n = \text{Hom}_\mathbb{Q}(K, \mathbb{C}) \). Then \( \tilde{A} \) is obtained by exchanging \( \sigma_j \) with \( \tilde{\sigma}_j \), which involves exchanging \( s \) columns. It follows that \( \det \tilde{A} = (-1)^s \det A \). It follows that \( D_K = (\det A)^2 = (-1)^s |\det A|^2 \). \( \square \)

3.5. Everywhere unramified extensions

LEMMA 171. 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 \( \sqrt{\Delta} = \prod_{i<j} (\alpha_i - \alpha_j) \in L \). \( \square \)

LEMMA 172. 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 173.** A lattice \( \Lambda \subset \mathbb{R}^n \) is discrete and cocompact subgroup, equivalently a free \( \mathbb{Z} \)-submodule generating by a basis.

**Lemma 174.** The two definitions are equivalent.

**Corollary 175.** (Of the proof of the Lemma) Let \( \Lambda = \oplus_i \mathbb{Z}v_i \). Then \( \mathcal{F} = \{ \sum_{i=1}^{n} a_i v_i \mid a_i \in [0, 1] \} \) is a bounded fundamental domain.

**Definition 176.** The covolume of \( \Lambda \) is \( \text{vol}(\mathcal{F}) = \det(\cdots v_i \cdots) = \sqrt{\det(\langle v_i, v_j \rangle)} \).

**Proposition 177.** \( \#\{ \mathbf{\lambda} \in \Lambda \cap B(0, R) \} \sim \frac{\text{vol}(\mathbb{R}^n/\Lambda)}{\text{vol}(\mathcal{F})} \).

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

**Corollary 178.** \( \text{vol}(\mathcal{F}) \) is independent of the choice of \( \mathcal{F} \), and will be denoted \( \text{vol}(\mathbb{R}^n/\Lambda) \) or \( \text{covol}(\Lambda) \).

**Theorem 179 (Minkowski).** Let \( \Lambda \subset \mathbb{R}^n \) be a lattice (discrete and cocompact subgroup, equivalently a free \( \mathbb{Z} \)-submodule generating by a basis). Let \( X \subset \mathbb{R}^n \) be convex, bounded and symmetric about the origin. Suppose that \( \text{vol}(X) \geq 2^n \text{vol}(\mathbb{R}^n/\Lambda) \). Then there is \( 0 \neq \mathbf{\lambda} \in X \cap \Lambda \).

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

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

Since the union on the left is disjoint, we have

\[
\#\{ \mathbf{\lambda} \in \Lambda \cap B(0, R) \} \frac{\text{vol}(X)}{2^n} \leq \text{vol}(B_{\mathbb{R}^n}(R + r)).
\]

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

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

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

### 4.2. Discriminant bounds

**Lemma 180.** For a number field \( K \) the image of \( \mathcal{O}_K \) in \( K_\infty \) is a lattice of covolume \( 2^{-s} \sqrt{|D_K|} \).

**Proof.** Let \( T \subset \text{Hom}_\mathbb{Q}(K, \mathbb{C}) \) be a set of representatives for the infinite places of \( K \), say \( T = T_R \cup T_C \), and let \( \iota : K \rightarrow K_\infty = \prod_{\tau \in T} K_\tau \) be the embedding. We have seen (Theorem 124) that \( \iota \) induces an isomorphism \( K \otimes \mathbb{Q}_v \rightarrow K_\infty \), and in particular \( \iota \) maps every \( \mathbb{Q}_v \)-basis of \( K \) to a \( \mathbb{R} \)-basis of \( K_\infty \). Since \( \mathcal{O}_K \) is the \( Z \)-span of an integral basis, it follows that its image is a lattice in \( K_\infty \). On \( K_\infty \) we take the inner product \( \langle (x_\tau), (y_\tau) \rangle = \sum_{\tau \in T} x_\tau \bar{y}_\tau \). 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 181.** 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 \( L(i) \) differs by a constant). Thus we are counting totally complex \( L \). Fix an infinite place \( v_0 \) and let

\[
X = \left\{ (x_v) \in L_\infty \mid \mathfrak{S}x_{v_0} \leq C \sqrt{|D|}, |\Re x_{v_0}| < 1, |x_v| < 1 \text{ for } v \neq v_0 \right\}.
\]

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 \( 2^n 2^{-n/2} \sqrt{|D|} \geq 2^n \text{vol}(L_\infty/\mathcal{O}_L) \) and it follows that there is \( \alpha \in \mathcal{O}_L \cap X \). Then from \( N_{\mathbb{Q}(\mathbb{Q})}(\alpha) \geq 1 \) it follows that \( |\alpha|_{v_0} > 1 \). Hence \( \mathfrak{S} \alpha_{v_0} \neq 0 \) and all conjugates of \( \alpha \) are distinct, so \( L = \mathbb{Q}(\alpha) \). But this means that the coefficients of the min poly are bounded in terms of \( D, \alpha \).

**Theorem 182.** \( |d_K|^{1/2} \geq \frac{n^n}{n!} \left( \frac{\pi}{4} \right)^s \geq \frac{n^n}{n!} \left( \frac{\pi}{4} \right)^{n/2} \).

**Proof.** Let

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

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

\[
1 \leq |\mathcal{N}_{\mathbb{Q}}(\alpha)| = \prod_{v|\infty} |\alpha|_v \leq \frac{1}{n^n} \left( \sum_{v} |\alpha|_v \right)^n = \frac{t^n}{n^n}
\]

the bound follows.

**Corollary 183 (Hermite).** There are finitely many extensions of bounded discriminant.

**Corollary 184 (Minkowski).** \( \mathbb{Q} \) has no unramified extensions.

**Proof.** By Stirling’s formula, \( n! \leq \sqrt{2\pi n} \frac{n^n}{e^n} e^{1/12n} \), we have \( |d_K| \geq \frac{1}{2\pi n} \left( \frac{\pi^2}{4} \right)^n e^{-1/6n} \), 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 185. Let \( C_K = \frac{n!}{n^n} (\frac{4}{\pi})^s \). Then every ideal class contains a representative of norm at most \( C_K^{-1} |d_K|^{1/2} \).

PROOF. Let \( a \triangleleft \mathcal{O}_K \). Since \( Na = [\mathcal{O}_K : a] \), the image of \( a \) in \( K_{\infty} \) is a lattice of covolume \( Na2^{-s}|d_K|^{1/2} \). As in the proof of Theorem 182 there is non-zero \( \alpha \in a \) such \( \sum_{v_{\infty}} |\alpha|_v \leq t \) where \( t^n = n! (\frac{4}{\pi})^s Na \sqrt{|d_K|} \), and again we have

\[
|N^K_Q(\alpha)| \leq \frac{t^n}{n^n} = C_K Na |d_K|^{1/2}.
\]

Let \( b \) be the ideal such that \( (\alpha) = ab \). Then

\[
|N^K_Q(\alpha)| = N(\alpha) = NaNb
\]

so

\[
Nb \leq C_K |d_K|^{1/2}.
\]

Note that \( b \) is in the class of \( a^{-1} \). \( \square \)

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

\[
\mathcal{O}_K^\times \rightarrow \prod_{v_{\infty}} \mathbb{R}_{>0}^\times
\]

\[
\varepsilon \mapsto (||\varepsilon||_v)_{v_{\infty}}.
\]

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

\[
\log: \mathcal{O}_K^\times \rightarrow \mathbb{R}^{r+s}
\]

\[
\varepsilon \mapsto (\log ||\varepsilon||_v)_{v_{\infty}}.
\]

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 186. 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 \( \prod_{\sigma \in \text{Hom}_Q(K,\mathbb{C})} (x - \sigma(\alpha)) \), 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. \( \square \)

COROLLARY 187. The image of \( \log \) is isomorphic to \( \mathbb{Z}^t \) for some \( t \leq r + s - 1 \).

LEMMA 188 (Kronecker). Let \( \alpha \in \mathcal{O}_Q^\times \) 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 \( \beta \in \mathcal{O}_K \), \( f_\beta(x) = \prod_{\sigma \in \text{Hom}_Q(K,\mathbb{C})} (x - \sigma(\beta)) \in \mathbb{Z}[x] \). If., furthermore, \( |\sigma(\beta)| \leq 1 \) for all \( \sigma \) then the coefficients of \( f_\beta \) are \( O_n(1) \). It follows that there are only finitely many such \( \beta \). But \( \{\alpha^k\}_{k \geq 1} \) all have this property. By the pigeon-hole principle \( \alpha^k = \alpha^l \) for some \( k \neq l \) so \( \alpha \) is a root of unity. \( \square \)
COROLLARY 189. The kernel of log consists of the roots of unity.

It follows that \( \mathcal{O}_K^\times \simeq \mu_n \times \mathbb{Z}^l \).

THEOREM 190. \( \mathcal{O}_K^\times \simeq \mu_n \times \mathbb{Z}^{r+s-1} \).

EXAMPLE 191. Some cases

1. \( K = \mathbb{Q}, r = 1, s = 0, \mathbb{Z}^\times = \{ \pm 1 \} \).

2. \( K = \mathbb{Q}(-d), r = 0, s = 1, \mathcal{O}_K^\times \) 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. \( K = \mathbb{Q}(\sqrt{3}), r = 1, s = 1, \mathcal{O}_K^\times = \left\{ \pm \left( 1 - \sqrt{3} \right)^n \right\}_{n \in \mathbb{Z}} \).

LEMMA 192. For each \( v_0 | \infty \) there is \( \epsilon \in \mathcal{O}_K^\times \) such that \( |\epsilon|_v < 1 \) for all infinite \( v \neq v_0 \).

PROOF. Fix \( M > 2^{-s} \sqrt{d_K} \). Identifying \( K_\infty = \mathbb{R}^n \), consider the rectangle \( X_v = \left[ Me^{-(n-1)}, Me^{-(n-1)} \right] \times \left[ -\epsilon, \epsilon \right]^{n-1} \) of volume \( 2^n M \). For all \( \epsilon \) we have \( X_v \cap \mathcal{O}_K \neq \{ 0 \} \). The norm of \( \alpha \in X_v \cap \mathcal{O}_K \) is a rational integer, bounded in terms of \( M \). In particular, there are at most finitely many norms occurring. There are finitely many ideals of a given norm, so the set of ideals \( (\alpha) \) occurring is finite. In particular, there is an infinite sequence \( \alpha_i \) such that \( \alpha_i \in X_{\epsilon_i} \) with \( \epsilon_i \to 0 \) and \( (\alpha_i) \) 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. \( \square \)

LEMMA 193. Let \( X = (x_{ij}) \in M_n(\mathbb{R}) \) be a matrix with \( x_{ij} < 0 \) for \( i \neq j, x_{ii} > 0 \). Suppose that \( X \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = 0 \). Then \( \text{rk} X \geq n - 1 \).

PROOF. Suppose the first \( r = n - 1 \) columns are dependent, say \( \sum_{j=1}^r c_j x_{ij} = 0 \) 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 \( x_{11} = -\sum_{j=2}^n x_{1,j} \geq -\sum_{j=2}^r c_j x_{1,j} \). Multiplying by \( c_1 \) we find \( c_1 x_{11} \geq -\sum_{j=2}^r c_1 x_{1,j} \geq -\sum_{j=2}^r c_j x_{1,j} \), with strict inequality unless the \( c_j \) are all equal. So unless the \( c_j \) are all equal we have

\[ \sum_{j=1}^r c_j x_{1,j} > 0, \]

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

\[ \sum_{j=1}^r c_j x_{n,j} > 0, \]

a contradiction. \( \square \)

DEFINITION 194. The regulator of \( K \), denoted \( R_K \), is the covolume of \( \mathcal{O}_K^\times \) in the hyperplane \( \mathbb{R}^{r+s-1} \). Equivalently,

\[ R_K = |\det (\log |\mu_i|_v)| \]
where $\nu$ 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. Dirichlet Series

5.1.1. Definition. 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 195. \( D(s) \) 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.

5.1.2. Application: Counting.

5.1.2.1. 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 discontinuous, 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 \( [0,1 \pm h] \) with \( h \) an appropriate power of \( X \) (to optimize the error term). In many cases one can do better by dyadic counting: letting \( \varphi \) approximate the characteristic function of \( [1,2] \) and then summing dyadically.

5.1.2.2. The Mellin transform.

Definition 196. The Mellin transform of a function \( \varphi \) defined on \((0, \infty)\) is \( \tilde{\varphi}(s) = \int_0^{\infty} \varphi(x)x^s \frac{dx}{x} \).

Remark 197. Under the isom \( \exp: \mathbb{R}^+ \to \mathbb{R}_{>0}^* \) this is the usual Fourier transform.

Lemma 198. 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 holomorphic in some right half-plane.

Fact 199. Let \( \varphi \) be reasonable. Then for \( \sigma \) large enough (for proof see later discussion of Fourier inversion),

\[
\varphi(x) = \frac{1}{2\pi i} \int_{(\sigma)} \tilde{\varphi}(s)x^{-s} \frac{ds}{s}.
\]

5.1.2.3. 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)
\[ \sum_{n \geq 1} a_n \phi \left( \frac{n}{X} \right) = \frac{1}{2\pi i} \sum_{n \geq 1} a_n \int_{(\sigma)} \left( \frac{n}{X} \right)^{-s} \tilde{\phi}(s) \frac{ds}{s} = \frac{1}{2\pi i} \int_{(\sigma)} D(s) \tilde{\phi}(s) X^s \frac{ds}{s}. \]

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 \( \sigma \) is large enough so that \( D(s) \) converges absolutely and \( \tilde{\phi}(s) \) decays by the smoothness of \( \phi \). Now suppose that \( \tilde{\phi}(s) \) and \( D(s) \) continue meromorphically to the left. We can then shift the contour, gaining since the term \( X^s \) (with constant absolute value \( X^{\sigma} \)) will become smaller. We can do this as long as \( D(s) \) is bounded in vertical strips. When we do this we will pick up contribution from poles. The conclusion is:

\[ \sum_{n \geq 1} a_n \phi \left( \frac{n}{X} \right) = \sum_{\sigma' < \Re \rho < \sigma} X^\rho \text{Res}_{s=\rho} \left( D(s) \tilde{\phi}(s) \frac{1}{s} \right) + \frac{1}{2\pi i} \int_{(\sigma')} D(s) \tilde{\phi}(s) X^s \frac{ds}{s}. \]

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

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

Here we have ignored the possibility that \( D(s) \) might have a pole at \( s = 0 \), but in any case since a contribution from a possible pole at \( s = 0 \) is constant (independent of \( X \)) while in most cases the sums grow with \( X \), issues at \( s = 0 \) can be ignored.

5.1.2.4. 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

\[ \sum_{n \geq 1} \phi \left( \frac{n}{X} \right) = \phi(1) - \phi(0)\zeta(0) + \text{small}. \]

Note that \( \tilde{\phi}(1) = \int_0^\infty \phi(x) \, dx \), as expected.

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

Then

\[ \frac{I_4 + \chi_4}{2}(n) = \begin{cases} 1 & n \equiv 1 \pmod{4} \\ 0 & \text{otherwise} \end{cases} \]

\[ \frac{I_4 - \chi_4}{2}(n) = \begin{cases} 1 & n \equiv -1 \pmod{4} \\ 0 & \text{otherwise} \end{cases} \]

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

\[ \sum_{\text{even } n \geq 1} n^{-s} = \sum_{m \geq 1} \frac{1}{2} (2m)^{-s} = 2^{-s} \zeta(s) \]
so that
\[ \sum_{n=1}^{\infty} I_4(n) n^{-s} = (1 - 2^{-s}) \zeta(s). \]

It follows that the counts we want can be done using the Dirichlet series
\[ D(s) = \frac{1}{2} \left( (1 - 2^{-s}) \zeta(s) \pm L(s; \chi_4) \right) \]
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
\[ \sum_{n \equiv \pm 1 (4)} \phi \left( \frac{n}{X} \right) = \frac{1}{2} \left( \frac{1}{2} \phi(1)X \pm \phi(0)L(0; \chi_4) \right) + \text{small} \]
(note that \( 1 - 2^{-0} = 0 \)). In other words, about a quarter of all integers are in the relevant residue class.

**5.1.3. Counting primes: Riemann’s Zeta function and Dirichlet’s L-function.**

**5.1.3.1. In the region of absolute convergence.** Note that \( \zeta(s) = \sum_{n=1}^{\infty} n^{-s} \) converges absolutely for \( \Re(s) > 1 \). In that region,
\[
\prod_{p \leq x} (1 - p^{-s})^{-1} = \prod_{p \leq x} \left( \sum_{k_p=1}^{\infty} p^{-sk} \right) = \sum_{k_1=1}^{\infty} \cdots \sum_{k_{\pi(x)}=1}^{\infty} \left[ \prod_{i=1}^{\pi(x)} p_i^{k_i} \right]^{-s} = \sum_n n^{-s}
\]
where the last sum is over those integers \( n \) only divisible by primes \( p \leq x \). Note that the equalities are all justified by absolute convergence, and that the claim is equivalent to the fundamental theorem of arithmetic (unique factorization in \( \mathbb{Z} \)). In particular,
\[
\zeta(s) - \prod_{p \leq x} (1 - p^{-s})^{-1} = \sum_m m^{-s}
\]
the sum now extending over those \( m \) having a prime factor larger than \( x \). In particular, it follows that
\[
\left| \zeta(s) - \prod_{p \leq x} (1 - p^{-s})^{-1} \right| \leq \sum_{m > x} m^{-\sigma} \xrightarrow{x \to \infty} 0
\]
since the last sum is a tail of the convergent series for \( \zeta(\sigma) \).

**Lemma 200 (Euler Product).** We have shown that for \( \Re(s) > 1 \),
\[
\zeta(s) = \prod_p (1 - p^{-s})^{-1},
\]
the product extending over all prime numbers.

**Remark 201.** In fact, the product converges absolutely in \( \Re(s) > 1 \) since \( \sum_p p^{-s} \) converges absolutely there. In particular, it follows that \( \zeta(s) \neq 0 \) if \( \Re(s) > 1 \).
**Corollary 202 (Euler).** *There are infinitely many primes.*

**Proof.** By the monotone convergence theorem, \( \lim_{\sigma \to 1} \zeta(\sigma) = \sum_{n=1}^{\infty} n^{-1} = \infty \). But \((1 - p^{-s})^{-1}\) is perfectly regular at \( s = 1 \) (its poles are on the imaginary axis) so a finite product of such would be bounded in a neighbourhood of \( s = 1 \). \( \square \)

**Remark 203.** This was the first genuinely new proof of the result since Greek times, and ought to be considered the birth of analytic number theory.

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

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

### 5.1.3.2. Counting primes.

In the region of absolute convergence we have

\[
\log \zeta(s) = -\sum_p \log \left(1 - p^{-s}\right).
\]

Differentiating, we see:

\[
-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p \cdot p^{-s}}{1 - p^{-s}} = \sum_p \log p \sum_{k=1}^{\infty} p^{-ks} = \sum_{n=1}^{\infty} \Lambda(n)n^{-s}
\]

where \( \Lambda(n) = \begin{cases} 
\log p & n = p^k, k \geq 1 \\
0 & \text{otherwise}
\end{cases} \) is the von-Mangoldt function. Then

\[
\sum_{n=1}^{\infty} \Lambda(n) \phi \left( \frac{n}{X} \right)
\]

counts primes. Similarly,

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

so that

\[
\sum_{n=1}^{\infty} \Lambda(n) \phi \left( \frac{n}{X} \right) = \sum_{\rho} \text{Res}_{s=\rho} \left[ -\frac{\zeta'(s)}{\zeta(s)} \frac{\Phi(\rho)}{\rho} X^\rho - \frac{\zeta'(0)}{\zeta(0)} \Phi(0) \right]
\]

and

\[
\sum_{n \equiv \pm 1 \pmod{4}} \Lambda(n) \phi \left( \frac{n}{X} \right) = \frac{1}{2} \left[ \sum_{\rho} \text{Res}_{s=\rho} \left[ -\frac{\zeta'(s)}{\zeta(s)} \frac{\Phi(\rho)}{\rho} X^\rho - \frac{\zeta'(0)}{\zeta(0)} \Phi(0) \right] \right]
\]

\[
\pm \frac{1}{2} \left[ \sum_{\rho} \text{Res}_{s=\rho} \left[ -\frac{L'(s;\chi_4)}{L(s;\chi_4)} \frac{\Phi(\rho)}{\rho} X^\rho - \frac{L'(0;\chi_4)}{L(0;\chi_4)} \Phi(0) \right] \right].
\]

Finally, note that \( \frac{F'(s)}{F(s)} \sim \text{ord}_{s=\rho} F(s - \rho)^{-1} \) for all \( \rho \), that is the poles of the logarithmic derivative occur exactly at the zeroes and poles of the function. Since \( \zeta(s) \) has a pole at \( s = 1 \) we obtain the
explicit formulas
\[ \sum_{n=1}^{\infty} \Lambda(n) \varphi \left( \frac{n}{X} \right) = \hat{\Phi}(1)X - \sum_{\rho \neq 0} \frac{\hat{\varphi}(\rho)}{\rho} X^\rho - \frac{\zeta'(0)}{\zeta(0)} \hat{\Phi}(0) \]
and
\[ \sum_{n=\pm 1, 4} \Lambda(n) \varphi \left( \frac{n}{X} \right) = \frac{1}{2} \hat{\Phi}(1)X - \frac{1}{2} \sum_{\rho} \frac{\hat{\varphi}(\rho)}{\rho} X^\rho + \frac{1}{2} \sum_{\rho(x) = 4} \frac{\hat{\varphi}(\rho)}{\rho} X^\rho - \frac{1}{2} \frac{\zeta'(0)}{\zeta(0)} \hat{\Phi}(0) \mp \frac{1}{2} L'(0; \chi) \hat{\Phi}(0). \]

By estimating the terms involving the roots (using the decay of \( \hat{\varphi} \)) it is possible to deduce

**Theorem 204** (PNT; de la Vallée-Poussin, Hadamard). \( \sum_{n=1}^{\infty} \Lambda(n) \varphi \left( \frac{n}{X} \right) \sim \hat{\Phi}(1)X. \)

**Theorem 205** (PNT in AP; de la Vallée-Poussin, Hadamard). If \((a, q) = 1\) then \( \sum_{n\equiv a(q)} \Lambda(n) \varphi \left( \frac{n}{X} \right) \sim \frac{1}{\varphi(q)} \hat{\Phi}(1)X. \)

### 5.2. The Riemann zetafunction

#### 5.2.1. Convergence; the Euler product; infinitude of primes.

For \( \Re s > 1 \) set
\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \]

**Proposition 206** (Euler Product). We have \( \zeta(s) = \prod_p (1 - p^{-s})^{-1}. \)

**Proof.** Fix \( \sigma > 1. \) Now \( \sum_{k=0}^{\infty} p^{-ks} \leq \frac{1}{1-p^{-\sigma}} \) converges absolutely for \( \Re(s) \geq \sigma \) (dominated by \( \zeta(\sigma) \) there).

\[
\prod_{i=1}^{I} (1 - p_i^{-s})^{-1} = \sum_{(e_p)_{p \leq x}} \prod_{p \leq x} p^{-e_p s}
\]
\[
= \sum_{(e_p)_{p \leq x}} \left( \prod_{p \leq x} p^{e_p} \right)^{-s}
\]
\[
= \sum_{p|n=n \leq x} n^{-s}.
\]

It follows that
\[
\zeta(s) - \prod_{p \leq x} (1 - p^{-s}) = \sum_{n: \exists p > x: p|n} n^{-s}
\]
and hence that
\[
\left| \zeta(s) - \prod_{p \leq x} (1 - p^{-s}) \right| \leq \sum_{n \geq x} n^{-\sigma} \xrightarrow{x \to \infty} 0.
\]

**Corollary 207** (Euler). There are infinitely many primes.
PROOF. By the monotone convergence theorem, \( \lim_{\sigma \to 1^-} \zeta(\sigma) = \zeta(1) = \infty \) (the harmonic series diverges). On the other hand, each Euler factor \( (1 - p^{-s})^{-1} \) is regular as long as \( p^{-s} \neq 1 \), at least for \( \Re(s) > 0 \). In particular, any finite product \( \prod_{p \leq x} (1 - p^{-s})^{-1} \) is defined and continuous at \( s = 1 \). \( \square \)

5.2.2. Analytical continuation. For \( \phi(x) \in S(\mathbb{R}) \) and \( r > 0 \) set \( \phi(rz) \overset{\text{def}}{=} \sum_{n \neq 0} \phi(n) = (\sum_{x \in \mathbb{Z}} \phi(x)) - \phi(0) \). Now define the zeta-integral

\[
Z(\phi; s) = \int_0^\infty \phi(rz) r^s \frac{dr}{r}.
\]

**Remark 208.** Note that \( \Phi(r) \) is even, so we may consider this an integral on \( \mathbb{R}^+ / \mathbb{Z}^+ \).

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

**Proof.** Let \( N \) be even, and let \( C \) be such that \( \left| \phi(x) \right| \leq \frac{C}{1 + x^N} \) for all \( x \in \mathbb{R} \). Then

\[
\left| \sum_{n=1}^\infty \phi(n) \right| \leq \int_0^\infty \frac{C}{1 + (rx)^N} \, dx = \left( \int_0^\infty \frac{C}{1 + x^N} \, dx \right) r^{-N}.
\]

It follows that the sum converges absolutely for \( \left| r \right| \geq r_0 \) and that it decays faster than any polynomial. For \( r \) small break the sum up into \( |n| \leq r^{-1} \) and \( |n| > r^{-1} \). \( \square \)

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

**Proof.** We have \( \int_1^\infty |\phi(rz)| r^s \frac{dr}{r} \ll \int_0^1 r^{-1} r^\sigma \frac{dr}{r} = \sigma - 1 \), since \( \sigma - 2 > -1 \), and \( \int_1^\infty |\phi(rz)| r^s \frac{dr}{r} \ll \int_1^\infty r^{-N} r^\sigma \frac{dr}{r} = N - \sigma \) if \( N > \sigma \).

Now for \( \Re s > 1 \) we have:

\[
Z(\phi; s) = \int_0^\infty \phi(rz) r^s \frac{dr}{r} = \int_1^\infty \phi(rz) r^s \frac{dr}{r} + \int_0^1 \left[ \sum_{n \in \mathbb{Z}} \phi(n) \right] r^s \frac{dr}{r} - \phi(0) \int_0^1 r^s \frac{dr}{r}.
\]

The proof of the Proposition shows that \( \int_1^\infty \phi(rz) r^s \frac{dr}{r} \) defines an entire function. We have thus shown:
PROPOSITION 211. For all \( \phi \in S(\mathbb{R}) \), \( Z(\phi; s) \) extends to a meromorphic function with poles at most at \( s = 0, 1 \) and satisfies the functional equation

\[
Z(\phi; s) = Z(\phi; 1 - s).
\]

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

\[
Z(\phi; s) = 2 \int_0^\infty \left[ \sum_{n=1}^{\infty} \phi(rn) \right] r^s \frac{dr}{r} = 2 \sum_{n=1}^{\infty} \int_0^\infty \phi(rn) r^s \frac{dr}{r} = 2 \left( \int_0^\infty \phi(r) r^s \frac{dr}{r} \right) \left[ \sum_{n=1}^{\infty} n^{-s} \right].
\]

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

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

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

Next, make the specific choice \( \phi(x) = e^{-\pi x^2} \). In this case

\[
2 \int_0^\infty \phi(r) r^s \frac{dr}{r} = 2 \int_0^\infty e^{-\pi r^2} r^s \frac{dr}{r} = \int_0^\infty e^{-\left( \frac{t}{\pi} \right)^{s-1} \pi^{-\frac{1}{2}} \frac{dt}{\sqrt{t}}} = \pi^{\frac{s-1}{2}} \Gamma\left( \frac{s}{2} \right).
\]

Writing \( \xi(s) = Z(e^{-\pi x^2}; s) = \pi^{\frac{s-1}{2}} \Gamma\left( \frac{s}{2} \right) \zeta(s) \) we find that \( \xi(s) \) extends to an entire function with poles at \( s = 0, 1 \) where the residues are \( -1, 1 \) respectively. Since \( \hat{\phi} = \phi \) we also obtain the functional equation

\[
\xi(s) = \xi(1 - s).
\]

Finally, since \( \Gamma_{\mathbb{R}}(s) = \pi^{\frac{s-1}{2}} \Gamma\left( \frac{s}{2} \right) \) is everywhere non-vanishing and has a simple pole at \( s = 0 \), \( \zeta(s) \) a pole at \( s = 1 \). From the formula above we see that \( Z(\phi; s) \) is bounded in vertical strips (away from the poles). By Stirling’s approximation, \( \Gamma\left( \frac{s}{2} \right) \) is bounded below on vertical strips (it grows exponentially as \( \Re(s) \to \infty \)), and it follows that \( \zeta(s) \) is bounded in vertical strips.

5.3. The Dedekind Zetafunction
Bibliography