These are notes for the graduate course Math 6723: Algebraic Number Theory taught by Dr. David Wright at the Oklahoma State University (Fall 2014). The notes are taken by Pan Yan (pyan@okstate.edu), who is responsible for any mistakes. If you notice any mistakes or have any comments, please let me know.

Contents

1 Introduction I (08/18) 4
2 Introduction II (08/20) 5
3 Introduction III (08/22) 6
4 Introduction IV (08/25) 7
5 Group Rings, Field Algebras, Tensor Products (08/27) 9
6 More on Tensor Products, Polynomials (08/29) 11
7 Discriminant, Separable Extensions (09/03) 12
8 Trace and Norm, Commutative $F$-algebras (09/05) 13
9 Idempotent and Radical (09/08) 16
10 Integrality (09/10) 17
11 Noetherian Rings and Modules (09/12) 18
12 Dedekind Domains I (09/15) 19
13 Dedekind Domains II (09/17) 21
14 Dedekind Domains III (09/19) 23
15 Chinese Remainder Theorem for Rings (09/22) 23
16 Valuation (09/24) 24
17 Ideal Class Group in a Dedekind Domain (09/26) 25
18 Extensions of Dedekind Domain I (09/29) 26
19 Extensions of Dedekind Domain II (10/01) 28
20 Extensions of Dedekind Domain III (10/03) 29
21 Valuation Theory I (10/06) 31
22 Valuation Theory II (10/08) 32
23 Valuation Theory III (10/10) 34
24 Valuations of a Function Field (10/13) 34
25 Ostrowski’s Theorem I (10/15) 36
26 Ostrowski’s Theorem II (10/17) 37
27 Weak Approximation Theorem (10/20) 39
28 Completions of Valued Fields I (10/22) 41
29 Completions of Valued Fields II, Inverse Limits (10/27) 43
30 Compactness (10/29) 45
31 Hensel’s Lemma (10/31) 47
32 Teichmüller Units (11/03) 49
33 Adeles and Ideles I (11/05) 50
34 Adeles and Ideles II (11/07) 51
35 Module Theory over Dedekind Domain (11/10) 52
36 Extensions I (11/12) 53
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>37 Extensions II (11/14)</td>
<td>54</td>
</tr>
<tr>
<td>38 Correspondence Between Prime Ideals and Absolute Values (11/17)</td>
<td>56</td>
</tr>
<tr>
<td>39 Galois Extensions I (11/19)</td>
<td>57</td>
</tr>
<tr>
<td>40 Galois Extensions II (11/21)</td>
<td>58</td>
</tr>
<tr>
<td>41 Galois Extensions III (11/24)</td>
<td>59</td>
</tr>
<tr>
<td>42 Finiteness of the Class Group I (12/01)</td>
<td>61</td>
</tr>
<tr>
<td>43 Finiteness of the Class Group II (12/03)</td>
<td>64</td>
</tr>
<tr>
<td>44 Dirichlet’s Unit Theorem (12/05)</td>
<td>66</td>
</tr>
</tbody>
</table>
1 Introduction I (08/18)

\( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) denote natural numbers, integers, rational numbers, real numbers and complex numbers respectively.

For two sets \( A, B \), \( A \subset B \) means \( A \) is a subset of \( B \), and \( A \subsetneq B \) means \( A \) is a proper subset of \( B \).

We assume every ring \( R \) is commutative with a 1, unless otherwise indicated.

\( \mathbb{S} \subset R \) is a subring if: 1) \( \mathbb{S} \) is closed under multiplication and addition; 2) \( \mathbb{S}, R \) have the same multiplicative identity. \( R^* = R^\times \) = group of unity of \( R \). \( x \in R \) is a unit if \( \exists y \) such that \( xy = 1 \).

A subset of a ring \( I \subset R \) is an ideal if: 1) it is closed under addition and scalar multiplication by \( R \); 2) \( I \) contains 0.

Let \( A, B, C \) be \( R \)-modules, a sequence of \( R \)-module homomorphism

\[
A \xrightarrow{f} B \xrightarrow{g} C
\]

is exact if \( \text{im} f = \ker f \). The diagram

\[
\begin{array}{ccc}
B & \xrightarrow{g} & C \\
\downarrow f & & \downarrow \\
A & \xrightarrow{h} & C
\end{array}
\]

commutes if \( h = g \circ f \).

For two groups \( H \subset G \), the index \( [G : H] \) is the number of cosets in \( G/H \). For two fields \( K \subset L \), \( (L : K) \) is the degree of \( L/K \), which is the dimension of \( L \) as a \( K \)-vector space.

\( \mathbb{Z}[x] \) is the ring of polynomials in one indeterminate \( x \) with coefficients in \( \mathbb{Z} \), i.e., \( \mathbb{Z}[x] = \{ p(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n : c_0, c_1, \ldots, c_n \in \mathbb{Z} \} \). (\( \mathbb{Z} \) can be replaced by any ring \( R \).)

**Definition 1.1.** A complex number \( z \in \mathbb{C} \) is an algebraic number if there exists a polynomial \( p(x) \in \mathbb{Z}[x], p(x) \neq 0 \), such that \( p(z) = 0 \). An algebraic integer is an algebraic number \( z \) such that there is a monic polynomial \( p(z) \in \mathbb{Z}[x] \) with \( p(z) = 0 \).

**Remark 1.2.** A complex number is transcendental if it is not algebraic, for example, \( e, \pi \). \( e^\pi \) are transcendental, which follows from the Gelfond-Schneider theorem (which states that if \( a \) and \( b \) are algebraic numbers with \( a \neq 0, 1 \) and \( b \) is not a rational number, then \( a^b \) is transcendental) since \( e^\pi = (-1)^i \).

The structure of algebraic integers allows one to prove things about ordinary integers.

**Theorem 1.3** (Fermat’s Two Square Theorem (Lagrange)). An odd prime \( p = x^2 + y^2 \) for \( x, y \in \mathbb{Z} \) iff \( p \equiv 1 \pmod{4} \).
Proof. \((\Rightarrow)\) Assume \(p = x^2 + y^2, \ x, y \in \mathbb{Z}\). Notice that \(x^2 \equiv 0 \) or \(1 \pmod{4}\), hence \(p = x^2 + y^2 \equiv 0 \) or \(1 \pmod{4}\). But \(p\) is an odd prime, hence \(p \equiv 1 \pmod{4}\).

\((\Leftarrow)\) Assume \(p \equiv 1 \pmod{4}\). \(\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\) is a finite field of \(p\) elements, and \(\mathbb{F}_p^\times\) is a cyclic group of order \(p - 1 \equiv 0 \pmod{4}\). So \(\mathbb{F}_p^\times\) has an element of order 4. That is to say, there exists an integer \(m \in \mathbb{Z}/p\mathbb{Z}\) such that \(m^4 \equiv 1 \pmod{p}\), and \(m^2 \not\equiv 1 \pmod{p}\). Hence \(m^2 \equiv -1 \pmod{p}\). Then \(p|m^2 + 1 = (m + i)(m - i)\) in \(\mathbb{Z}[i]\). Notice that \(\mathbb{Z}[i]\) is an Euclidean domain with norm \(N(x + iy) = x^2 + y^2\). If \(p\) is a prime in \(\mathbb{Z}[i]\), then \(p|m + i\) or \(p|m - i\). If \(p|m + i\) or \(p|m - i\), then \(p\) divides both (suppose \(m + i = p(x + iy)\), then \(m - i = p(x - iy)\). The reverse is also true). Then \(p|(m + i) - (m - i) = 2i\). But \(p\) is an odd prime, so \(p > 3\), hence \(N(p) \geq 9\) while \(N(2i) = 2\). This is a contradiction. So \(p\) is not prime in \(\mathbb{Z}[i]\), hence \(p = (x + iy)(x' + iy')\) where \(x + iy, x' + iy'\) are not units. Then \(N(p) = p^2 = (x^2 + y^2)(x'^2 + y'^2)\), hence \(p = x^2 + y^2 = x'^2 + y'^2\). \(\square\)

There are more examples, such as primes of \(p = x^2 - 2y^2, \ p = x^2 + 6y^2\).

2 Introduction II (08/20)

**Theorem 2.1.** An odd prime \(p = x^2 - 2y^2\) for \(x, y \in \mathbb{Z}\) if and only if \(p \equiv \pm 1 \pmod{8}\).

To prove this theorem, we first recall the Law of Quadratic Reciprocity.

**Theorem 2.2** (Law of Quadratic Reciprocity). For odd prime \(p\),

\[
\left(\frac{a}{p}\right) = \begin{cases} 
0, & \text{if } p|a \\
1, & \text{if } a \equiv m^2 \pmod{p} \\
-1, & \text{if } a \not\equiv m^2 \pmod{p}
\end{cases}
\]

is the Legendre symbol. Then

\[
\left(\frac{-1}{p}\right) = \begin{cases} 
1, & \text{if } p \equiv 1 \pmod{4} \\
-1, & \text{if } p \equiv 3 \pmod{4}
\end{cases}
\]

\[
\left(\frac{2}{p}\right) = \begin{cases} 
1, & \text{if } p \equiv \pm 1 \pmod{8} \\
-1, & \text{if } p \equiv \pm 3 \pmod{8}
\end{cases}
\]

If \(p, q\) are odd primes, then

\[
\left(\frac{p}{q}\right) = \begin{cases} 
\left(\frac{q}{p}\right), & \text{if } p \text{ or } q \equiv 1 \pmod{4} \\
-\left(\frac{q}{p}\right), & \text{if } p \equiv q \equiv 3 \pmod{4}
\end{cases}
\]

Now we prove Theorem 2.1.
Proof. ($\Rightarrow$) Suppose $p = x^2 - 2y^2$ for $x, y \in \mathbb{Z}$ is an odd prime. For $x \in \mathbb{Z}$, $x^2 \equiv 0, 1, 4 \pmod{8}$. Since $p$ is odd, $x^2 \equiv 1 \pmod{8}$. Hence, $p = x^2 - 2y^2 \equiv 1 - 2 \cdot \{0, 1, 4\} \pmod{8} \equiv 1, -1 \pmod{8}$.

($\Leftarrow$) Suppose $p \equiv \pm 1 \pmod{8}$. (In Fermat’s Two Square Theorem, when $p \equiv 1 \pmod{4}$, we first show there is an integer $m$ such that $m^2 \equiv -1 \pmod{p}$.) Here we have to show that there is an integer $m$ such that $m^2 \equiv 2 \pmod{p}$. This follows from the Law of Quadratic Reciprocity. Hence, $p|m^2 - 2 = (m - \sqrt{2})(m + \sqrt{2})$ in $\mathbb{Z}[\sqrt{2}]$. If $p$ is prime in $\mathbb{Z}[\sqrt{2}]$, then $p|m - \sqrt{2}$ or $p|m + \sqrt{2}$. By conjugation, then $p$ divides both $m - \sqrt{2}$ and $m + \sqrt{2}$. Then $p|(m + \sqrt{2}) - (m - \sqrt{2}) = 2\sqrt{2}$. Then $N(p) = p^2$ divides $N(2\sqrt{2}) = (2\sqrt{2}) \cdot (-2\sqrt{2}) = -8$. This contradiction proves that $p$ is not prime in $\mathbb{Z}[\sqrt{2}]$. $\mathbb{Z}[\sqrt{2}]$ is a UFD, so $p = (x + \sqrt{2}y)(x' + \sqrt{2}y')$ for some nonunits. By taking norm, we get $p^2 = (x^2 - 2y^2)(x'^2 - 2y'^2)$. Note that $x + \sqrt{2}y$ is a unit iff $x^2 - 2y^2 = \pm 1$. Since $x + \sqrt{2}y, x' + \sqrt{2}y'$ are nonunits, we have $x^2 - 2y^2 = p$ or $-p$. If $x^2 - 2y^2 = -p$, replace $x + \sqrt{2}y$ by $(x + \sqrt{2}y)(1 + \sqrt{2}) = (x + 2y) + (x + y)\sqrt{2}$, then we get $N((x + \sqrt{2}y)(1 + \sqrt{2})) = (x^2 - 2y^2) \cdot (1 - 2) = -(x^2 - 2y^2) = p$. \hfill \Box

Remark 2.3. $x^2 - 2y^2 = \pm 1$ is true if and only if $x + \sqrt{2}y = \pm (1 + \sqrt{2})^n$ for some $n \in \mathbb{Z}$.

3 Introduction III (08/22)

Next question: which primes are of the form $p = x^2 + 6y^2$?

Theorem 3.1. An odd prime $p = x^2 + 6y^2$ for $x, y \in \mathbb{Z}$ iff $p \equiv 1, 7 \pmod{24}$.

Proof. ($\Rightarrow$) If $p = x^2 + 6y^2$, then $x^2 \equiv -6y^2 \pmod{p}$, hence $-6 \equiv m^2 \pmod{p}$ since $x, y \neq 0 \pmod{p}$. Therefore, $(-6) = 1$ since $\left( \frac{6}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{3}{p} \right)$ (residue symbol is a homomorphism $(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$). The squares form a subgroup $H$ in $G = (\mathbb{Z}/p\mathbb{Z})^*$ of index 2. $G/H = \{H, xH\}$ where $x$ is any non-square, it has order 2), then we have $\left( \frac{x^2}{p} \right) = \left( \frac{x^2}{p} \right) \left( \frac{3}{p} \right)$.

We have

$$
\left( \frac{3}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{3} \\
-1 & \text{if } p \equiv 2 \pmod{3}.
\end{cases}
$$

(Reference for this formula: Hardy and Wright, Introduction to the Theory of Numbers).

Moreover, by Quadratic Reciprocity Law,

$$
\left( \frac{-1}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4} \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
$$
So \((\frac{3}{p}) = (\frac{-1}{p})(\frac{2}{p})\). So \((\frac{-6}{p}) = (\frac{-1}{p})(\frac{2}{p})(\frac{p}{3}) = (\frac{2}{p})(\frac{p}{3})\). Then

\[
(\frac{-6}{p}) = 1 \iff (\frac{2}{p}) = (\frac{p}{3}) = 1 \text{ or } (\frac{2}{p}) = (\frac{p}{3}) = -1
\]

\[
\iff p \equiv \pm 1 \pmod{8}, p \equiv 1 \pmod{3} \text{ or } p \equiv \pm 3 \pmod{8}, p \equiv 2 \pmod{3}
\]

The Chinese Remainder Theorem implies

\[
(\frac{-6}{p}) = 1 \iff p \equiv 1, 5, 7, 11 \pmod{24}.
\]

\((\Leftarrow)\) Conversely, if \(p \equiv 1, 5, 7, 11 \pmod{24}\), then \(\exists m\) such that \(m^2 \equiv -6 \pmod{p}\), so \(p|m^2 + 6 = (m + \sqrt{-6})(m - \sqrt{-6})\). Same proof as before shows that \(p\) is not a prime in \(\mathbb{Z}[\sqrt{-6}]\). \(\mathbb{Z}[\sqrt{-6}]\) is not a UFD. However, the ideals in \(\mathbb{Z}[\sqrt{-6}]\) have unique factorization as a product of prime ideals. Every \(p\) in \(\mathbb{Z}\) has a prime ideal factorization in \(\mathbb{Z}[\sqrt{-6}]\): \((p)\) is prime or \((p) = \mathfrak{p}\mathfrak{p}\). \((p) = \mathfrak{p}\mathfrak{p}\) happens for \(p \equiv 1, 5, 7, 11 \pmod{24}\). In addition, \(p = (x + y\sqrt{-6})\) is a principal ideal iff \(p \equiv 1, 7 \pmod{24}\).

More generally, for an algebraic number field \(K/\mathbb{Q}\), \(\mathcal{O}_K\) is the set of algebraic integers in \(K\). We say two ideals \(a, b \subset \mathcal{O}_K\) are equivalent if there exists \(\alpha, \beta \in \mathcal{O}_K\setminus\{0\}\) such that

\[
\alpha a = \beta b.
\]

Under multiplication \(ab\) of ideals, the equivalence classes form a group, called the class group of \(K\). \(a\) is principal iff \(a \sim (1) = \mathcal{O}_K\). The class group \(C_K\) is always a finitely generated abelian group, its size is the class number of \(K\), denoted as \(h_K\).

A big open question is that there exists infinitely many \(d\) such that \(\mathbb{Q}(\sqrt{d})\) has class number 1.

4 Introduction IV (08/25)

The Riemann zeta function is defined as

\[
\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}
\]

where \(s\) is a complex variable. It converges locally uniformly for \(\text{Re}(s) > 0\). It has a meromorphic continuation to the whole complex plane \(\mathbb{C}\) which is holomorphic except for a single pole at \(s = 1\) with residue \(\text{Res}_{s=1}\zeta(s) = 1\). If \(\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t} \, dt\), then

\[
\Lambda(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)
\]

satisfies the functional equation

\[
\Lambda(1 - s) = \Lambda(s).
\]
It has an Euler product expansion

\[ \zeta(s) = \prod_{\text{primes } p} (1 - \frac{1}{p^s})^{-1}. \]

By taking logarithms and a lot of work, we get a formula (Von Mangoldt’s Prime Power Counting Formula):

\[ \sum_{\text{primes } p, m \geq 1, p^m < x} (\log p) = x - \sum_{\zeta(\rho) = 0, 0 \leq \Re(\rho) \leq 1} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log(1 - x^{-2}) \]

for \( x > 0 \).

All the zeroes \( \rho \) of \( \zeta(s) \) are either

\[ \rho = -2, -4, -6, \ldots \]

or in the critical strip \( 0 \leq \Re(\rho) \leq 1 \). The Prime Number Theorem

\[ \pi(x) = \sum_{p < x} 1 \sim \text{li}(x) = \int_2^x \frac{dt}{\ln(t)} \]

was derived by proving all the nontrivial zeroes are in \( 0 < \Re(\rho) < 1 \). The Riemann Hypothesis is that all nontrivial zeroes have \( \Re(\rho) = \frac{1}{2} \). Riemann based this on detailed numerical calculations which were uncovered only after nearly a century after his paper appeared.

For a complex variable \( s \), the Dedekind zeta function is

\[ \zeta_K(s) = \prod_{\text{prime ideals } p \text{ in } \mathcal{O}_K} (1 - (Np)^{-s})^{-1} \]

where \( Np = [\mathcal{O}_K : p] \) is the absolute norm of ideal \( p \).

\( \zeta_K(s) \) is holomorphic at all \( s \) except for \( s = 1 \). Moreover,

\[ \lim_{s \to 1} (s - 1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_KR_K}{w_K|d_K|^\frac{1}{2}} \]

where \( r_1 \) is the number of real embeddings \( K \hookrightarrow \mathbb{R} \), \( r_2 \) is the number of conjugate pairs of embeddings \( K \hookrightarrow \mathbb{C} \) which are not real, \( d_K \) is the discriminant of \( K \) (measurement of size of \( \mathcal{O}_K \)), \( R_K \) is the regulator of \( K \) (measurement of size of unit group \( U_K = \mathcal{O}_K^* \)), \( w_K \) is the number of \( x \in K \) with \( x^n = 1 \) for some \( n \). This formula gives an effective numerical procedure for calculating \( h_K \), that is used in number theory software.
5 Group Rings, Field Algebras, Tensor Products (08/27)

**Definition 5.1.** Let $G$ be a group and $R$ a commutative ring with identity. The group ring $R[G]$ is the set of all formal finite sums $\sum_{g\in G} x_g g$ with each $x_g \in R$.

Define addition by
\[
\left(\sum x_g g\right) + \left(\sum y_g g\right) = \sum (x_g + y_g) g
\]
and multiplication by
\[
\left(\sum x_g g\right) \left(\sum y_g g\right) = \sum_{g\in G} \sum_{h\in G} x_g y_h (gh) = \sum_{g\in G} \left(\sum_{h\in G} x_{gh^{-1}} y_h\right) g.
\]

One can show that $R[G]$ is a ring.

**Example 5.2.** For the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ where $ij = k = -ji, i^2 = j^2 = -1$,
we have the group algebra $\mathbb{R}[Q_8]$ which is an 8-dimensional vector space over $\mathbb{R}$. It has a subgroup $\mathbb{H}$ of dimension 4, which is the kernel of the linear map
\[
\mathbb{R}[Q_8] \to \mathbb{R}[Q_8] \\
q \mapsto q + (-1)q
\]
where $-1 \in Q_8$. $\mathbb{H}$ is a 4-dimensional division algebra over $\mathbb{R}$ (Every $q \in \mathbb{H}, q \neq 0$ is a unit).

**Definition 5.3.** Let $F$ be a field. An algebra $A$ over a $F$ is a ring that contains $F$ in its center (So $za = az$ for all $a \in A, z \in F$).

A finite algebra over $F$ is a finite-dimensional vector space over $F$. A division algebra is one in which every nonzero element is a unit.

If $R = K$ is a field, $K[G]$ is an algebra where $K \hookrightarrow K[G]$ by $x \mapsto x \cdot 1$.

Suppose $K/F$ is a finite separable field extension, and suppose $L/F$ is any field extension. Then the tensor product $K \otimes_F L$ is an $L$-algebra.

**Theorem 5.4.** $K \otimes_F L$ has dimension $(K : F)$ over $L$. $K \otimes_F L$ is isomorphic to a direct sum $\bigoplus_{i=1}^{t} L_i$ where each $L_i$ is a field extension of $L$ and $(K : F) = \sum_{i=1}^{t} (L_i : L)$.

We need to review tensor product to prove the Theorem 5.4.
**Definition 5.5.** For a commutative ring $R$, the *tensor product* $M \otimes_R N$ of two $R$-modules $M, N$ is the unique $R$-module such that every $R$-bilinear map

$$M \times N \xrightarrow{\phi} P$$

$$(m, n) \mapsto \varphi(m, n)$$

($P$ is another $R$-module) factors through $M \otimes_R N$:

$$M \times N \xrightarrow{c} M \otimes_R N \xrightarrow{h} P$$

$$(m, n) \mapsto m \otimes n$$

such that $\varphi = h \circ c$ where $h$ is a linear map.

If $K/F$ is a finite separable field extension, then $K = F(\alpha)$ for a root $\alpha$ of an irreducible polynomial $f(x) \in F[x]$. Then $K = F(\alpha) \cong F[x]/(f(x)F[x])$.

**Proof of Theorem 5.4.** Suppose we have a bilinear map $\varphi : K \times L \to P$ where $L$ is a field extension of $F$. Define $g : K \times L \to L[x]/(f(x)L[x])$ by

$$g(p(x) + f(x)F[x], y) = yp(x) + f(x)L[x].$$

This is well-defined and bilinear. Then define $h : L[x]/(f(x)L[x]) \to P$ by

$$h(c_0 + c_1x + \cdots + c_m x^m + f(x)L[x]) = \varphi(1 + f(x)F[x], c_0) + \cdots + \varphi(x^m + f(x)F[x], c_m).$$

This is $F$-linear and $\varphi = h \circ g$. By uniqueness that proves

$$K \otimes_F L = L[x]/(f(x)L[x]).$$

$f(x)$ may factor in $L[x]$ as a product of distinct coprime irreducible factors $f(x) = \prod_{i=1}^t f_i(x)$ (since $f$ is separable). Chinese Remainder Theorem implies that

$$L[x]/(f(x)L[x]) \cong \oplus_{i=1}^t L[x]/(f_i(x)L[x]).$$

Since $f_i$ is irreducible, $L_i = L[x]/(f_i(x)L[x])$ is a field. Since $\sum \deg(f_i) = \deg(f)$, we have $(K : F) = \sum (L_i : L)$.

**Example 5.6.** For $d \in \mathbb{Z}$, $d$ is square-free, $\mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathbb{R} \cong \oplus_{i=1}^t L_i$ for extensions $L_i/\mathbb{R}$. These can be $\mathbb{R}$ or $\mathbb{C}$. Since $\sum (L_i : \mathbb{R}) = (\mathbb{Q}(\sqrt{d} : \mathbb{Q})) = 2$, these are two possibilities $\mathbb{R} \oplus \mathbb{R}$ or $\mathbb{C}$. The former happens iff $\sqrt{d} \in \mathbb{R}$. 

10
6 More on Tensor Products, Polynomials (08/29)

Remark 6.1. Here is another application of tensor products. Consider the following tensor product
\[ Z[\sqrt{d}] \otimes_{Z}(Z/7Z) \cong Z[\sqrt{d}]/7Z[\sqrt{d}]. \]
Even though \( Z/7Z \) is a field, this tensor product is not always a field. For example, for \( d = 2 \), \( Z[\sqrt{2}]/7Z[\sqrt{2}] \) has zero divisors
\[ (3 + \sqrt{2})(3 - \sqrt{2}) = 7 = 0. \]

\( F[x] \) is a \( F \)-vector space with basis \( \{1, x, x^2, \ldots\} \). We may define a unique linear map \( D : F[x] \to F[x] \) by \( D(x^n) = nx^{n-1} \). \( D \) is not a ring homomorphism since \( D(ab) \neq D(a)D(b) \).

Definition 6.2. A derivation on an algebra \( A \) over \( F \) is a linear map \( d : A \to A \) such that \( d(ab) = d(a)b + ad(b) \).

Remark 6.3. (i) The formal derivative \( D \) is a derivation. It suffices to check on basis elements:
\[ D(x^m) = D(x^m)x^n + x^mD(x^n). \]
If \( \text{char}(F) = 0 \), then \( D(f) = f' = 0 \) if and only if \( f \) is constant. If \( \text{char}(F) = p \), \( D(\sum a_n x^n) = \sum a_n nx^{n-1} = 0 \) if and only if \( p | n \) or \( a_n = 0 \) if and only if \( f(x) = \sum b_n x^n = g(x^p) \).

(ii) All the derivative of an algebra form a ring \( D \) (the theory of \( D \)-modules).

Since \( F[x] \) is Euclidean and thus a UFD, then the greatest common divisor \( \text{GCD}(f, g) = (f, g) \) is defined.

Theorem 6.4. The following statements are equivalent.
(i) \( f \) is separable.
(ii) \( f'(\alpha_j) \neq 0 \) for all roots \( \alpha_j \) of \( f \).
(iii) \( (f, f') = 1 \).

Proof. (i)\(\Rightarrow\)(ii) In a splitting field \( L/F \), \( f(x) = c(x - \alpha_1)\cdots(x - \alpha_n) \) for \( c \neq 0, \alpha_i \neq \alpha_j \) for \( i \neq j \), all \( c, \alpha \)'s are in \( L \). Then
\[ f'(x) = c \sum_{k=1}^{n} \prod_{i=1, i \neq k}^{n} (x - \alpha_i). \]
So \( f'(\alpha_j) = c \prod_{i \neq j} (\alpha_j - \alpha_i) \neq 0 \).

(ii)\(\Rightarrow\)(iii) If \( g = (f, f') \neq 1 \), then \( g(\alpha_j) = 0 \) for some root \( \alpha_j \) of \( f \). Since \( g|f' \), that implies \( f'(\alpha_j) = 0 \), contrary to (ii).

(iii)\(\Rightarrow\)(i) Suppose \( f \) is not separable. Then \( \alpha_i = \alpha_j \) for some \( i \neq j \). Then \( f = (x - \alpha_i)^2g(x) \) for some \( g(x) \). Then \( f'(x) = 2(x - \alpha_i)g(x) + (x - \alpha_i)^2g'(x) \) is divisible by \( x - \alpha_i \), so \( (f, f') \neq 1 \). \(\square\)
7  Discriminant, Separable Extensions (09/03)

Definition 7.1. Let \( f(x) = (x - \alpha_1^i) \cdots (x - \alpha_n^i) \) be an irreducible polynomial of \( \alpha \) over \( F \) and \( E = F(\alpha) \). Then the discriminant of \( f \) is defined as

\[
\text{Disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).
\]

Corollary 7.2. \( f \) is separable iff \( \text{Disc}(f) \neq 0 \).

Remark 7.3. The Vandermonde determinant of \( T_1, T_2, \cdots, T_n \) is

\[
V(T_1, \cdots, T_n) = \begin{vmatrix}
1 & T_1 & \cdots & T_1^{n-1} \\
1 & T_2 & \cdots & T_2^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & T_n & \cdots & T_n^{n-1}
\end{vmatrix} = \prod_{1 \leq i < j \leq n} (T_j - T_i).
\]

Hence, \( \text{Disc}(f) = V(\alpha_1^i, \cdots, \alpha_n^i)^2 \).

Definition 7.4. A field \( F \) is perfect if every irreducible polynomial \( f \in F[x] \) is separable.

Theorem 7.5. \( F \) is perfect if either (i) \( \text{char}(F) = 0 \) or (ii) \( \text{char}(F) = p \) and \( x \mapsto x^p \) is a field automorphism of \( F \).

Proof. Suppose \( f(x) \in F[x] \) is irreducible and monic. If \( f \) is not separable, then \( d = (f, f') \) is a nonconstant polynomial. Since \( d|f \) and \( f \) is irreducible and monic, we have \( d = f \). Then \( f|f' \) and since \( \deg(f') < \deg(f) \), this means \( f' = 0 \) identically. That cannot happen in characteristic 0, except \( f \) is a constant. Hence, if \( \text{char}(F) = 0 \), then \( F \) is perfect. In characteristic \( p \), \( f(x) = g(x^p) \) for some polynomial \( g(x) \). Since \( x \mapsto x^p \) is an automorphism, we can find a polynomial \( g_1(x) \) such that

\[
g(x^p) = (g_1(x))^p = (c_0 + c_1 x + \cdots + c_l x^l)^p = c_0^p + c_1^p x^p + \cdots + c_l^p x^{lp}.
\]

This contradicts the assumption that \( f \) is irreducible.

For any field \( K \) and for an “indeterminant” \( T \), the function field is the field of rational functions

\[
K(T) = \left\{ \frac{p(T)}{q(T)} : p, q \in K[T] \right\}
\]

where \( K[T] \) is the set of polynomials in \( T \) over \( K \).
Example 7.6 (Example of non-perfect field). If $K$ is characteristic $p$, then $K(T)$ is not perfect.

Proof. We claim $f(x) = x^p - T \in K(T)[x]$ is irreducible and inseparable. Since $f'(x) = pxx^{p-1} - 0 = 0$, $(f, f') \neq 1$, and so $f$ is inseparable. Let $F = K(T)$, and let $\alpha$ be a root of $f$ in the algebraic closure $\overline{F}$. Let $E = F(\alpha)$. Then $(x - \alpha)^p = x^p - \alpha^p = x^p - T$. We have to prove $(x - \alpha)^r \in F[x]$ and $r \geq 1$ if $r = p$. If $(x - \alpha)^r \in F[x]$, then $(-\alpha)^r$ (where $x = 0$) is in $F$. So $\alpha^r \in F$ and $\alpha^p \in E$. If $1 \leq r < p$, then $(r, p) = 1$ and so $ru + pv = 1$ for integers $u, v$. Then $\alpha = \alpha^{ru+pv} = (\alpha^r)^u(\alpha^p)^v \in F$. So $T = \alpha^p = \frac{h(T)^p}{g(T)^p} = \frac{h_1(T^p)}{g_1(T^p)}$.

Hence $Tg_1(T^p) = h_1(T^p)$, but this is impossible in $K[T]$. \qed

Suppose $E/F$ is a finite extension of fields. $E/F$ is separable iff for any embedding $\sigma : F \rightarrow L$ where $L$ is algebraic closure of $F$, there exists exactly $(E : F)$ distinct embeddings $\sigma_i : E \hookrightarrow L$ such that $\sigma_i | F = \sigma$.

Remark 7.7. In general, there are $\leq (E : F)$ such embeddings.

Theorem 7.8. For $F \subset E \subset H$, $H/F$ is separable $\iff$ both $E/F$, $H/E$ are separable.

Theorem 7.9. $F(\alpha)/F$ is separable iff the minimal irreducible polynomial $m_{F, \alpha}(x)$ satisfied by $\alpha$ has distinct roots in an algebraic closure of $F$.

Theorem 7.10 (Primitive Element Theorem). Suppose $E/F$ is a finite extension of fields, then there exists $\alpha \in E$ such that $E = F(\alpha)$ iff there are at most finitely many fields $K$ with $F \subset K \subset E$. If $E/F$ is separable, then $E = F(\alpha)$ for some $\alpha \in E$.

8 Trace and Norm, Commutative $F$-algebras (09/05)

Let $E/F$ be separable finite extension, $L$ algebraic closure of $F$. The distinct embedding of $E \hookrightarrow L$ over $F$ are $\sigma_1, \cdots, \sigma_n$, $n = [E : F]$. If $(u_1, \cdots, u_n)$ is a basis of $E$ over $F$, define

$$V^*(u_1, \cdots, u_n) = \det([u^\sigma_j])_{1 \leq i,j \leq n}.$$ 

Theorem 8.1.

$$V^*(u_1, \cdots, u_n) \neq 0.$$ 

Proof. If $\det([u^\sigma_j]) = 0$, then the columns are linearly dependent. So there is a $\overrightarrow{t} = \begin{bmatrix} l_1 \\ \vdots \\ l_n \end{bmatrix} \neq \overrightarrow{0}$ ($l_i \in L$) such that

$$[u^\sigma_j]^T \overrightarrow{t} = \overrightarrow{0}.$$
Then for each $i$,
\[ \sum_{j=1}^{n} u_{ij}^{\sigma_j} l_j = 0. \]
For any $c_1, \ldots, c_n \in F$,
\[ \sum_{i=1}^{n} c_i \sum_{j=1}^{n} u_{ij}^{\sigma_j} l_j = 0. \]
Hence,
\[ \sum_{j=1}^{n} \left( \sum_{i=1}^{n} c_i u_i \right)^{\sigma_j} l_j = 0 \]
where $\sum_{i=1}^{n} c_i u_i$ is any element of $E$. Hence, $\sum_{j=1}^{n} (\alpha)^{\sigma_j} l_j = 0$ for all $\alpha \in E$. This contradicts linear independence of characters. \( \square \)

If $(w_1, \ldots, w_n)$ is another basis of $E$ over $F$, then
\[ w_i = \sum_{j=1}^{n} c_{ij} u_j \]
for some $c_{ij} \in F$ and $\det [c_{ij}] \neq 0$ since this is invertible. Then
\[ [w_i^{\sigma_k}] = [c_{ij}][u_i^{\sigma_k}]. \]
Therefore,
\[ V^*(w_1, \ldots, w_n) = \det([c_{ij}])V^*(u_1, \ldots, u_n). \]

**Example 8.2.** If $E = F(\alpha)$, $\alpha$ is separable over $F$, $\sigma_i \in \text{Gal}(E/F)$ and we take the basis to be $(1, \alpha, \ldots, \alpha^{n-1})$, then
\[ V^*(1, \alpha, \ldots, \alpha^{n-1}) = V(\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_n}) \text{ (Vandermonde determinant)} \]
\[ = \prod_{1 \leq i < j \leq n} (\alpha^{\sigma_i} - \alpha^{\sigma_j}) \]
\[ \neq 0. \]

**Definition 8.3.** Trace and norm are defined as
\[ t_{E/F}(\alpha) = \sum_{i=1}^{n} \alpha^{\sigma_i}, \]
\[ N_{E/F}(\alpha) = \prod_{i=1}^{n} \alpha^{\sigma_i}. \]
Both of trace and norm are in $F$. If $H$ is the Galois closure of $E$ over $F$ (smallest Galois extension over $F$ containing $E$). If $E = F(\alpha), H = F(\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_n})$, $\text{Gal}(H/F)$ fixes $t_{E/F}(\alpha), N_{E/F}(\alpha)$. Hence they are in $F$.

For a basis $(u_1, \ldots, u_n)$ of $E/F$,

$$t_{E/F}(u_iu_j) = \sum_{k=1}^{n} u_i^{\sigma_k}u_j^{\sigma_k} = ([u_i^{\sigma_k}] [u_j^{\sigma_k}]^T)_{ij}.$$ 

So

$$[t_{E/F}(u_iu_j)] = [u_i^{\sigma_k}] [u_j^{\sigma_k}]^T,$$
$$\det[t_{E/F}(u_iu_j)] = (V^*(u_1, \ldots, u_n))^2 = d(u_1, \ldots, u_n) \in F.$$

If $f(x)$ is minimal polynomial of $\alpha$ such that $E = F(\alpha)$, then $d(1, \alpha, \ldots, \alpha^{n-1}) = \text{Disc}(f)$.

**Theorem 8.4** (Tower Laws). If $K \subset F \subset E$ are separable finite extension, then

$$t_{E/K}(\alpha) = t_{F/K}(t_{E/F}(\alpha)),$$
$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha)).$$

Suppose $A$ is a finite commutative $F$-algebra. Each $a \in A$ defines an $F$-linear map

$$l_a : A \to A \text{ by } l_c(b) = ab.$$ 

Suppose $(v_1, \ldots, v_n)$ is a basis of $A$ over $F$. Then

$$av_i = \sum c_{ij} v_j$$
for some $c_{ij} \in F$. So $[c_{ij}]$ is a matrix of $l_a$ relative to $(v_1, \ldots, v_n)$.

$$\text{Trace}(l_a) = \sum_{i=1}^{n} c_{ii} = t_{A/F}(a),$$
$$\text{Norm}(l_a) = \det[c_{ij}] = N_{A/F}(a).$$

If $A = E$ is a separable field extension of $F$ of degree $n$ and $E = F(\alpha)$, then this agrees with previous definitions.
9 Idempotent and Radical (09/08)

**Definition 9.1.** An idempotent $e \in A$ is an element satisfying $e^2 = e$.

**Remark 9.2.**

(i) $e = 0, 1$ are both idempotent.

(ii) If $e^2 = e$, then

\[(1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e.\]

Therefore, $1 - e$ is also an idempotent. Also,

\[e(1 - e) = e - e^2 = e - e = 0.\]

So $e, 1 - e$ are orthogonal idempotents.

**Definition 9.3.** An idempotent $e$ is primitive if $e = e' + e''$ for two idempotents $e', e''$ with $e' e'' = 0$ implies $e' = 0$ or $e'' = 0$.

**Remark 9.4.**

If $e \neq 0$ is an idempotent, then $A e$ is a subalgebra of $A$ since $(ae)(be) = (ab)e^2 = (ab)e$. $A e$ is a vector space over $F$, and $1 \leq \dim_F A e \leq \dim_F A$.

**Theorem 9.5.** There exists a maximal finite collection of nonzero orthogonal idempotents $e_1, \cdots, e_n$ with $1 = e_1 + \cdots + e_n$ and then $A = \bigoplus_{i=1}^n A e_i$.

**Remark 9.6.**

(i) $e$ is primitive iff $A e$ is indecomposable, meaning $A e$ cannot be written as $B \oplus C$ for nonzero algebras $B, C$.

(ii) If $A = \bigoplus_{i=1}^n A_i = \prod_{i=1}^n A_i$ where $A_i = A e_i$, then for $c = (c_1, \cdots, c_n) \in A$, we have

\[t_{A/F}(c) = \sum_{i=1}^n t_{A_i/F}(c_i),\]

\[N_{A/F}(c) = \prod_{i=1}^n N_{A_i/F}(c_i).\]

**Definition 9.7.** The radical of $A$ is the set

\[\text{Rad}(A) = \{ a \in A : a^n = 0 \text{ for some } n \geq 1 \}.\]

**Theorem 9.8.** $\text{Rad}(A)$ is an ideal of $A$.

**Proof.** Clearly $0 \in \text{Rad}(A)$. If $a^n = 0$, then for any $c \in A$,

\[(ca)^n = c^n a^n = 0.\]

If $a^n = 0$ and $b^m = 0$, then

\[(a + b)^{m+n} = 0.\]
Theorem 9.9. If \( \overline{A} = A / \text{Rad}(A) \), then \( \text{Rad}(\overline{A}) = 0 \).

Proof. Suppose \((a + \text{Rad}(A))^n = 0\) in \( \overline{A} \), then \( a^n \in \text{Rad}(A) \). Then \( a^{nm} = (a^n)^m = 0 \) for some integer \( m \geq 1 \) and so \( a \in \text{Rad}(A) \). \( \square \)

Theorem 9.10. If \( A \) is an indecomposable finite \( F \)-algebra and \( \text{Rad}(A) = 0 \), then \( A \) is a field.

Theorem 9.11. Suppose \( A \) is a finite commutative \( F \)-algebra, then the following (i) and (ii) are equivalent:

(i) \( \text{Rad}(A) = 0 \).

(ii) \( A = \bigoplus_{i=1}^{t} A_i \) where each \( A_i \) is a field extension of \( F \).

Moreover, if \( F \) is perfect, then (i), (ii) are equivalent to (iii), (iv):

(iii) \( d(v_1, \ldots, v_n) \neq 0 \) for some basis \( v_1, \ldots, v_n \) of \( A \) over \( F \).

(iv) \( d(v_1, \ldots, v_n) \neq 0 \) for all basis \( v_1, \ldots, v_n \) of \( A \) over \( F \).

Theorem 9.12. \( t_{A/F}(a) = 0 \) if \( a \) is nilpotent.

Proof. Let \( l_a : A \to A \) be the linear map \( l_a(b) = ab \). If \( v_1, \ldots, v_n \) is a basis of \( A \) over \( F \), then \( av_i = \sum_{j=1}^{n} c_{ij}v_j \) for \( c_{ij} \in F \). So \([c_{ij}]\) is the matrix of \( l_a \) with respect to \( v_1, \ldots, v_n \).

Let \( p(x) = \det(xI_n - [c_{ij}]) = x^n + u_1x^{n-1} + \cdots + u_n \). By Cayley-Hamilton Theorem, \( A = [c_{ij}] \) satisfies \( p(A) = A^n + u_1A^{n-1} + \cdots + u_nI = 0 \). Since \( a^m = 0 \) for some \( m \geq 1 \), then \( t_{a}^m(b) = 0 \) for all \( b \), and \([c_{ij}]^m = 0 \). Also, all the eigenvalues of \([c_{ij}]\) are 0 in some algebraic closure \( F \) of \( F \), we have

\[
\det(xI_n - [c_{ij}]) = \prod_{i=1}^{n} (x - \lambda_i) = x^n.
\]

Since \( t_{A/F}(a) \) is the coefficient of \( x^{n-1} \) in \( \det(xI_n - [c_{ij}]) \), we have \( t_{A/F}(a) = 0 \). \( \square \)

10 Integrality (09/10)

Theorem 10.1. For an integral domain \( \mathfrak{o} \) and an extension ring \( \mathcal{O} \) of \( \mathfrak{o} \), \( a \in \mathcal{O} \) is integral over \( \mathfrak{o} \) iff \( \mathfrak{o}[a] \) is a finitely generated \( \mathfrak{o} \)-module.

Theorem 10.2. \( a \in \mathcal{O} \) is integral over \( \mathfrak{o} \) iff \( a \in \mathcal{R} \subseteq \mathcal{O} \) where \( \mathcal{R} \) is a subring of \( \mathcal{O} \) containing \( \mathfrak{o} \) and is a finitely generated \( \mathfrak{o} \)-module.

Proof. (\( \Rightarrow \)) By Theorem 10.1 \( \mathcal{R} = \mathfrak{o}[a] \) is a subring that works.

(\( \Leftarrow \)) Suppose \( \mathcal{R} = (r_1, \ldots, r_n)\mathfrak{o} = r_1\mathfrak{o} + \cdots + r_n\mathfrak{o} \). Then

\[
ar_i = \sum_{j=1}^{n} c_{ij}r_j
\]
for some $c_{ij} \in \mathfrak{o}$. Then $p(x) = \det (xI_n - [c_{ij}]) = x^n + \text{terms of smaller degree} \in \mathfrak{o}[x]$ (so it is monic). By Cayley-Hamilton Theorem, $p([c_{ij}]) = 0$. This implies that $p(a)r_i = 0$ for all $i$ (since $ar_i = [c_{ij}][r_j]_{j=1}^n$). Some $r_i \neq 0$ because $1 \in \mathfrak{R}$. So $p(a) = 0$. So $a$ is integral over $\mathfrak{o}$. \hfill \Box

**Definition 10.3.** The integral closure of $\mathfrak{o}$ in $\mathcal{O}$ is the set of $a$ which are integral over $\mathfrak{o}$.

**Definition 10.4.** $\mathfrak{o}$ is integrally closed if it equals to its integral closure in its field of fractions.

**Example 10.5.** $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed. $a = \frac{1 + \sqrt{-3}}{2}$ lies in the field of fractions $\mathbb{Q}[\sqrt{-3}]$, and is integral ($a^2 - a + 1 = 0$) over $\mathbb{Z}[\sqrt{-3}]$, but it is not in $\mathbb{Z}[\sqrt{-3}]$.

**Example 10.6.** $\mathfrak{o} = F[T^2, T^3] = \{c_0 + c_2T^2 + c_3T^3 + \cdots + c_nT^n | c_0, c_2, \cdots, c_n \in F\}$ for any field $F$ is not integrally closed. Its field of fractions is $K = \{(\frac{p(T)}{q(T)}) | p(T), q(T) \in \mathfrak{o}\}$. $a = \frac{T^3}{T^2}$ is integral over $\mathfrak{o}$ (since $a^2 - T^2 = 0$), but $a$ is not in $\mathfrak{o}$.

Let $\mathfrak{o}$ be an integral domain which is integrally closed, $K$ the field of fractions, $E$ a separable finite extension of $K$ of degree $n$, $L$ is some algebraic closure of $E$. Let $\sigma_1, \sigma_2, \cdots, \sigma_n : E \to L$ be the distinct embeddings over $K$.

**Proposition 10.7.** If $a \in E$ is integral over $\mathfrak{o}$, then so is $a^{\sigma_j}$ for $1 \leq j \leq n$.

*Proof.* Suppose $a$ satisfies a monic polynomial $p(x) \in \mathfrak{o}[x]$, so $p(a) = 0$ and $0 = (p(a))^{\sigma_j} = p(a^{\sigma_j})$ because coefficients of $p(x)$ are in $\mathfrak{o} \subseteq K$. Then $p(x) = \prod_{j=1}^n (x - a^{\sigma_j})$. So $a^{\sigma_j}$ is integral over $\mathfrak{o}$. \hfill \Box

**11 Noetherian Rings and Modules (09/12)**

**Definition 11.1.** An $\mathfrak{o}$-module $M$ is Noetherian if it satisfies the following equivalent conditions:

(i) All $\mathfrak{o}$-submodules of $M$ are finitely generated;

(ii) (Ascending Chain Condition) Every strictly increasing $\mathfrak{o}$-submodules $N_1 \subset N_2 \subset \cdots \subset M$ is finite;

(iii) Every nonempty family of $\mathfrak{o}$-submodules of $M$ has a maximal element.

**Remark 11.2.** (i) An $\mathfrak{o}$-module $M$ is Artinian module if it satisfies Descending Chain Condition.

(ii) $\mathfrak{o}$ is a Noetherian ring if it is a Noetherian $\mathfrak{o}$-module ($\iff$ Every ideal of $\mathfrak{o}$ is finitely-generated).

(iii) Every finitely-generated module over a Noetherian ring is a Noetherian module.

**Theorem 11.3.** If $0 \to M \to N \to P \to 0$ is an exact sequence of $\mathfrak{o}$-modules, then $N$ is Noetherian iff $M$ and $P$ are Noetherian.
Theorem 11.4. If $\mathfrak{o}$ is a Noetherian ring and $M$ is a finitely-generated $\mathfrak{o}$-module, then $M$ is a Noetherian $\mathfrak{o}$-module.

Theorem 11.5. If $\phi : \mathfrak{o} \to \mathfrak{R}$ is a surjective ring homomorphism and $\mathfrak{o}$ is Noetherian, then $\mathfrak{R}$ is Noetherian.

Theorem 11.6 (Hilbert Basis Theorem). If $\mathfrak{o}$ is Noetherian, then $\mathfrak{o}[X]$ is Noetherian.

Proof. Let $\mathfrak{a}$ be an ideal in $\mathfrak{o}[x]$. Let

$$\mathfrak{b} = \{ c \in \mathfrak{o} | \exists f(x) = cx^n + c_1x^{n-1} + \cdots + c_n \in \mathfrak{a} \text{ for some } n \}.$$ 

$\mathfrak{b}$ is an ideal in $\mathfrak{o}$, hence it is finitely generated, and so $\mathfrak{b} = (b_1, \cdots, b_n)\mathfrak{o}$. Let $f_1, \cdots, f_n \in \mathfrak{a}$ be such that the leading coefficient of $f_j$ is $b_j$. Let $d = \max(\deg(f_j))$. Let

$$\mathfrak{c} = \{ f \in \mathfrak{a} | f = 0 \text{ or } \deg(f) \leq d \}.$$ 

Thus, $\mathfrak{c} \subseteq (1, x, \cdots, x^d)\mathfrak{o}$ is a submodule of a finitely generated module over $\mathfrak{o}$. So $\mathfrak{c}$ is finitely generated with generators $g_1, \cdots, g_m$. Then we claim $(f_1, \cdots, f_n, g_1, \cdots, g_m)$ generate $\mathfrak{a}$. We use induction on $k = \deg(f(x))$ for $f \in \mathfrak{a}$. If $k \leq d$, $f$ is a linear combination of $g_1, \cdots, g_m$. If $k > d$, let $f(x) = cx^k + c_1x^{k-1} + \cdots + c_k$. Then $c \in \mathfrak{b}$ and so $c = a_1b_1 + \cdots + a_nb_n$ where $a_i \in \mathfrak{o}$. Then

$$f(x) - a_1f_1(x)x^{k-\deg(f_1)} - \cdots - a_nf_n(x)x^{k-\deg(f_n)}$$

has degree $< k$. By induction, $\mathfrak{a}$ is generated by $(f_1, \cdots, f_n, g_1, \cdots, g_m)$.

Corollary 11.7. If $\mathfrak{o}$ is Noetherian, then $\mathfrak{o}[X_1, X_2, \cdots, X_n]$ is Noetherian.

12 Dedekind Domains I (09/15)

An integral domain $\mathfrak{o}$ is not usually a UFD. But under slightly some general conditions $\mathfrak{o}$ will have unique factorization of ideals into products of prime ideals.

Definition 12.1. $\mathfrak{o}$ is a Dedekind domain if

(i) $\mathfrak{o}$ is Noetherian;

(ii) $\mathfrak{o}$ is integrally closed;

(iii) All prime ideals $\mathfrak{p} \neq 0$ are maximal.

Example 12.2. Here is an example of a ring where we have a prime ideal $\neq 0$ which is not maximal. Let $K$ be a field, $R = K[X, Y], \mathfrak{p} = RX = (X)R, \mathfrak{m} = (X, Y)R = XR + YR$, then $0 \subset \mathfrak{p} \subset \mathfrak{m} \subset R$.

Definition 12.3. The Krull dimension of an integral domain $\mathfrak{o}$ is the maximal $l$ such that there is a sequence of prime ideals $\mathfrak{p}_l \subset \cdots \subset \mathfrak{p}_1 \subset \mathfrak{p}$ in $\mathfrak{o}$. 

19
Theorem 12.4. Every nonzero ideal \( a \) of a Dedekind domain may be written as a product of prime ideals \( a = p_1p_2 \cdots p_n \) which is unique up to rearrangement.

Theorem 12.5. Any PID is a Dedekind Domain.

Proof. Suppose \( \mathfrak{o} \) is a PID. Then \( \mathfrak{o} \) is Noetherian, since every ideal is generated by 1 element.

Let \( K \) be the field of fractions of \( \mathfrak{o} \), and suppose \( \alpha \in K \) is integral over \( \mathfrak{o} \). Then
\[
\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0
\]
for \( c_i \in \mathbb{R} \). Suppose \( \alpha = a/b \) for \( a,b \in K \) and \( a,b \) have no non-unit common divisor. Substituting \( \alpha \) with \( a/b \) in equation (12.1) and multiplying each side by \( b^n \), we get
\[
a^n + c_{n-1}a^{n-1}b + \cdots + c_1ab^{n-1} + c_0b^n = 0
\]
If \( b \) is a non-unit, we can always find a prime element \( p \) which is a divisor of \( b \) since \( \mathfrak{o} \) is a PID, and hence a UFD. From equation (12.2), we must have \( p \) also divides \( a \) since \( p \) divides the rest terms of the equation (12.2). Then \( p \) divides both \( a \) and \( b \). This contradiction shows that \( b \) is a unit. Hence \( \alpha = a/b \) is actually in \( \mathfrak{o} \). Therefore, \( \mathfrak{o} \) is integrally closed.

Suppose \( (p) \varsubsetneq (m) \varsubsetneq \mathfrak{o} \). Then \( p = mx \) for some \( x \in \mathfrak{o}, x \notin \mathfrak{o}^* \) (\( x \) is not a unit). Since \( (m) \varsubsetneq \mathfrak{o}, m \notin \mathfrak{o}^* \). If \( m \in (p) \), then \( m = pu \), so \( p = mx = pux \). Therefore, \( ux = 1 \), and so \( x \in \mathfrak{o}^* \). But \( x \notin \mathfrak{o}^* \), so \( m \notin (p) \). Then \( mx \in (p) \) and \( m, x \) are not in \((p)\). That contradicts \((p)\) being a prime ideal.

Remark 12.6. The prime ideal factorization theorem will prove that a PID is a UFD.

Definition 12.7. Let \( \mathfrak{o} \) be an integral domain, \( K \) its field of fractions. Then an \( \mathfrak{o} \)-submodule \( b \subset K \) is a fractional ideal if there exists \( c \in K^* \) and a nonzero ideal \( a \subset \mathfrak{o} \) such that \( b = ca \).

Theorem 12.8 (D1). Suppose \( \mathfrak{o} \) is Noetherian and integrally closed, and \( a \) is any fractional ideal of \( \mathfrak{o} \), then
\[
\{ x \in K | xa \subset a \} = \mathfrak{o}.
\]

Proof. Clearly \( \mathfrak{o} \subset \{ x \in K | xa \subset a \} \), since \( a \) is fractional ideal of \( \mathfrak{o} \). For the reverse inclusion, since \( \mathfrak{o} \) is Noetherian, \( a = (c_1, c_2, \ldots, c_m)\mathfrak{o} \). If \( ba \subset a \), then \( bc_j = \sum_{j=1}^{m} a_{ij}c_j \) for some \( a_{ij} \in \mathfrak{o} \). Then by Cayley-Hamilton Theorem \( b \) satisfies \( \det(xI_m - [a_{ij}]) = 0 \). This is a monic polynomial in \( \mathfrak{o}[x] \). Since \( \mathfrak{o} \) is integrally closed, \( b \in \mathfrak{o} \).

Remark 12.9. If \( \mathfrak{o} \) is Noetherian, \( a \subset K \) is a fractional ideal if and only if it is a finitely generated \( \mathfrak{o} \)-submodule.

Theorem 12.10 (D2). Suppose all the prime ideals of an integral domain \( \mathfrak{o} \) are maximal, then if \( p \supset p_1 \cdots p_n \) for nonzero prime ideals \( p, p_1, \cdots, p_n \), then \( p = p_j \) for some \( j \).
Proof. By induction on \( n \). For \( n = 1 \), if \( p \supset p_1 \), then since prime ideals are maximal, we have \( p = p_1 \).

Assume the theorem is true for \( n - 1 \). Suppose \( p \supset p_1 \cdots p_n \) and \( p \neq p_n \). Then there exists \( c \in p_n \setminus p \). (Again since prime ideals are maximal) Let \( b \in p_1 \cdots p_{n-1} \). Then \( bc \in p_1 \cdots p_n \subset p \). Since \( c \notin p \), we must have \( b \in p \), since \( p \) is prime. Thus \( p \supset p_1 \cdots p_{n-1} \) and by the induction assumption \( p = p_j \) for some \( 1 \leq j \leq n - 1 \).

Let \( a \) be a (nonzero) fractional ideal of \( o \). Define the inverse of a fractional ideal to be

\[ a^{-1} = \{ x \in K \mid xa \subset o \} \]

Then \( a^{-1} \) is clearly an \( o \)-submodule of \( K \). If \( \alpha \in a \) and \( \alpha \neq 0 \), then \( a^{-1} \alpha = b \subset o \) is an ideal of \( o \). So \( a^{-1} = \frac{1}{a} b \) is a fractional ideal. Also \( aa^{-1} \subset o \).

For any fractional ideals \( a, b, \) \( ab \) def \( \{ \sum_{i=1}^{t} a_i b_i \mid a_i \in a, b_i \in b \} \) is also a fractional ideal.

**Definition 12.11.** \( a \) is invertible iff \( aa^{-1} = o \).

**Theorem 12.12.** Every fractional ideal in a Dedekind domain \( o \) is invertible.

**Remark 12.13.** If \( o \) is a field, there are only two ideals: 0 and \( o \).

Let \( S \) be the set of integral ideals \( a \neq 0 \subset o \), such that there is a \( c \in K \setminus o \) such that \( ca \subset o \). If \( o \) is not a field, there is an \( a \neq 0 \) such that \( a \in o \setminus o^* \). Then \( \frac{1}{a} \notin o \) and \( \frac{1}{a}(ao) = o \). So \( S \neq \emptyset \) because \( ao \) is in \( S \). If \( o \) is Noetherian and not a field, \( S \) has a maximal element \( m \).

**Theorem 12.14** (D3). Let \( o \) be a Dedekind domain and not a field. Then any maximal element \( m \) of \( S \) is an invertible prime ideal.

Proof. Suppose \( ab \in m \) and \( a \in o \setminus m \) and \( b \in o \). Consider \( m + ao \supseteq m \). Since \( m \subset S \), \( \exists c \in K \setminus o \) such that \( cm \subset o \). Then \( c(m + ao) = cm + cao \). \( m + ao \) can not be in \( S \) because \( m \) is maximal in \( S \). So \( ca \notin o \). Now consider \( m + bo \supseteq m \) (\( bo \subset o \)). Then \( ac(m + bo) = acm + c(ab)m \subset o \) (\( cm \in o \), \( ab \in m \)). By maximality, \( m + bo \) is in \( S \) and contains \( m \) and so \( m + bo = m \). So \( b \in m \). That proves \( m \) is prime.

\( m \) is maximal by definition of Dedekind domain. Then \( mm^{-1} \) is an ideal containing \( m \) and so \( mm^{-1} = m \) or \( mm^{-1} = o \). If \( mm^{-1} = m \), then by theorem 12.8 that \( \{ x \in K \mid xa \subset o \} \) = \( o \) then we’d have \( m^{-1} \subset o \). Since \( m \subset S \), there is a \( c \in m^{-1} \setminus o \). That contradiction proves \( mm^{-1} = o \).

\[ \square \]

## 13 Dedekind Domains II (09/17)

**Theorem 13.1** (D4). Let \( o \) be a Dedekind domain. A nonzero ideal \( a \) in \( o \) is invertible iff \( a = m_1 \cdots m_r \) for some invertible prime ideals \( m_1, \cdots, m_r \).
Proof. \((\Leftarrow)\) Ideal multiplication is associative and commutative:

\[ ab = ba, \quad (ab)c = c(bc). \]

Hence,

\[ (m_1^{-1} \cdots m_r^{-1})(m_1 \cdots m_r) = (m_1^{-1}m_1) \cdots (m_r^{-1}m_r) = o. \]

Thus, \(a^{-1} = m_1^{-1} \cdots m_r^{-1}\) satisfies \(a^{-1}a = o.\)

\((\Rightarrow)\) Assume \(a \neq 0\) is a proper invertible ideal. Then \(a \subset o^\times o^\times\). Since \(a^{-1}a = o\), there are \(a_1, \ldots, a_n \in a\) and \(b_1, \ldots, b_n \in a^{-1}\) such that \(a_1b_1 + \cdots + a_nb_n = 1.\) Some \(b_j\) is not in \(o\) (otherwise \(1 \in a\)). Thus \(a^{-1} \neq o\) and \(o\) belongs to the family of ideals \(S.\) Then there is a maximal \(m_1\) in \(S\) such that \(a \subset m_1.\) Since \(m_1\) is invertible by Theorem \([12.14]\) we have \(m_1^{-1}a \subset o\) and \(a \subset m_1^{-1}a.\) If \(m_1^{-1}a = o\), then \(m_1(m_1^{-1}a) = a = m_1.\) Otherwise repeat the process with the nonzero proper ideal \(m_1^{-1}a\) to produce another \(m_2\) and so on. Then we get a sequence

\[ a \subset m_1^{-1}a \subset m_2^{-1}a \subset \cdots \subset o. \]

Since \(o\) is Noetherian, this ascending sequence must terminate with \(a = m_1m_2 \cdots m_r.\)

**Theorem 13.2 (D5).** Every prime ideal \(p\) of a Dedekind domain is invertible.

**Proof.** Pick \(a \in p \setminus \{0\}.\) Then \(ao\) is invertible because \((ao)^{-1} = \frac{1}{a}o\) and \((ao)(ao)^{-1} = o.\) By Theorem \([13.1]\) \(ao = m_1 \cdots m_r\) where \(m_1, \ldots, m_r\) are invertible prime ideals. So \(p \supset ao = m_1 \cdots m_r.\) So by Theorem \([12.10]\) \(p = m_j\) for some \(j.\)

**Theorem 13.3 (D6).** Every nonzero ideal \(a\) in a Dedekind domain \(o\) is a product of prime ideals \(a = p_1 \cdots p_r.\)

**Proof.** If \(a = o,\) then we are done with \(r = 1.\) If \(a \subsetneq o,\) then \(a\) is contained in a maximal (hence prime) ideal \(a \subset p_1 \subset o.\) Then \(a \subset p_1^{-1}a \subset o.\) If \(p_1^{-1}a = o,\) then \(a = p_1(p_1^{-1}a) = p_1.\) Otherwise, repeat the process for \(a \subset p_1^{-1}a \subset p_2^{-1}a \subset \cdots.\) Since \(o\) is Noetherian, we must have \(a = p_1p_2 \cdots p_r\) at some point.

**Theorem 13.4 (D7).** For every \(a \neq 0\) in a Dedekind domain \(o,\) the prime ideal factorization in Theorem \([13.3]\) is unique up to rearrangement.

**Proof.** Suppose \(a = p_1 \cdots p_r = q_1 \cdots q_s\) for prime ideals \(p_1, \ldots, p_r, q_1, \ldots, q_s\) with \(r \geq 0\) as small as possible. Then by Theorem \([12.10]\) \(p_j = q_j\) for some \(j.\) Renumber so that \(j = 1\) and \(p_1 = q_1.\) Then by Theorem \([13.2]\) \(p_1^{-1}(p_1 \cdots p_r) = q_1^{-1}(q_1 \cdots q_s)\) reduces to \(p_2 \cdots p_r = q_2 \cdots q_s.\) That contradicts \(r\) being minimal.

**Corollary 13.5.** In a Dedekind domain, every fractional ideal \(a\) can be uniquely written as \(a = p_1^{a_1} \cdots p_r^{a_r}\) for distinct prime ideals \(p_1, \ldots, p_r\) and nonzero integers \(a_1, \ldots, a_r\) up to rearrangement.
Example 14.1. \( \mathbb{Z}[\sqrt{-5}] \) is not a PID. 6 can be written as

\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \]

as ideals. All of these factors are irreducible.

Definition 14.2. Let \( \mathfrak{o} \) be a Dedekind domain. We say \( a \mid b \) if there is an ideal \( c \subset \mathfrak{o} \) such that \( b = ac \).

Proposition 14.3. \( a \mid b \iff a \supset b \).

Definition 14.4. The greatest common divisor of two ideals \( a, b \subset \mathfrak{o} \) is the minimal ideal \( c \) such that \( c \mid a \) and \( c \mid b \).

Remark 14.5. \( \gcd(a, b) = a + b \).

Definition 14.6. The least common multiple of two ideals \( a, b \subset \mathfrak{o} \) is the maximal ideal \( m \) such that \( a \mid m \) and \( b \mid m \).

Remark 14.7. \( \operatorname{lcm}(a, b) = a \cap b \).

Definition 14.8. \( a, b \) are relatively prime iff \( a + b = \mathfrak{o} \).

15 Chinese Remainder Theorem for Rings (09/22)

Theorem 15.1 (Chinese Remainder Theorem for Rings). Let \( R \) be a ring with 1. Let \( a_1, \ldots, a_n \) be two-sided ideals in \( R \) such that \( a_i + a_j = \mathfrak{o} \) for any \( i \neq j \). Then the map

\[ R/(a_1 \cap \cdots \cap a_n) \rightarrow \prod_{i=1}^n R/a_i \]

defined by

\[ x + (a_1 \cap \cdots \cap a_n) \mapsto (x + a_i) \]

is an \( R \)-module isomorphism.

Proof. This map is clearly well-defined and a module homomorphism. It is injective since if \( x \in a_i \) for all \( i \), then \( x \in a_1 \cap \cdots \cap a_n \). To prove surjectivity, we use induction on \( n \), and then it suffices to prove the theorem for \( n = 2 \) ideals. Since \( a_1 + a_2 = R \), there are \( a_1 \in a_1 \) and \( a_2 \in a_2 \) such that \( a_1 + a_2 = 1 \). Suppose we are given \( (y_1 + a_1, y_2 + a_2) \in R/a_1 \times R/a_2 \). Let \( x = y_2a_1 + y_1a_2 \). Then

\[ x = y_2a_1 + y_1(1 - a_1) = y_1 - y_1a_1 + y_2a_1 \equiv y_1 \pmod{a}, \]
and
\[ x = y_2(1 - a_2) + y_1a_2 = y_2 - y_2a_2 + y_1a_2 \equiv y_2 \pmod{a_2}. \]

For \( n > 2 \) assume the theorem is true for \( n - 1 \) ideals, since it is true for 2 ideals, we can say
\[ R/a_1 \cap \cdots \cap a_n \cong (R/a_1 \cap \cdots \cap a_{n-1}) \times R/a_n \]
if \( a_1 \cap \cdots \cap a_{n-1} + a_n = R \). Since \( a_i + a_n = R \) for \( 1 \leq i \leq n - 1 \), then \( u_i + v_i = 1 \) for some \( u_i \in a_i, v_i \in a_n \). So
\[ 1 = (u_1 + v_1) \cdots (u_n + v_n) = u_1u_2 \cdots u_n + \text{multiple of } v's \in a_1 \cap \cdots \cap a_{n-1} + a_n. \]

**Theorem 15.2.** For every proper prime ideal \( p \) in a Dedekind domain \( \mathfrak{a} \), \( \mathfrak{a} \supseteq p \supseteq p^2 \supseteq p^3 \supseteq \cdots \).

**Proof.** The inequalities follow from unique factorization into prime ideals.

**Corollary 15.3.** For any nonzero ideals \( a, b \in \mathfrak{a} \), there exists \( \alpha \in a \) such that \( \alpha a^{-1} + b = \mathfrak{a} \).

**Proof.** Let \( b = p_1^{m_1} \cdots p_m^{m_n} \). For each \( j \), suppose \( p_j^{n_j} \) exactly divides \( a \). Pick \( \alpha_j \in p_j^{n_j} \setminus p_j^{n_j+1} \).

Pick \( \alpha \equiv \alpha_j \pmod{p_j^{n_j+1}} \) for all \( j \), by Chinese Remainder Theorem. Then \( \alpha \in p_j^{n_j} \) for all \( j \). Hence, \( \alpha \in \prod_{j=1}^{k} p_j^{n_j} \), then \( \alpha \mathfrak{a} = \left( \prod_{j=1}^{k} p_j^{n_j} \right) \) is a product of primes \( q \neq \text{any } p_j \). Since \( \alpha \mathfrak{a} \subseteq \mathfrak{a} \), \( a|\alpha \mathfrak{a} \), and together with the assumption that \( p_j^{n_j} \) exactly divides \( a \), \( (\alpha \mathfrak{a})a^{-1} = \alpha a^{-1} \) is a product of primes \( q \neq \text{any } p_j \). So \( \alpha a^{-1} \) is relatively prime to \( b \), and so \( \alpha a^{-1} + b = \mathfrak{a} \).

**Corollary 15.4.** If \( a \) is a nonzero integral ideal in a Dedekind domain \( \mathfrak{a} \) and \( \alpha \neq 0 \) is in \( a \), there is an \( \alpha' \in a \) such that \( a = (\alpha, \alpha') = \alpha \mathfrak{a} + \alpha' \mathfrak{a} \).

**Proof.** Take \( b = \alpha^{-1}a \) in Corollary 15.3. Then there is an \( \alpha' \in \mathfrak{a} \) such that \( \alpha' a^{-1} + \alpha a^{-1} = \mathfrak{a} \). Then \( (\alpha', \alpha) = a \).

### 16 Valuation (09/24)

**Definition 16.1.** For a prime \( p \) and an ideal \( \mathfrak{a} \neq 0 \), we define the \( p \)-adic valuation of \( \mathfrak{a} \) to be
\[ v_p(\mathfrak{a}) = \text{exponent of } p \text{ in the prime factorization of } \mathfrak{a}. \]

**Remark 16.2.** Properties of valuation:

(i) \( v_p(ab) = v_p(a) + v_p(b) \).

(ii) \( v_p(\mathfrak{a}) \leq v_p(b) \).

(iii) \( v_p(\mathfrak{a} \cap b) = \max\{v_p(\mathfrak{a}), v_p(b)\} \).

(iv) \( v_p(\mathfrak{a} + b) = \min\{v_p(\mathfrak{a}), v_p(b)\} \).

(v) \( v_p(\mathfrak{a} \cap b) + v_p(\mathfrak{a} + b) = v_p(\mathfrak{a}) + v_p(b) \).

(vi) \( \mathfrak{a} + b = \mathfrak{a} \iff \mathfrak{a} \cap b = \mathfrak{a}b \).
Example 16.3. In a noncommutative ring, we may have \(a + b = 0\) but \(a \cap b \neq ab\). For example, let \(R = \mathbb{R}[X,Y]\) with \(XY \neq YX\) be a noncommutative polynomial ring, let \(a = (X), b = (XY + 1)\), then \(a + b = 0, a \cap b \neq ab\).

Definition 16.4. We can define an absolute value \(| \cdot |_p : K^* \to (0, \infty)\). Pick some number \(c > 1\). Define \(|\alpha|_p = c^{-v_p(\alpha)}\).

Remark 16.5. Properties of absolute value:
(i) \(|\alpha\beta|_p = |\alpha|_p|\beta|_p|.
(ii) \(|\alpha + \beta|_p \leq \max(\{|\alpha|_p, |\beta|_p\}) \leq |\alpha|_p + |\beta|_p|.

\(|\cdot|_p\) is a \(p\)-adic absolute value. Extend \(|\cdot|_p\) to \(0| = 0\), \(|\cdot|_p\) defines a metric on \(K\). The completion of \(K\) relative to this metric is \(K_p\) (the field of \(p\)-adic numbers).

Theorem 16.6. For a Dedekind domain \(\mathfrak{o}\) and a prime ideal \(p\), \(\mathfrak{o}/p\) is a field, and \(\mathfrak{o}/p \cong \mathbb{p}^n/p^{n+1}\) for all \(n \in \mathbb{Z}\).

Proof. Define an isomorphism \(f : \mathfrak{o}/p \to \mathbb{p}^n/p^{n+1}\).

Pick \(a \in \mathbb{p}^n/p^{n+1}\). Define \(f(x + p) = ax + p^{n+1}\) for all \(x \in \mathfrak{o}\).

It is well-defined: If \(x + p = x' + p\), then \(x - x' \in p\). Then \(a \cdot (x - x') \in \mathbb{p}^n \cdot p = p^{n+1}\). Therefore, \(f(x + p) = ax + p^{n+1} = ax' + p^{n+1} = f(x' + p)\).

It is injective: If \(ax \in p^{n+1}\), then \(v_p(ax) \geq n + 1\). On the other hand, \(v_p(px) = v_p(a) + v_p(x) = n + v_p(x)\). Therefore, \(v_p(ax) = v_p(a) + v_p(x) = n + 1\) and so \(x \in p\).

It is surjective: Since \(a \in \mathbb{p}^n/p^{n+1}\), \((a) = \mathbb{p}^n b\) where \(p \nmid b\). Then \(p + b = \mathfrak{o}\), and so \(\mathbb{p}^n + \mathbb{p}^n b = \mathbb{p}^n\). For \(y \in \mathbb{p}^n\), there exists \(x \in \mathfrak{o}\) and \(z \in p^{n+1}\) such that \(y = z + ax\). Then \(y + p^{n+1} = f(x + p)\).

\(\square\)

Theorem 16.7 (Chinese Remainder Theorem for Dedekind Domains). For an ideal \(a\) in a Dedekind domain \(\mathfrak{o}\) with prime factorization \(a = p_1^{m_1} \cdots p_r^{m_r}\) where each \(p_j\) is distinct. Then \(\mathfrak{o}/a \cong \prod_{j=1}^r \mathfrak{o}/p_j^{m_j}\).

Definition 16.8. If \(K/\mathbb{Q}\) is a finite extension, we will see \(\mathfrak{o}/p\) is a finite field where \(\mathfrak{o}\) is the ring of integers in \(K\). Then we define absolute norm \(N(p) = |\mathfrak{o} : \mathfrak{p}|\).

Remark 16.9. \(N(a) = |\mathfrak{o} : a| = \prod_{j=1}^r N(p_j)^{m_j}\) for \(a = p_1^{m_1} \cdots p_r^{m_r}\).

17 Ideal Class Group in a Dedekind Domain (09/26)

Let \(I_\mathfrak{o}\) be the group of fractional ideals \(a\) in the Dedekind domain \(\mathfrak{o}\), \(P_\mathfrak{o}\) be the subgroup of principal ideals \((\alpha) = \alpha \mathfrak{o}\), \(\text{Cl}(\mathfrak{o}) = I_\mathfrak{o}/P_\mathfrak{o}\) be the class group. Then \(1 \to \mathfrak{o}^* \to K^* \to I_\mathfrak{o} \to \text{Cl}(\mathfrak{o}) \to 1\) is exact.
Corollary 17.1. \( Cl(o) = 1 \) if and only if \( o \) is a PID.

If \( L \) is a finite separable extension of \( K \), \( o \) is the ring of integers of \( K \), and \( O_L \) is the integral closure of \( o \) in \( L \), then for any ideal \( a \subset o \), \( aO_L \) is an ideal in \( O_L \). \( aO_L \) is called the lift of \( a \) to \( O_L \).

Theorem 17.2 (Principal Ideal Theorem (Furtwungler, 1929)). For any algebraic number field \( K/Q \), there is a finite extension \( L/K \) such that every ideal \( a \) in \( o_K \) lifts to a principal ideal in \( O_L \). The smallest degree extension \( H_K \) with this property is uniquely determined, it’s Galois over \( K \), and \( \text{Gal}(H/K) \cong Cl(o_K) \). \( H_K \) is called the Hilbert Class Field of \( K \).

Remark 17.3. A prime \( p = x^2 + 6y^2 \) for some integers \( x,y \) iff \( (\frac{-6}{p}) = 1 \) and for any integers \( u,v \) such that \( p|a^2 + 6v^2 \), the ideal \( p = (p,u+\sqrt{-6}v) \) is principal. It will turn out that \( Cl(Q(\sqrt{-6})) \cong C_2 \). \( p \) is 1 in \( Cl(Q(\sqrt{-6})) \) if and only if \( p \equiv 1,7 \mod 24 \).

18 Extensions of Dedekind Domain I (09/29)

Let \( o \) be a Dedekind domain, \( K \) be its field of fractions, \( L \) be a finite separable extension of \( K \), and \( O_L \) be the integral closure of \( o \) in \( L \). Consider the trace

\[
 t_{L/K}(x) = \sum_{\text{embeddings } \sigma \text{ of } L \text{ into } K} x^\sigma.
\]

We have \( t_{L/K}(x) \subset o \). This is because the embeddings \( \sigma \) generate the Galois group of the Galois closure \( N \) of \( L/K \). \( t_{L/K}(x) = \sum_{\sigma} x^\sigma \) is just permuted by applying any particular \( \sigma \). So \( t_{L/K}(x) \) is invariant under \( \text{Gal}(N/K) \). So \( t_{L/K}(x) \in K \) for all \( x \in L \). Each \( x^\sigma \) is an algebraic integer. So \( t_{L/K}(x) \in K \cap O_L = o \) since \( o \) is integrally closed.

Definition 18.1. For any \( o \)-submodule \( X \subset L \), the dual module of \( X \) is defined as

\[
 X^D = \{ x \in L | t_{L/K}(xy) \in o \text{ for all } y \in X \}.
\]

Remark 18.2. (i) \( (X^D)^D = X \).

(ii) If \( X \subset Y \), then \( Y^D \subset X^D \).

(iii) \( t_{L/K}(O_L) \subset o \) implies that \( O_L^D \supset O_L \).

Proposition 18.3. Suppose \( \{x_1, \cdots, x_n\} \) is a basis of \( L/K \). Let \( X = x_1o + \cdots + x_no \) be a free \( o \)-submodule of \( L \). For every \( j \), \( \exists y_j \in L \) with \( t_{L/K}(x_iy_j) = \delta_{ij} \) where

\[
 \delta_{ij} = \begin{cases} 
 1, & \text{if } i = j \\
 0, & \text{if } i \neq j.
\end{cases}
\]

Proof. We have a \( K \)-linear map \( L \to K^n \) defined by \( y \mapsto (t_{N/K}(yx_i))_{i=1}^n \). The kernel is 0 due to the fact that \( t_{N/K} \) is nonsingular \( \Leftrightarrow \) the embeddings are linear independent. Since
(L : K) = n, dim_L L = n = dim_K (K^n). Since the kernel is 0, the map is surjective. So there is some \( y_i \) such that

\[
(t_{N/L}(x_i y_j))_{i=1}^n = e^j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}
\]

Remark 18.4. \( \{y_1, \cdots, y_n\} \) is the dual basis.

Proposition 18.5. For \( X = x_1 \mathfrak{o} + \cdots + x_n \mathfrak{o} \) with dual basis \( \{y_1, \cdots, y_n\} \), we have

\[ X^D = \{c_1 y_1 + \cdots + c_n y_n | c_i \in \mathfrak{o}\} \]

is a free module spanned by \( y_1, \cdots, y_n \).

Proof. Suppose \( y = c_1 y_1 + \cdots + c_n y_n \in L \) with \( c_i \in K \). Then \( t_{L/K}(x_i y_i) = c_i \in \mathfrak{o} \) for all \( i \).

Example 18.6. Let \( K = \mathbb{Q}, \mathfrak{o} = \mathbb{Z}, L = \mathbb{Q}(\sqrt{-6}) \). Then \( \mathcal{O}_L = \mathbb{Z}[\sqrt{-6}] \),

\[ \mathcal{O}_L^D = \{x + y\sqrt{-6} | x, y \in \mathbb{Q} \text{ such that } t_{L/K}((x + y\sqrt{-6})(u + v\sqrt{-6})) \in \mathbb{Z} \text{ where } u, v \in \mathbb{Z} \}. \]

Since \( t_{L/K}(x + y\sqrt{-6}) = 2x \), \( t_{L/K}((x + y\sqrt{-6})\sqrt{-6}) = -12y \), then \( \mathcal{O}_L^D = \mathbb{Z}[\frac{1}{2}] + \mathbb{Z}[\sqrt{-6}] \), and \( [\mathcal{O}_L^D : \mathcal{O}_L] = 2 \cdot 12 = 24 \).

Theorem 18.7. Let \( \mathfrak{o} \) be a Dedekind domain, \( K \) be its field of fractions, \( L \) be a finite separable extension of \( K \), and \( \mathcal{O}_L \) be the integral closure of \( \mathfrak{o} \) in \( L \). Then \( \mathcal{O}_L \) is a Dedekind domain.

Proof. (i) \( \mathcal{O}_L \) is integrally closed by the theorem that integral closures are integrally closed.

(ii) Let \( \mathcal{A} \) be a non-zero ideal of \( \mathcal{O}_L \). Let \( x_1, \cdots, x_n \) be a basis of \( L \) over \( K \). Then \( \exists c_1, \cdots, c_n \neq 0 \) such that \( c_1 x_1, \cdots, c_n x_n \in \mathcal{O}_L \). For any \( a \in \mathcal{A}, a \neq 0 \), then \( a c_1 x_1, \cdots, a c_n x_n \) is a basis of \( L \) over \( K \) contained in \( \mathcal{A} \). Suppose \( x_1, \cdots, x_n \) is a basis of \( L \) over \( K \) contained in \( \mathcal{A} \). Then

\[ \mathcal{O}_L \supseteq \mathcal{A} \supseteq X = x_1 \mathfrak{o} + \cdots + x_n \mathfrak{o}. \]

Then

\[ X^D \supseteq \mathcal{A}^D \supseteq \mathcal{O}_L^D \supseteq \mathcal{O}_L \supseteq \mathcal{A}. \]

So \( X^D \) is a finitely-generated \( \mathfrak{o} \)-module containing \( \mathcal{A} \). Since \( \mathfrak{o} \) is Noetherian, then \( \mathcal{A} \) is finitely-generated \( \mathfrak{o} \)-module, then \( \mathcal{O}_L \) is Noetherian.

(iii) Let \( \mathcal{P} \) be a prime ideal in \( \mathcal{O}_L \). Then \( \mathcal{P} \cap \mathfrak{o} = p \) is a prime ideal in \( \mathfrak{o} \). \( p \mathcal{O}_L \) is an ideal in \( \mathcal{O}_L \).
We claim that \( pO_L \neq O_L \). In \( K \), we know that \( p^{-1} \supsetneq \mathfrak{o} \) because \( \mathfrak{o} \) is a Dedekind domain. Then \( p^{-1} \not\supseteq O_L \) because \( O_L \cap K = \mathfrak{o} \) by integral closure. Then \( pO_L \not\subseteq O_L \).

Then \( O_L/pO_L = \mathcal{A} \) is a commutative algebra over \( \mathfrak{o}/p = k \). Since \( O_L \) is finitely-generated as \( \mathfrak{o} \)-module, \( \mathcal{A} \) is a finite dimensional algebra over \( k \). Every commutative finite dimensional algebra \( \mathcal{A} \) over a field is isomorphic to a direct sum \( \mathcal{A} = \prod_{i=1}^t \mathcal{A}_i \) where \( \mathcal{A}_i \) is an algebra. \( \mathcal{A}_i \) is a field iff \( \text{Rad}(\mathcal{A}_i) = 0 \). The radical is an ideal and if \( \mathcal{A} = \mathcal{A}/\text{Rad}(\mathcal{A}) \) then \( \text{Rad}(\mathcal{A}) = 0 \). Also \( \mathcal{A} = \prod_{i=1}^t \mathcal{A}_i \) with \( \mathcal{A}_i = \mathcal{A}_i/\text{Rad}(\mathcal{A}_i) \). So each \( \mathcal{A}_i \) is a field.

Then \( O_L/\mathfrak{p}O_L = A \) is a commutative algebra over \( \mathfrak{o}/\mathfrak{p} = k \). Since \( O_L \) is finitely-generated as \( \mathfrak{o} \)-module, \( A \) is a finite dimensional algebra over \( k \). Every commutative finite dimensional algebra \( A \) over a field is isomorphic to a direct sum \( A = \prod_{i=1}^t A_i \) where \( A_i \) is a field.

The maximal ideals in \( \mathcal{A}_i \) are

\[
J_i = \prod_{j=1, j \neq i}^t \mathcal{A}_j.
\]

The maximal ideals in \( \mathcal{A} \) are the lifts

\[
J_i = \prod_{j=1, j \neq i}^t A_j.
\]

From the map \( O_L \to O_L/pO_L = \mathcal{A} \) the inverse images of the \( J_i \)'s are all the maximal ideals \( \mathcal{P}_i \) that contain \( pO_L \). This proves there are only finitely many maximal ideals containing \( pO_L \).

If \( \mathcal{P} \) is a prime ideal in \( O_L \) that contains \( pO_L \), then \( O_L/\mathcal{P} \) is a finite dimensional commutative \( k \)-algebra (\( k = \mathfrak{o}/p \)) and \( O_L/\mathcal{P} \) is an integral domain. That means that \( O_L/\mathcal{P} \) is indecomposable. Since \( \mathcal{P} \) is prime, if \( x^n \in \mathcal{P} \), then \( x \in \mathcal{P} \) for some \( n \geq 1 \). That means \( \text{Rad}(O_L/\mathcal{P}) = \mathfrak{o} \). Then \( O_L/\mathcal{P} \) is a field. Then \( \mathcal{P} \) is maximal.

19 Extensions of Dedekind Domain II (10/01)

**Example 19.1.** Let \( K = \mathbb{Q}, \mathfrak{o} = \mathbb{Z} \). Theorem 18.7 implies that for any finite extension \( L/\mathbb{Q} \), \( O_L \) is a Dedekind domain. Because \( \mathbb{Z} \) is a PID, \( O_L \) is a free \( \mathbb{Z} \)-module. Since \( O_L \) spans \( L \) over \( \mathbb{Q} \), \( O_L \) is a free \( \mathbb{Z} \)-module of rank \( n \), and has an integral basis

\[
\{w_1, \ldots, w_n\}.
\]

The discriminant is

\[
d_L = \det([t_{L/\mathbb{Q}}(w_iw_j)]) = \det([w_i^{\sigma_j}])^2 \neq 0
\]

where \( \sigma_1, \ldots, \sigma_n \) are the distinct embeddings \( L \hookrightarrow \overline{\mathbb{Q}} \). Suppose \( \{u_1, \ldots, u_n\} \) is another basis of \( O_L \). Then there exists integers \( a_{ij}, b_{ij} \in \mathbb{Z} \) such that

\[
w_i = \sum_{j=1}^n a_{ij}u_i, \quad u_i = \sum_{j=1}^n b_{ij}w_i.
\]
Then \([w_i^\sigma j] = [a_{ij}] [u_i^\sigma j], [u_i^\sigma j] = [b_{ij}] [w_i^\sigma j]\) as \(n \times n\) matrices. This implies \([a_{ij}] [b_{ij}] = I\). Hence \(\det([a_{ij}]) \det([b_{ij}]) = I\). Both determinants are integers, then \(\det([a_{ij}]) = \det([b_{ij}]) = \pm 1\). Hence, \(\det([u_i^\sigma j]) = \pm \det([u_i^\sigma j])\). So

\[d_L = \det([w_i^\sigma j])^2 = \det([u_i^\sigma j])^2.\]

**Theorem 19.2** (Stickelberger-Schur Theorem). For any finite extension \(L/\mathbb{Q}\), \(d_L \equiv 0, 1 \pmod{4}\).

**Proof.** We use the permutation definition of determinant:

\[
\det(w_i^\sigma j) = \sum_{\pi \in S_n} \text{sign}(\pi) w_1^{\sigma(1)} \cdots w_n^{\sigma(n)} = \sum_{\pi \text{ even}} w_1^{\sigma(1)} \cdots w_n^{\sigma(n)} - \sum_{\pi \text{ odd}} w_1^{\sigma(1)} \cdots w_n^{\sigma(n)} = E - O.
\]

If we apply any embedding \(\sigma\) to these terms,

\[(w_j^{\sigma(j)})^\sigma = w_j^{\sigma(\lambda j)}\]

for some permutation \(\lambda \in S_n\) determined by \(\sigma\). So either

\[E^\sigma = E, O^\sigma = O, \text{ if } \text{sgn}(\lambda) = 1\]

or

\[E^\sigma = O, O^\sigma = E, \text{ if } \text{sgn}(\lambda) = -1.\]

Then \((E + O)^\sigma = E + O\) for all \(\sigma\). So \(E + O \in \mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}\). Also \(d_L = (E - O)^2 \in \mathbb{Z}\). Then

\[d_L = (E - O)^2 = E^2 - 2EO + O^2 = (E + O)^2 - 4EO.
\]

Since \(E - O \in \mathbb{Z}, E + O \in \mathbb{Z}\), we have \(EO \in \mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}\). Then

\[d_L = (E + O)^2 - 4EO \equiv 0, 1 \pmod{4}.
\]

\[\square\]

**20 Extensions of Dedekind Domain III (10/03)**

**Theorem 20.1.** For \(K = \mathbb{Q}((\sqrt{m}))\) where \(m \neq 1\) is square-free,

\[
\mathcal{O}_K = \begin{cases} \mathbb{Z}[(\sqrt{m})] & \text{if } m \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}[1 + \sqrt{m}] & \text{if } m \equiv 1 \pmod{4}. \end{cases}
\]
Also, the fundamental discriminant is
\[ d_K = \begin{cases} 
4m & \text{if } m \equiv 2,3 \pmod{4}, \\
3m & \text{if } m \equiv 1 \pmod{4}.
\end{cases} \]

In all cases, \( \mathcal{O}_K = \mathbb{Z} \left[ \frac{d_K + \sqrt{d_K}}{2} \right] \).

**Proof.** The minimal polynomial of \( \alpha = u + v\sqrt{m} \in K = \mathbb{Q}(\sqrt{m}) \) is \( x^2 - t_{K/\mathbb{Q}}(\alpha) + N_{K/\mathbb{Q}}(\alpha) \). So
\[
\alpha \in \mathcal{O}_K \iff t_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \text{ and } N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}.
\]

So \( t_{K/\mathbb{Q}}(\alpha) = 2u, N_{K/\mathbb{Q}}(\alpha) = u^2 - mv^2 \). So \( \mathbb{Z}[\sqrt{m}] \subseteq \mathcal{O}_K \) with finite index \( l = [\mathcal{O}_K : \mathbb{Z}[\sqrt{m}]] \).

In general, \( \mathcal{O}_K \) has a free integral basis \( \{w_1, \ldots, w_n\} \). Suppose \( \wedge = \mathbb{Z}\{u_1, \ldots, u_n\} \subseteq \mathcal{O}_K \). So \( u_i = \sum_{j=1}^n a_{ij}w_i \) for some integers \( a_{ij} \). Then \([\mathcal{O}_K : \wedge] = |\text{det}(a_{ij})| \) from module theory over a PID. \( \mathcal{O}_K/\wedge \) is a finite abelian group. We can choose a basis \( \alpha_1, \ldots, \alpha_n \) of \( \mathcal{O}_K \) so that \( d_1\alpha_1, \ldots, d_n\alpha_n \) is a basis of \( \wedge \) with \( d_1|d_2|\cdots|d_n \). \([\mathcal{O}_K : \wedge] = d_1d_2\cdots d_n \). Also,
\[
\text{det}(\{u_i^{\sigma_j}\})^2 = \text{det}(\{a_{ij}\})^2 \cdot \text{det}(\{w_i^{\sigma_j}\})^2,
\]
so
\[
d(u_1, \ldots, u_n) = [\mathcal{O}_K : \wedge] \cdot d_K.
\]

In our quadratic case, \( u_1 = 1, u_2 = \sqrt{m} \), because \( \mathbb{Z}[\sqrt{m}] \subseteq \mathcal{O}_K \).
\[
d(\sqrt{m}) = \left| \frac{1}{n} \right| \left| \frac{\sqrt{m}}{\sqrt{m}} \right|^2 = 4m
\]
and \( d(\mathcal{O}_K) \cdot t^2 = d(\sqrt{m}) \), we have \( t^2|4m \). Since \( m \) is squarefree, \( l = 1 \) or \( 2 \). If \( l = 2 \), then
\[
\frac{1}{2} \mathbb{Z}[\sqrt{m}] \supset \mathcal{O}_K \supset \mathbb{Z}[\sqrt{m}].
\]

All we have to check are representatives of \( \frac{1}{2} \mathbb{Z}[\sqrt{m}] / \mathbb{Z}[\sqrt{m}] \). Try \( \alpha = \frac{1}{2}, \frac{\sqrt{m}}{2}, \frac{1+\sqrt{m}}{2} \), and we will see \( t(\alpha), N(\alpha) \in \mathbb{Z} \) iff \( m \equiv 1 \pmod{4} \). \( \square \)

**Theorem 20.2.** Let \( \mathfrak{o} \) be a Dedekind domain with field of fractions \( K \). Assume \( \mathfrak{o}/\mathfrak{p} \) is finite for all prime ideals \( \mathfrak{p} \). Then \( \mathfrak{o}/\mathfrak{a} \) is finite for all ideals \( \mathfrak{a} \neq 0 \) in \( \mathfrak{o} \).

**Proof.** First, we have shown \( \mathfrak{o}/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1} \) for all \( n \in \mathbb{Z} \). Then
\[
[\mathfrak{o} : \mathfrak{p}^n] = [\mathfrak{o} : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{n-1} : \mathfrak{p}^n] = [\mathfrak{o} : \mathfrak{p}]^n < \infty.
\]
For general ideals \( \mathfrak{a} \neq 0 \), Dedekind Theorem implies that \( \mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r} \) for distinct prime ideals \( \mathfrak{p}_j \). Then
\[
\mathfrak{o}/\mathfrak{a} \cong \prod_{j=1}^r \mathfrak{o}/\mathfrak{p}_j^{m_j}
\]
by Chinese Remainder Theorem. That proves \( [\mathfrak{o} : \mathfrak{a}] = \prod_{j=1}^r [\mathfrak{o} : \mathfrak{p}]^{m_j} \). \( \square \)
Theorem 21.3. We define the absolute norm of \( \mathfrak{a} \) to be

\[
N(\mathfrak{a}) = [\mathfrak{o} : \mathfrak{a}] \in \mathbb{N}.
\]

\( N \) extends to a homomorphism \( N : I_\mathfrak{o} \to \mathbb{Q}^* \):

\[
N(ab) = [\mathfrak{o} : ab] = [\mathfrak{o} : a][\mathfrak{o} : b] = [\mathfrak{o} : a][\mathfrak{o} : b] = N(\mathfrak{a})N(b).
\]

Let \( L/K \) be a finite separable extension with \( \mathcal{O}_L \) as the integral closure of \( \mathfrak{o} \). Then for any prime ideal \( \mathcal{P} \subset \mathcal{O}_L \) lying over \( \mathfrak{p} \subset \mathfrak{o}, \mathcal{O}_L/\mathcal{P} \) is an extension of finite degree over \( \mathfrak{o}/\mathfrak{p} \). So if \( \mathfrak{o}/\mathfrak{p} \) is finite for all \( \mathfrak{p} \) for all \( \mathfrak{o} \), then \( \mathcal{O}_L/\mathcal{P} \) is finite for all primes \( \mathcal{P} \) in \( \mathcal{O}_L \). If \( [\mathfrak{o}/\mathfrak{p}] = N_K(\mathfrak{p}) = q = p^f \) for a prime \( p \in \mathbb{Z} \), then \( [\mathcal{O}_L/\mathcal{P}] = N_L(\mathcal{P}) = q^{f_L/K(\mathcal{P})} \) where \( f_{L/K}(\mathcal{P}) \) is the residue degree of \( \mathcal{P} \) over \( \mathfrak{p} \) in \( L/K \). Also, \( \mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r} \) for distinct prime ideals \( \mathcal{P}_j \) in \( \mathcal{O}_L \). The \( e_j \) is the ramification degree of \( \mathcal{P}_j \) over \( \mathfrak{p} \).

21 Valuation Theory I (10/06)

Definition 21.1. Let \( K \) be a field. A discrete valuation is a map \( v : K^* \to \mathbb{Z} \) such that

(i) \( v(xy) = v(x) + v(y), \forall x, y \in K^*; \)
(ii) \( v(x + y) \geq \min(v(x), v(y)); \)
(iii) \( v \) is surjective.

Extend \( v \) to \( K \) by \( v(0) = \infty \) with \( +\infty + +\infty = \infty, \infty + n = \infty, \infty > n, \forall n \in \mathbb{Z} \). Define

\[
\mathfrak{o}_v = \{ x \in K | v(x) \geq 0 \},
\]

\[
\mathcal{P}_v = \{ x \in K | v(x) > 0 \}.
\]

\( \mathfrak{o}_v \) is a subring of \( K \) and \( \mathcal{P}_v \) is an ideal of \( \mathfrak{o}_v \).

Remark 21.2. From the definition, we know that \( v(1) = v(-1) = 0 \).

Theorem 21.3. \( \mathfrak{o}_v \) is a PID with a unique maximal ideal \( \mathcal{P}_v \).

Proof. If \( x \in \mathfrak{o}_v \), then \( x \) is in \( \mathfrak{o}_v^* \) iff \( x^{-1} \) is in \( \mathfrak{o}_v \) iff \( v(x) = 0 \). Since \( x^{-1} = 1, v(x) + v(-x) = v(1) = 0 \). Since \( x \in \mathfrak{o}_v^* \), then \( x^{-1} \in \mathfrak{o}_v^* \), and \( v(x) \geq 0, v(x^{-1}) \geq 0 \). So \( x \in \mathfrak{o}_v^* \) iff \( v(x) = v(x^{-1}) = 0 \). That proves \( \mathfrak{o}_v^* = \{ x \in K^* | v(x) = 0 \} = \mathfrak{o}_v/\mathcal{P}_v \). So \( \mathcal{P}_v \) is maximal and is the only maximal ideal. There exists \( \pi \in \mathcal{P}_v \) such that \( v(\pi) = 1 \) because \( v \) is surjective.

We claim that \( \mathcal{P}_v = \pi \mathfrak{o}_v = (\pi) \) and every non-zero ideal in \( \mathfrak{o}_v \) equals \( \mathcal{P}_v^m = (\pi^m) \) for some integer \( m \geq 0 \). Suppose \( x \in \mathcal{P}_v \). Then \( v(x) > 0 \) and \( v(x) \) is an integer, and so \( v(x) \geq 1 \) by definition. Then \( x = (x\pi^{-1})\pi \) and \( v(x\pi^{-1}) = v(x) - v(\pi) \geq 1 - 1 = 0 \). So \( x\pi^{-1} \in \mathfrak{o}_v \).

For any non-zero ideal \( \mathfrak{a} \subset \mathfrak{o}_v \), choose \( a \in \mathfrak{a} \) with minimal valuation \( v(a) = m \). We claim \( a = \mathcal{P}_v^m = (\pi^m) \). For any \( b \in \mathfrak{a}, b = (b\pi^{-m})\pi^m \) and again \( v(b\pi^{-m}) = v(b) - m \geq m - m = 0 \). That proves \( a \subset (\pi^m) \). By similar reasoning, \( v(a\pi^{-m}) = 0 \), and so \( a\pi^{-m} \in \mathfrak{o}_v^* \). So \( \pi^{-m} \in a \). □
For a general Dedekind domain, we had an exact sequence

\[ 1 \to \mathfrak{o}^* \to K^* \to I_\mathfrak{o} \to \text{Cl}(\mathfrak{o}) \to 1. \]

For a discrete valuation domain \( \mathfrak{o}_v \), this reduces to

\[ 1 \to \mathfrak{o}_v^* \to K^* \to \mathbb{Z} \to 0. \]

Let \( U^{(n)}_K = 1 + \mathcal{P}_v^n \) for \( n \geq 1 \). Then

\[ \mathfrak{o}_v^* \supseteq U^{(1)}_K \supseteq U^{(2)}_K \supseteq U^{(3)}_K \cdots \]

and

\[ \mathfrak{o}_v^*/U^{(1)}_K \cong (\mathfrak{o}_v/\mathcal{P}_v)^*, \]

\[ U^{(n)}_K/U^{(n+1)}_K \cong \mathcal{P}_v^n/\mathcal{P}_v^{n+1} \cong \mathfrak{o}_v/\mathcal{P}_v = k_v. \]

Here is the proof. Define the homomorphism: \( \mathfrak{o}_v^* = \mathfrak{o}_v/\mathcal{P}_v \to (\mathfrak{o}_v/\mathcal{P}_v)^* \): \( x \mapsto x + \mathcal{P}_v \). Suppose \( x \) maps to \( 1 + \mathcal{P}_v \) in \( (\mathfrak{o}_v/\mathcal{P}_v)^* \), then \( x \in 1 + \mathcal{P}_v \). The kernel of the map is \( 1 + \mathcal{P}_v = U^{(1)}_K \), so \( \mathfrak{o}_v^*/U^{(1)}_K \cong (\mathfrak{o}_v/\mathcal{P}_v)^* \). \( U^{(n)}_K \) is the largest ideal in \( \mathcal{P}_v^n = 1 + \pi^n a + \pi^{n+1} b \) for some \( a \in \mathfrak{o}_v \). Consider the map \( U^{(n)}_K \to \mathfrak{o}_v/\mathcal{P}_v : 1 + \pi^n a + \pi^{n+1} b \mapsto a + \mathcal{P}_v \). This is well-defined and is actually a homomorphism. The kernel is when \( a \in \mathcal{P}_v \) and in that case \( 1 + \pi^n a \in \mathcal{P}_v^{n+1} \). That proves \( (1 + \mathcal{P}_v)/(1 + \mathcal{P}_v^{n+1}) \cong \mathfrak{o}_v/\mathcal{P}_v \).

22 Valuation Theory II (10/08)

**Theorem 22.1.** Let \( \mathfrak{o} \) be the ring of algebraic integers in a finite extension \( K/\mathbb{Q} \). If \( v \) is a discrete valuation of \( K \), then \( \mathfrak{o} \subset \mathfrak{o}_v \).

**Proof.** Since \( v(-1) + v(-1) = v(1) = 0 \), \( v(-1) = v(1) = 0 \). For positive \( n \in \mathbb{N} \),

\[ v(n) = v(1 + 1 + \cdots + 1) = v(1) = 0. \]

For negative \( n \in \mathbb{N} \),

\[ v(n) = v(-1 + -1 + \cdots + -1) = v(-1) = 0. \]

So we conclude that \( v(n) \geq 0 \) for all \( n \in \mathbb{N} \). Suppose \( x \in \mathfrak{o} \) and satisfies \( x^n + a_n x^{n-1} + \cdots + a_1 = 0 \) where \( a_1, \ldots, a_n \in \mathbb{Z} \). Then \( x^n = -a_1 x^{n-1} - \cdots - a_n \) and so

\[ v(x^n) = nv(x) \geq \min_{1 \leq j \leq n} (v(a_j) + (n-j)v(x)) \]

\[ \geq \min_{1 \leq j \leq n} ((n-j)v(x)). \]

If \( v(x) < 0 \), then \( nv(x) \geq (n-1)v(x) \), which is a contradiction. Hence \( v(x) \geq 0 \), and so \( x \in \mathfrak{o}_v \). Therefore, \( \mathfrak{o} \subset \mathfrak{o}_v \). \( \square \)
Theorem 22.2. If \( \mathfrak{o} \) is a Dedekind domain and \( v \) is a valuation such that \( \mathfrak{o} \subset \mathfrak{o}_v \), then

(i) \( p_v = \mathcal{P}_v \cap \mathfrak{o} \) is a prime ideal in \( \mathfrak{o} \),

(ii) \( p_v \mathfrak{o}_v = \mathcal{P}_v \),

(iii) \( \mathfrak{o}/p_v \cong \mathfrak{o}_v/\mathcal{P}_v \).

We first give an example to illustrate Theorem 22.2, then give the proof.

Example 22.3. \( \mathfrak{o} = \mathbb{Q} \), valuations correspond to prime numbers \( p \), where \( v(p) \) equals the exponent of \( p \) in the prime factorization of \( x \in \mathbb{Q}^* \). Then

\[
\mathbb{Z}_v = \{ \text{all fractions } \frac{r}{s} \text{ where } p \nmid s \},
\]

\[
\mathcal{P}_v = \{ \text{all fractions } \frac{r}{s} \text{ where } p \mid s, p|r \},
\]

\[
\mathbb{Z}_v/\mathcal{P}_v \cong \mathbb{Z}/p\mathbb{Z}.
\]

Proof of part (i) of Theorem 22.2 Suppose \( a, b \in \mathfrak{o} \) and \( ab \in \mathfrak{p}_v = \mathcal{P}_v \cap \mathfrak{o} \). We know that \( \mathfrak{o} \subset \mathfrak{o}_v \), so \( v(a) \geq 0, v(b) \geq 0 \). Since \( ab \in \mathfrak{p}_v \), \( v(ab) = v(a) + v(b) \geq 1 \). So \( v(a) \geq 1 \) or \( v(b) \geq 1 \) since \( v(a), v(b) \in \mathbb{Z}_{\geq 0} \). That proves \( \mathfrak{p}_v \) is a prime ideal in \( \mathfrak{o} \).

Example 22.4 (Example of \( v \) where \( \mathfrak{o} \not\subset \mathfrak{o}_v \)). Let \( F \) be a field, \( K = F(x) \) be a field of rational functions over \( F \), then \( \mathfrak{o} = F[x] \) is the ring of polynomials over \( F \) which is a PID. The prime ideals \( \mathfrak{p} \) of \( \mathfrak{o} \) corresponds to monic irreducible polynomials \( f(x) \in F[x] \). So these correspond to all valuations \( v \) where \( \mathfrak{o}_v \supset \mathfrak{o} \), by previous theorem. There is one more valuation defined by

\[
v_\infty : K^* \to \mathbb{Z}
\]

\[
\frac{f(x)}{g(x)} \mapsto -\deg(f) + \deg(g)
\]

for \( f, g \in F[x] \). By definition,

\[
v_\infty \left( \frac{f(x)}{g(x)} \cdot \frac{r(x)}{s(x)} \right) = -\deg(f(x)) - \deg(r(x)) + \deg(g(x)) + \deg(s(x))
\]

\[
= v_\infty \left( \frac{f(x)}{g(x)} \right) + v_\infty \left( \frac{r(x)}{s(x)} \right),
\]

\[
v_\infty \left( \frac{f(x)}{g(x)} + \frac{r(x)}{s(x)} \right) = v_\infty \left( \frac{f(x)s(x) + r(x)g(x)}{g(x)s(x)} \right)
\]

\[
= -\deg(f(x)s(x) + r(x)g(x)) + \deg(g(x)) + \deg(s(x))
\]

\[
\geq -\max \{ \deg(f(x)s(x)), \deg(r(x)g(x)) \}
\]

\[
= \min \{ -\deg(f(x)) + \deg(g(x)), -\deg(r(x)) + \deg(s(x)) \}
\]

\[
= \min \{ v_\infty \left( \frac{f(x)}{g(x)} \right), v_\infty \left( \frac{r(x)}{s(x)} \right) \}.
\]
Let \( f(x) = -1, \deg\left(\frac{1}{x}\right) = 1, \) and \( \frac{1}{x} \not\in \mathfrak{a}. \) Moreover, we have the following sum formula

\[
v_\infty \left( \frac{f(x)}{g(x)} \right) + \sum_{\text{prime } p(x)} v_p \left( \frac{f(x)}{g(x)} \right) \cdot \deg(p(x)) = 0.
\]

### 23 Valuation Theory III (10/10)

**Proof of part (ii) of Theorem 22.2** \( \mathfrak{p}_v \mathfrak{o}_v \) is an ideal of \( \mathfrak{o}_v. \) Because \( \mathfrak{o}_v. \) a discrete valuation domain, \( \mathfrak{p}_v \mathfrak{o}_v = \mathcal{P}_v^e \) for some \( e \geq 1. \) Since \( \mathfrak{p}_v \) is a prime ideal of \( \mathfrak{o}, \) we can define a valuation \( v_\mathfrak{p}: K^* \to \mathbb{Z} \) by \( v_\mathfrak{p}(x) = n \) where \( x \mathfrak{o} \) is a product of \( \mathfrak{p}_v^n \) and other prime ideal powers. \( v_\mathfrak{p} \) is surjective on \( \mathbb{Z} \) because \( \mathfrak{p}_v^n \neq \mathfrak{p}_v^{n+1}. \)

We claim that for \( z \in K^*, \) if \( v_\mathfrak{p}_z(z) = 0, \) then \( v(z) = 0. \) Here is the proof. Write \( z = \frac{a}{b} \) for some \( a, b \in \mathfrak{o}. \) Then \( a \mathfrak{o} = \mathfrak{p}_v^e a \) and \( b \mathfrak{o} = \mathfrak{p}_v^f b \) for some ideal \( a, b \) with \( \mathfrak{p}_v \nmid a, \mathfrak{p}_v \mid b. \) The same power occurs because \( v_\mathfrak{p}_z(z) = 0 = v_\mathfrak{p}_v(a) - v_\mathfrak{p}_v(b). \) Pick \( c \in \mathfrak{p}_v^{-l}\mathfrak{p}_v^{-l+1}. \)

Then \( ca \in (\mathfrak{p}_v^{-l}\mathfrak{p}_v^{-l+1}) = a\mathfrak{p}_v. \) That proves \( v_\mathfrak{p}(ca) = 0. \) Similarly, \( v_\mathfrak{p}(cb) = 0. \)

Now pick \( x \in \mathfrak{o}, x \neq 0. \) Then \( v_\mathfrak{p}_z(x) = l \geq 0. \) Then \( x \mathfrak{o} = \mathfrak{p}_v^e a \) for some ideal \( a \) with \( \mathfrak{p}_v \nmid a. \) So there exists \( \alpha \in a, \) \( \alpha \not\in \mathfrak{p}_v, \alpha \in \mathfrak{o}. \) By the previous claim, \( \alpha \mathfrak{o} = 0. \) Then \( \alpha \mathfrak{o}_v = \mathfrak{o}_v, \) then \( \alpha \mathfrak{o}_v = \mathfrak{o}_v. \) So \( x \mathfrak{o}_v = \mathfrak{p}_v^e \mathfrak{o}_v = \mathfrak{p}_v^f \mathfrak{o}_v = (\mathfrak{p}_v \mathfrak{o}_v)^l = (\mathcal{P}_v^e)^l = \mathcal{P}_v^e. \) That proves \( v(x) = el = ev_\mathfrak{p}_z(x). \) Since \( v(K^*) = \mathbb{Z} \), we must have \( e = 1. \)

**Proof of part (iii) of Theorem 22.2** By the Second Homomorphism Theorem, we have

\[
\mathfrak{o}/\mathfrak{p}_v = \mathfrak{o}/(\mathfrak{o} \cap \mathcal{P}_v) \cong (\mathfrak{o} + \mathcal{P}_v)/\mathcal{P}_v.
\]

We claim that \( \mathfrak{o} + \mathcal{P}_v = \mathfrak{o}_v. \) Suppose \( z \in \mathfrak{o}_v, \) we have \( z = \frac{a}{b} \) where \( a, b \in \mathfrak{o}. \) If \( v(z) > 0, \) then \( z \in \mathcal{P}_v, \) we are done. If \( v(z) = 0, \) then by previous argument \( z = \frac{a}{b} \) for some \( a, b \in \mathfrak{o}/\mathfrak{p}_v. \) \( a, b \) correspond to non-zero elements in \( \mathfrak{o}/\mathfrak{p}_v \) which is a field. So there exists \( c \in \mathfrak{o} \) such that \( bc = 1 \) (mod \( \mathfrak{p}_v). \) So \( bc - 1 \in \mathfrak{p}_v. \) Then \( z = \frac{a}{b} = (\frac{a}{b} - ac) + ac \) with \( ac \in \mathfrak{o}, \) and \( \frac{a}{b} - ac = \frac{a(1-bc)}{b}. \) Since \( 1 - bc \in \mathfrak{p}_v \subset \mathcal{P}_v, \) we have \( v\left(\frac{a(1-bc)}{b}\right) \geq 1 \) and thus \( \frac{a(1-bc)}{b} \in \mathcal{P}_v. \) So \( z \in \mathfrak{o} + \mathcal{P}_v. \)

### 24 Valuations of a Function Field (10/13)

Let \( F \) be a field, \( K = F(x) \) be the rational function field over \( F, \mathfrak{o} = F[x] \) be the polynomial ring over \( F. \)

We consider valuations of \( K. \) For any prime ideal \( \mathfrak{p} \subset \mathfrak{o}, \)

\[
v_\mathfrak{p}(x) = \text{exponent of } \mathfrak{p} \text{ in prime factorization of } x \mathfrak{o}, \text{ for } x \neq 0,
\]
\[ v_\infty(x) = -\deg(f) + \deg(g), \text{ for } f, g \in F[x] = \mathfrak{o}. \]

If \( 0 \neq f(x) \in F[x] \) factors as
\[ f(x) = up_1(x)^{a_1} \cdots p_k(x)^{a_k} \]
for \( u \in F^* \), where \( p_j(x) \) are irreducible monic polynomials which are distinct, then
\[ v_{p_j}(f(x)) = a_j \]
and
\[ v_\infty(f(x)) = -\deg(f(x)) = -\sum_{j=1}^{k} a_j \deg(p_j(x)), \]
i.e.,
\[ v_\infty(f) + \sum_{j=1}^{k} v_{p_j}(f) \deg(p_j(x)) = 0. \]

Define \( \deg(v_\infty) = 1 \), then
\[ \sum_{\text{all valuations } v} v(f) \deg(f) = 0 \]
for all \( f \in K = F(x) \).

**Theorem 24.1.** The set of all valuations on \( K = F(x) \) such that \( v(F^*) = 0 \) consists of \( v_\infty \) and all \( v_{p} \) for irreducible monic polynomials \( p \in F[x] \).

To prove Theorem 24.1 we need the following lemma.

**Lemma 24.2.** If \( v(a) < v(b) \), then \( v(a + b) = v(a) \).

**Proof.** Since \( v(\frac{b}{a}) = v(b) - v(a) \geq 1 \), so \( \frac{b}{a} \in \mathcal{P}_v \). So \( 1 + \frac{b}{a} \in 1 + \mathcal{P}_v \subset \mathfrak{o}_v \mathcal{P}_v = \mathfrak{o}_v^* \). So \( v(1 + \frac{b}{a}) = 0 \). Then
\[ v(a + b) = v(a(1 + \frac{b}{a})) = v(a) + v(1 + \frac{b}{a}) = v(a). \]

**Proof of Theorem 24.1** If \( v(x) \geq 0 \), then \( v(F[x]) \geq 0 \), and so \( \mathfrak{o} = F[x] \subset \mathfrak{o}_v \). By our previous theorem, \( v = v_p \) for some monic irreducible polynomial \( p \in F[x] \). (Note that for any two irreducible polynomials \( p \neq q \in F[x] \), \( v_p(p) = 1, v_p(q) = 0 \) and \( v_q(p) = 0, v_q(q) = 1 \). So \( v_p \neq v_q \).) If \( v(x) = \alpha < 0 \), then \( v(x^n) = n\alpha, \forall n \in \mathbb{Z} \). So for \( f(x) = a_0x^n + \cdots + a_n \in F[x] \) with \( a_0 \in F^* \), \( v(f(x)) = v(a_0x^n) = -n\alpha \) by Lemma 24.2. Hence
\[ v\left(\begin{array}{c} f(x) \\ g(x) \end{array}\right) = (-\deg(f) + \deg(g))\alpha \in \alpha \mathbb{Z}. \]

Since \( v \) maps \( K^* \) onto \( \mathbb{Z} \), we have \( \alpha = -1 \). Thus \( v\left(\begin{array}{c} f(x) \\ g(x) \end{array}\right) = -\deg(f) + \deg(g) \). \( \square \)
Definition 24.3. An absolute value on a field $K$ is a function $|\cdot| : K \to [0, \infty)$ satisfying
(i) $|x| = 0$ iff $x = 0$;
(ii) $|xy| = |x||y|$;
(iii) $|x + y| \leq |x| + |y|$

Remark 24.4. (i) Trivial absolute value is an absolute value $|\cdot|$ such that $|x| = 1$ for all $x \in K^*$. From now on we assume our absolute values to be non-trivial.
(ii) If $v$ is a discrete valuation on $K$ and $\lambda$ is any number with $0 < \lambda < 1$, then
$$|x|_v = \begin{cases} 
\lambda^v(x) & \text{if } x \neq 0 \\
0 & \text{if } x = 0
\end{cases}$$
is an absolute value on $K$.
(iii) If $|x + y| \leq \max(|x|, |y|)$, $|\cdot|$ is called ultrametric or nonarchimedean. If not, $|\cdot|$ is called archimedean.
(iv) If $v$ is a discrete valuation, then $|\cdot|_v$ is nonarchimedean.

Definition 24.5. Two absolute values $|\cdot|, |\cdot|'$ on $K$ are equivalent iff $\exists a > 0$ such that $|x|' = |x|^a$ for all $x \in K$.

25 Ostrowski’s Theorem I (10/15)

Theorem 25.1. Two absolute values $|\cdot|, |\cdot|'$ on a field $K$ are equivalent iff
$$\{x \in K : |x| > 1\} \subset \{x \in K : |x|^a > 1\}.$$ 

Proof. ($\Rightarrow$) If $|x'| = |x|^a$ for some $a > 0$ for all $x \in K$, then if $|x| > 1$, then $|x'| = |x|^a > 1$.
($\Leftarrow$) Since we assume $|\cdot|$ is nontrivial, there exists $x_0$ with $|x_0| > 1$. So by assumption, $|x_0| > 1$, too. Then $|x_0'| = |x_0|^a$ for some $a > 0$.
For any other $x \neq 0$ in $K$, suppose $|x| < |x|^a$. We’ve given that if $|x| > 1$, then $|x'| > 1$. So if $|x^{-1}| > 1$, then $|x^{-1}|' > 1$. So if $|x| < 1$, then $|x|' < 1$. Now take logs, we have
$$\log |x_0|' = a \log |x_0|,$$
and
$$\log |x|' < a \log |x|.$$
We can find a rational number $\frac{m}{n} \in \mathbb{Q}$ with $m, n$ integers and $n > 0$ such that
$$\log |x|' < \frac{m}{n} \log |x_0|' < a \log |x|$$
(by density of $\log |x_0|' \mathbb{Q}$ in $\mathbb{R}$). So
$$n \cdot \log |x|' - m \cdot \log |x_0|' < 0.$$
So
\[ |x^n x_0^{-m}|' < 1. \]
Also, we have
\[ na \cdot \log |x| - m \cdot \log |x_0|' > 0, \]
then
\[ na \cdot \log |x| - ma \cdot \log |x_0| > 0 \]
since \( |x_0|' = |x_0|^a \). Hence,
\[ n \cdot \log |x| - m \cdot \log |x_0| > 0. \]
So
\[ |x^n x_0^{-m}| > 1. \]
This contradicts the inclusion \( |y|' > 1 \Rightarrow |y| < 1 \) proved earlier. A similar contradiction proves \( |x|' > |x|^a \) is also impossible. Therefore, \( |x| = |x|^a \) for all \( x \in K^* \). \( \square \)

**Theorem 25.2** (Ostrowski's Theorem (Acta Mathematica, 1916)). *Every absolute value of \( \mathbb{Q} \) is equivalent to exactly one of \( | \cdot | \mathbb{R} \) (ordinary absolute value on \( \mathbb{R} \)) or \( | \cdot |_p \) for some prime \( p \) in \( \mathbb{Z} \) where \( |x|_p = p^{-v_p(x)} \) (the \( p \)-adic absolute value).

**26 Ostrowski’s Theorem II (10/17)**

**Proof of Theorem 25.2** Assume first that \( |n| \leq 1 \) for all \( n \in \mathbb{Z} \). The nontriviality of \( | \cdot | \) implies that there exists a prime \( p \) with \( |p| < 1 \) (if not, then by prime factorization \( |x| = 1 \) for all \( x \in K^* \)). Suppose there is another prime \( q \) with \( |q| < 1 \). Choose integers \( a, b \geq 1 \) with \( |p|^a < \frac{1}{2}, |q|^b < \frac{1}{2} \). Then there are integers \( m, n \) with \( mp^a + nq^n = 1 \) since \( p^a \) and \( q^b \) are relatively prime. So
\[ 1 = |mp^a + nq^b| \leq |m||p|^a + |n||q|^b < 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1. \]
That contradiction proves no such prime \( q \) exists. So \( |q| = 1 \) for all prime \( q \neq p \). Then clearly \( |x| = |p|^{v_p(x)} \) by prime factorization for all \( x \in K^* \). Since \( |p| < 1 \), \( |p| = p^{-a} \) for some \( a > 0 \). Then \( |x| = |x|^a_p \).

Now assume \( |n| > 1 \) for some integer \( n > 1 \). Then \( |n| = n^\alpha \) for some \( \alpha > 0 \). It is sufficient to prove that \( |m| = m^\alpha \) for all integers \( m \geq 1 \). First, \( |m| = |1 + 1 + \cdots + 1| \leq 1 + 1 + \cdots + 1 = m \) for all integers \( m \geq 1 \). In particular, \( n^\alpha \leq n \). So \( \alpha \leq 1 \). Write
\[ m = c_0 + c_1 n + c_2 n^2 + \cdots + c_k n^k \]
for integers \( 0 \leq c_j < n, 0 \leq j < k, \) and \( 1 \leq c_k < n \). So
\[ |m| \leq \sum_{j=0}^k |c_j| n^j \leq \sum_{j=0}^k c_j n^j \]
\[ \leq (n-1) \sum_{j=0}^k n^{j\alpha} = (n-1) \cdot \frac{n^{(k+1)\alpha} - 1}{n^\alpha - 1}. \]

37
Only $k$ depends on $m$. That proves

$$|m| \leq c \cdot n^k \leq c \cdot m^\alpha$$

for all $m \geq 1$, for some constant $c > 0$. Replace $m$ by $m^r$ for an integer $r \geq 1$. Then $|m^r| \leq c \cdot m^{r\alpha}$. So $|m| \leq c^{\frac{r}{r}} \cdot m^\alpha$. Then $\lim_{r \to \infty} c^{\frac{r}{r}} = 1$. Then that proves

$$|m| \leq m^\alpha$$

for all integers $m \geq 1$.

To prove $|m| \geq m^\alpha$, write

$$m = c_0 + c_1 n + c_2 n^2 + \cdots + c_k n^k$$

for integers $0 \leq c_j \leq n$, $0 \leq j < k$, and $1 \leq c_k < n$. Then $m < n^{k+1}$. Also $m \geq n^k$. Let $b = n^{k+1} - m > 0$. Then

$$n^{k+1} - m \leq n^{k+1} - n^k.$$

So $|b| \leq b^\alpha$ by our above argument. Then

$$|b| \leq (n^{k+1} - n^k)^\alpha.$$

On the other hand, by the Triangle Inequality, we have

$$|m| \leq |n^{k+1}| - |b| \leq n^{(k+1)\alpha} - (n^{k+1} - n^k)^\alpha$$

$$= n^{(k+1)\alpha} \left(1 - (1 - \frac{1}{n})^\alpha\right)$$

$$\geq c' \cdot n^{(k+1)\alpha}$$

$$\geq c' \cdot m^\alpha$$

where $c'$ is a constant independent of $m$. Replace $m$ by $m^r$ for an integer $r \geq 1$. Then $|m^r| \geq c' \cdot (m^r)^\alpha$, so $|m|^r \geq c' \cdot m^{r\alpha}$. Hence $|m| \geq (c')^{\frac{1}{r}} \cdot m^\alpha$. Since $\lim_{r \to \infty} (c')^{\frac{1}{r}} = 1$, this proves $|m| \geq m^\alpha$.

**Theorem 26.1** (Ostrowski’s Theorem for Algebraic Number Fields $K/\mathbb{Q}$). If $K/\mathbb{Q}$ is a finite extension, then every absolute value $| \cdot |$ on $K$ is equivalent to a $p$-adic absolute value for a unique prime ideal $p$ in $\mathfrak{o}_K$, or is equivalent to an absolute value coming from a real or complex embedding of $K$.

**Definition 26.2.** Equivalence classes of absolute values of $K$ are called *places* of $K$.

An absolute value $| \cdot |$ on $K$ defines a topology on $K$ by means of the basis of neighborhoods:

$$B(a, r) = \{ x \in K | |x - a| < r \}$$

for all $a \in K$, $r > 0$, $r \in \mathbb{R}$.

$U \subset K$ is open if for every $a \in U$, there exists $r > 0$ such that $B(a, r) \subset U$. Addition, multiplication, and $| \cdot |$ are all continuous on $K$ relative to this topology.
Theorem 26.3. If $|n| \leq 1$ for all $a \in \mathbb{Z}$, where $\mathbb{Z}$ is the image of $\mathbb{Z}$ in $K$, then $|\cdot|$ is ultrametric, i.e., $|x + y| \leq \max(|x|, |y|)$.

Proof. First, we prove $|1 + a| \leq 1$ for all $a \in K$ with $|a| \leq 1$. By the Binomial Theorem,

$$|1 + a|^m = \left| \sum_{j=0}^{m} \binom{n}{j} a^j \right| \leq \sum_{j=0}^{m} |\binom{n}{j}| |a|^j \leq \sum_{j=0}^{m} |a|^j \leq m + 1.$$ 

So $|1 + a| \leq (m + 1)^{\frac{1}{m}}$. Since $\lim_{m \to \infty}(m + 1)^{\frac{1}{m}} = 1$, we have $|1 + a| \leq 1$.

If $x \neq 0$ and $|y| \leq |x|$, then

$$|x + y| = |x| \left| 1 + \frac{y}{x} \right| \leq |x|$$

by the above result, and so by symmetry,

$$|x + y| \leq \max(|x|, |y|), \forall x, y \in K.$$ 

\[
\square
\]

27 Weak Approximation Theorem (10/20)

Theorem 27.1 (Weak Approximation Theorem). Let $|\cdot|_1, \ldots, |\cdot|_n$ be inequivalent absolute values on a field $K$. Let $K_j$ be the field with the topology derived from $|\cdot|_j$. Embed $K \hookrightarrow K_1 \times \cdots K_n$ along diagonal:

$$x \mapsto (x, \cdots, x).$$

Then the image of $K$ is dense in $\prod_{j=1}^{n} K_j$, i.e., for any $\varepsilon > 0$, and any $x_1, \cdots, x_n \in K$, $\exists y \in K$ such that $|y - x_j|_j < \varepsilon$ for $1 \leq i \leq n$.

Before we prove Weak Approximation Theory, let’s see an example.

Example 27.2 (A special case). If $K$ is the field of fractions of a Dedekind domain $\mathfrak{o}$ and if $|\cdot|_i$ corresponds to a prime ideal $p_i$ in $\mathfrak{o}$, then the Chinese Remainder Theorem says that for any $M > 0$ and any $y_1, \cdots, y_n \in \mathfrak{o}$, $\exists x$ with $x \equiv y_j \pmod{p_j^M}$, that’s equivalent saying $|x - y_j| \leq (N_{p_j})^{-M}$. So if we choose $M$ large enough so that $(N_{p_j})^{-M} < \varepsilon$, then this proves a special case of Weak Approximation Theorem.

Remark 27.3. Weak Approximation Theorem involves any absolute values including archimedean ones.

Lemma 27.4. Suppose $|\cdot|_1, \cdots, |\cdot|_n$ are inequivalent absolute values on a field $K$, then there exists $a \in K$ such that $|a|_1 > 1$ and $|a|_i < 1$ for all $2 \leq i \leq n$. 

39
Proof. We prove by induction on \( n \).

The first case is \( n = 2 \). Since \(| \cdot |_1, | \cdot |_2\) are inequivalent, by our earlier theorem,

\[
\{ |x|_1 < 1 \} \not\subseteq \{ |x|_2 < 1 \}
\]

and

\[
\{ |x|_2 < 1 \} \not\subseteq \{ |x|_1 < 1 \}.
\]

So there exists \( x, y \neq 0 \) such that

\[
|x|_1 < 1, |x|_2 \geq 1
\]

and

\[
|y|_2 < 1, |y|_1 \geq 1.
\]

Then

\[
\left| \frac{x}{y} \right|_1 < 1 < \left| \frac{x}{y} \right|_2.
\]

That proves the \( n = 2 \) case.

Assume it is true for \( n \) absolute values for some \( n \geq 2 \). Assume there is a \( b \) with

\[
|b|_1 > 1, |b|_i < 1 \text{ for } i = 2, \ldots, n.
\]

By \( n = 2 \) case, there exists \( c \) with

\[
|c|_1 > 1, |c|_{n+1} < 1.
\]

If \(|b|_{n+1} < 1\), then \( a = b \) works. So assume \(|b|_{n+1} \geq 1\). If \(|b|_{n+1} = 1\), take \( a = cb^r \) where \( r \) is chosen large enough so that for \( 2 \leq i \leq n\),

\[
|cb^r|_i = |c|_i |b|^r_i < 1
\]

which we can do because \(|b|_i < 1\). Also

\[
|cb^r|_1 = |c|_1 |b|^r_1 > 1,
\]

\[
|cb^r|_{n+1} = |c|_{n+1} |b|^r_{n+1} = |c|_{n+1} < 1.
\]

So \( cb^r \) works. Finally, assume \(|b|_{n+1} > 1\). Then take

\[
a = \frac{cb^r}{1 + b^r}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]

Note that since \(|b|_1 > 1\), \( \lim_{r \to \infty} \frac{|b|^r_1}{1 + b^r_1} = 1 \), we can choose \( r \gg 0 \) such that \(|a|_1 > 1\) because \(|c|_1 > 1\) for \( 2 \leq i \leq n\),

\[
|a|_i \leq \frac{|c|_i |b|^r_i}{1 - |b|^r_i}
\]

for some integer \( r > 0 \). Then

\[
|a|_1 = \frac{|c|_1 |b|^r_1}{1 + b^r_1} \geq \frac{|c|_1 |b|^r_1}{1 + |b|^r_1}.
\]
because $|b|_i < 1$, and

$$
\lim_{r \to \infty} \frac{|b|^r_i}{1 - |b|^r_i} = 0.
$$

So we can choose $r \gg 0$ so that $|a|_i < 1$. Moreover,

$$
|a|_{n+1} \leq \frac{|c|_{n+1}|b|^r_{n+1}}{|b|^r_{n+1} - 1}
$$

and

$$
\lim_{r \to \infty} \frac{|b|^r_{n+1}}{|b|^r_{n+1} - 1} = 1
$$

because $|b|_{n+1} > 1$. Since $|c|_{n+1} < 1$, we can choose $r \gg 0$ so that $|a|_{n+1} < 1$. \qed

**Proof of Theorem 27.1** By Lemma 27.4 choose $a_j \in K$ so that $|a_j|_i > 1$, $|a_j|_i < 1$ for $i \neq j$. Let

$$
y = \sum_{j=1}^{n} \frac{a_j^r x_j}{1 + a_j^r}.
$$

For $r \gg 0$, we will verify that this $y$ works.

$$
|y - x_i|_i \leq \sum_{j \neq i} \left| a_j^r x_j \right| \frac{1}{1 + a_j^r} + \left| a_i^r x_i \right| \frac{1}{1 + a_i^r}
$$

$$
\leq \sum_{j \neq i} \left| a_j^r \right| \left| x_j \right|_i \frac{1}{1 - \left| a_j \right|_i^r} + \left| x_i \right|_i \frac{1}{1 - \left| a_i \right|_i^r} \left( \text{since } |a_j|_i < 1, |a_i|_i > 1 \right).
$$

Since $\lim_{r \to \infty} \frac{|a_j|_i^r}{1 - |a_j|_i^r} = 0$ and $\lim_{r \to \infty} \frac{1}{1 - |a_j|_i^r} = 0$, we can choose $r \gg 0$ such that $|y - x_i|_i < \varepsilon$. \qed

**Corollary 27.5.** Suppose $K/\mathbb{Q}$ is a finite extension. Suppose $|·|_1, \ldots, |·|_m$ are inequivalent real absolute values:

$$
|x|_i = |x^{\sigma_i}|_\mathbb{R} \text{ for distinct embeddings } \sigma_i : K \hookrightarrow \mathbb{R}.
$$

Let each $\varepsilon_i(1 \leq i \leq m)$ be $\pm 1$. Then there exists $x \in K$ such that $\text{sign}(\sigma_i(x)) = \varepsilon_i$.

**28 Completions of Valued Fields I (10/22)**

**Definition 28.1.** Let $K$ be a field with an absolute value $|·|$. A sequence $\{a_n\}_{n=1}^{\infty}$ with $a_n \in K$ is Cauchy if $\forall \varepsilon > 0, \exists N > 0$ with $|a_n - a_m| < \varepsilon$ for $n > m \geq N$. 


51
A Cauchy sequence \( \{a_n\}_{n=1}^{\infty} \) has a limit \( l \in K \) if \( \lim_{n \to \infty} |a_n - l| = 0 \). \( \{a_n\} \) is a null sequence if \( l = 0 \). We say \( K \) is complete if every Cauchy sequence has a limit in \( K \).

The set of Cauchy sequences forms a commutative ring \( R \) with a 1 = \( \{1\} \) with operations:

\[
\{a_n\} + \{b_n\} = \{a_n + b_n\},
\]

\[
\{a_n\}\{b_n\} = \{a_nb_n\}.
\]

The set \( \mathfrak{N} \) of null sequences forms an ideal in \( R \). If \( \{a_n\} \in R \setminus \mathfrak{N} \), then there exists \( \varepsilon > 0 \) such that \( |a_n| \geq \varepsilon \) for infinitely many \( n \). Choose \( N \) such that \( |a_n - a_m| < \frac{\varepsilon}{2} \) for \( n > m \geq N \). Choose \( N \) with \( |a_N| \geq \varepsilon \). Then

\[
|a_n| = |a_n - a_N + a_N| \\
\geq |a_N| - |a_n - a_N| \\
\geq \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2}
\]

for all \( n \geq N \). So \( a_n \neq 0 \). Now choose \( \{b_n\} \) with \( b_n = \frac{1}{a_n} \) for \( n \geq N \). Then \( \{b_n\} \) is Cauchy. Then

\[
\{a_n\}\{b_n\} = \{1\} + \text{some sequence in } \mathfrak{N}.
\]

That proves \( \mathfrak{N} \) is maximal (if we add any \( \{a_n\} \in R \setminus \mathfrak{N} \) to \( \mathfrak{N} \), then \( 1 = \{1\} \in \mathfrak{N} \)). Then \( \overline{K} = R \setminus \mathfrak{N} \) is a field.

**Theorem 28.2.**

(i) \( \overline{K} \) has an absolute value

\[
\|\{a_n\}\| = \lim_{n \to \infty} |a_n|.
\]

(ii) \( \overline{K} \) is complete with respect to \( \|\cdot\| \).

(iii) There is an embedding

\[
K \hookrightarrow \overline{K} \\
\alpha \mapsto \{\alpha\} + \mathfrak{N}
\]

satisfying \( \|\{\alpha\}\| = |\alpha| \).

(iv) The image of \( K \) is dense in \( \overline{K} \).

(v) If \( \overline{K} \) is a complete field containing \( K \) as a dense subset, then \( \overline{K} \) is isomorphic to \( \overline{K} \), with \( K \) mapping to \( \overline{K} \) by the identity.

If \( K/\mathbb{Q} \) is a finite extension, and \( \sigma : K \hookrightarrow \mathbb{R} \) is a real embedding, then the completion of \( K \) relative to \( |\cdot|_{\mathbb{R}} \) is isomorphic to \( \mathbb{R} \). For \( \sigma : K \hookrightarrow \mathbb{C} \) which are nonreal, the completion of \( K \) relative to \( |\cdot|_{\mathbb{C}} \) is always isomorphic to \( \mathbb{C} \).

Suppose \( o \) is a Dedekind domain and not a field, \( K \) is its field of fractions, \( p \) is a nonzero prime ideal of \( o \). Define \( |x|_p = \lambda^p \) with some \( 0 < \lambda < 1 \). \( |\cdot|_p \) is an absolute value on \( K \). Then \( K_p \) is the completion of \( K \) relative to \( |\cdot|_p \) (p-adic field). The valuation \( v_p \) extends to
$K_p$ so that $|x|_p = \lambda^{|x|}(x)$. Then for any Cauchy sequence $\{a_n\}$ in $K$, $\lim_{n \to \infty} |a_n|_p$ exists. 
\{\{x\}_p \mid x \in K\} \subset \{\lambda^n \mid n \in \mathbb{Z}\} \cup \{0\}$ and since this is a discrete subset of $(0, \infty)$, the only possible limits of sequence of these are \{\{\lambda^n \mid n \in \mathbb{Z}\} \cup \{0\}$. Then $\lim_{n \to \infty} |a_n| = 0$ or $\lambda^m$ for some integer $m \in \mathbb{Z}$. Then if $x \neq 0$, define $v_p(x) = m$. Then $v_p$ is a valuation on $\overline{K}$. Then denote $K_p$ as $K_v$, and $\sigma_v = \{x \in K_v : |x|_v \leq 1\}$ as the valuation ring, $\mathcal{P}_v = \{x \in K_v : |x|_v < 1\}$.

29 Completions of Valued Fields II, Inverse Limits (10/27)

Let $K$ be a field of fractions of a Dedekind domain $\sigma$, $v$ be a valuation on $K$, and $K_v$ be the completion of $K$ with respect to $v$. Suppose $\{a_n\}$ is Cauchy in $K$, representing $x \in K_v$. Let

$$L_0 = \liminf_{n \to \infty} |a_n|_v, L_1 = \limsup_{n \to \infty} |a_n|_v.$$ 

For $\varepsilon > 0$, there exists $N > 0$ such that $|a_n - a_m|_v < \frac{\varepsilon}{3}$ for all $n > m \geq N$. There exists $n, m \geq N$ such that $|a_n|_v \leq L_0 + \frac{\varepsilon}{3}$ and $|a_m|_v \geq L_1 - \frac{\varepsilon}{3}$. Then

$$\frac{\varepsilon}{3} - |a_n - a_m|_v \geq |a_m|_v - |a_n|_v \geq L_1 - \frac{\varepsilon}{3} - (L_0 + \frac{\varepsilon}{3}) = L_1 - L_0 - \frac{2\varepsilon}{3}.$$ 

Thus $L_1 - L_0 < \varepsilon$ for any $\varepsilon > 0$. Hence $L_1 = L_0$ and $\lim_{n \to \infty} |a_n|_v$ exists.

If $v$ is a discrete valuation, then $|x|_v = \lambda^{|x|}(x)$ for some $0 < \lambda < 1$. Since $\{\lambda^n \mid n \in \mathbb{Z}\}$, then $\lim_{n \to \infty} |a_n| = 0$ or $\lambda^n$ for some $n \in \mathbb{Z}$. The first case happens if and only if $x = 0$. If $x \neq 0$, then $\lim_{n \to \infty} |a_n| \neq 0$ by definition of Null Cauchy sequence. Then $\lim_{n \to \infty} |a_n|$ is in the closure of $\{\lambda^n \mid n \in \mathbb{Z}\}$. The only limit point of that set not in the set is $0$. Then $\lim_{n \to \infty} |a_n| = \lambda^m$ for some $m$. Define $v(x) = m$, then there exists $N > 0$ such that $|a_n|_v = \lambda^m$ for all $n \geq N$.

Let

$$\sigma_v = \text{valuation ring of } v \text{ in } K_v$$

$$= \{x \in K_v : |x|_v \leq 1\}$$

$$= \text{closure of } \sigma \text{ in } K_v$$

and

$$\mathcal{P}_v = \text{unique prime ideal in } \sigma_v$$

$$= \{x \in K_v : |x|_v < 1\}$$

$$= \{x \in K_v : |x|_v \leq \lambda\}$$

$$= \text{closure of } p \text{ in } K_v.$$

Theorem 29.1.

$$\sigma_v/\mathcal{P}_v^r \cong \sigma/p^r$$

for $r \geq 1$. 43
Proof. Consider the map
\[
\mathfrak{o}/p^r \to \mathfrak{o}/P_v^r
\]
\[
x + p^r \mapsto x + P_v^r.
\]
Since \(| \cdot |_v\) is discrete in \(K_v\),
\[
P_v^r = \{ x \in K_v : |x|_v \leq \lambda^r \}.
\]
Since \(v\) is an extension of the valuation on \(K\), \(p^r \subset P_v^r\). So the map is well-defined.

Suppose \(x \in \mathfrak{o} \cap P_v^r\), then \(x \in p^r\). So the map is injective. Given \(x \in \mathfrak{o}_v\), \(x\) is represented by a Cauchy sequence \(\{a_n\} \subset K\). Also \(|a_n|_v = |x|_v \neq 0\) for \(n \gg 0\). Choose \(0 < \varepsilon < \lambda^r\).

Then there exists \(N > 0\) such that for \(n \geq N\)
\[
|a_n - x|_v < \varepsilon < \lambda^r.
\]
Then \(a_N - x \in P_v^r\). So \(a_N + p^r\) maps to \(x + P_v^r\). That proves the map is surjective.

Example 29.2. \(\mathbb{Z}/p^r\mathbb{Z} \simeq \mathbb{Z}_p/p^r\mathbb{Z}_p\).

Corollary 29.3. If \(q\) is any prime ideal of \(\mathfrak{o}\) with \(q \neq p\), then \(q\mathfrak{o}_v = \mathfrak{o}_v\).

Proof. Since \(q \subset \mathfrak{o}, q\mathfrak{o}_v \subset \mathfrak{o}_v\). Then \(q\mathfrak{o}_v = P_v^r\) for some \(r \geq 0\). Since \(q \neq p\), there exists \(\alpha \in q \setminus p\). Then \(|\alpha|_v = 1\) and hence \(r = 0\).

Now we come to the Inverse Limits.

Suppose we have a sequence of commutative groups: for \(n \geq 1\)
\[
A_n = \mathfrak{o}/p^n
\]
with homomorphisms
\[
\alpha^n_m : A_n \to A_m
\]
for all \(n \geq m \geq 1\), satisfying for \(n \geq m \geq r \geq 1\)
\[
\alpha^n_r = \alpha^m_r \circ \alpha^n_m
\]
where
\[
\alpha^n_m(x + p^n) = x + p^m
\]
which is well-defined because since \(n \geq m, p^n \subset p^m\). To any such inverse system \(\{A_n\}\), there is associated an inverse limit
\[
\mathcal{A} = \lim_{\leftarrow n} A_n = \left\{ (x_n) \in \prod_{n=1}^{\infty} A_n : \alpha^n_m(x_n) = x_m \text{ for } n \geq m \geq 1 \right\}
\]
with natural surjective homomorphisms
\[
\beta_n : \mathcal{A} \to A_n
\]
such that for \(n \geq m \geq 1\), \(\beta_m = \alpha^n_m \circ \beta_n\).
Theorem 29.4. \[ \lim_{n \to -} \mathfrak{o}/p^n \cong \mathfrak{o}_u. \]

**Proof.** Define for \( x \in \mathfrak{o}_u \), the sequence \((a_n)\), \( a_n \in \mathfrak{o}/p^n \) where \( a_n \) is the image of \( x \) under the isomorphism \( \mathfrak{o}_u/P^n \cong \mathfrak{o}/p^n \). Then \((a_n) \in \overline{A} \) and this gives the isomorphism. \( \square \)

Choose \( \pi \in p \setminus p^2 \). So \( |\pi|_v = \lambda \). Let \( R \) be any set of representatives in \( \mathfrak{o} \) for the residue field \( k = \mathfrak{o}/p \). Let \( x \in K_v \), \( x \neq 0 \). Then \( |x|_v = \lambda^{n_1} = |\pi|^{n_1} \) for some \( n_1 \in \mathbb{Z} \). Then \( |x\pi^{-n_1}|_v = 1 \). Then \( x\pi^{-n_1} \in \mathfrak{o}_u \). Choose \( a_1 \in R \) with \( x\pi^{-n_1} = a_1 \) (mod \( p \)). Either \( |x^{-n_1} - a_1|_v = 0 \) or \( |x^{-n_1} - a_1|_v = \lambda^{n_2} = |\pi|^{n_2} \) for some \( n_2 \geq 1 \). Then \( ||x\pi^{-n_1} - a_1|\pi^{-n_2}|_v = 1 \). Choose \( a_2 \in R \) with \((x\pi^{-n_1} - a_1)\pi^{-n_2} = a_2 \) (mod \( p \)). We can continue the process. This gives a unique expansion \[ x = \sum_{m=n}^{\infty} a_m \pi^m \] with every \( a_m \in R \) for all \( x \in K_v \).

### 30 Compactness (10/29)

**Example 30.1.** Here is an example of 2-adic expansion of \(-1\) in \( \mathbb{Q}_2 \). \( R = \{0,1\} \) is a set of representatives for \( \mathbb{Z}/2\mathbb{Z} \). \(-1 \in 1 + 2\mathbb{Z}_2 \), so \( a_0 = 1 \). Then \((-1 - 1)2^{-1} = -1 \in 1 + 2\mathbb{Z}_2 \), so \( a_1 = 1 \), and this pattern repeats forever. This establishes \[ -1 = \sum_{n=0}^{\infty} 2^n. \]

**Example 30.2.** Does a solution to \( x^2 = -1 \) exist in \( \mathbb{Q}_5 \)? The Binomial Series \[ (1 + x)^{\frac{1}{2}} = \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} x^n \]
formally satisfies \((1 + x)^{\frac{1}{n}}\)^2 = 1 + x. Note

\[
\binom{\frac{1}{n}}{n} = \frac{\frac{1}{2} \cdot \left(\frac{1}{2} - 1\right) \cdots \left(\frac{1}{2} - (n - 1)\right)}{n!} = \frac{(-1)^{n-1}(2n - 3)(2n - 1) \cdots 3 \cdot 1}{2^n 
\cdot \frac{n!}{n!(2n - 2)(2n - 4) \cdots 2} = \frac{(-1)^{n-1} \cdot (2n - 2)!}{2^{2n-2} \cdot n! \cdot (n - 1)!} = \frac{(-1)^{n-1} \cdot (2n - 2)}{2^{2n-2} \cdot (n - 1) \cdot \frac{1}{n}} \in \mathbb{Z}_{2^{n-1}}.
\]

So

\[v_p \left( \binom{\frac{1}{n}}{n} \right) \geq -(2n - 1)v_p(2) - v_p(n) \geq -c \cdot \log(n)\]

for \(p = 5\). For \(p = 5\), as long as \(v_p(x) \geq 1\), the series converges, because

\[v_p \left( \binom{\frac{1}{n}}{n} x^n \right) \geq n - c \log(n) \to \infty \text{ as } n \to \infty.
\]

So \((1 - 5)^{1/2} = \sum_{n=0}^{\infty} \binom{\frac{1}{n}}{n} (-5)^n = x\) converges in \(\mathbb{Z}_5\) and this satisfies \(x^2 = 1 - 5 = -4\). So \((\frac{2}{5})^2 = -1\).

Let \(K\) be a complete field with a nonarchimedean absolute value \(\cdot|\cdot\). Then

\[\mathfrak{o} = \{x : |x| \leq 1\}\]

is a subring of \(K\),

\[\mathfrak{p} = \{x : |x| < 1\}\]

is the unique maximal or prime ideal of \(\mathfrak{o}\). We can choose \(\pi \in \mathfrak{p}\backslash \mathfrak{p}^2\). Let \(v = v_\pi\) be the valuation on \(K\).

**Theorem 30.3.** If \(k = \mathfrak{o}/\mathfrak{p}\) is finite, then \(\mathfrak{o}\) is compact with respect to the topology defined by \(|\cdot|\).

Recall that a basis of neighborhoods of \(x \in K\) is \(\{x + \mathfrak{p}^n\}\) for \(n \in \mathbb{Z}\).

**Theorem 30.4.** If \(\{A_n\}\) is a projective sequence of finite abelian groups, then \(\lim_\leftarrow A_n = A\) is compact with respect to the projective topology.
A basis of neighborhoods of 0 in $\mathbb{A}$ is 
$$U_N = \{(a_n) : a_n = 0 \text{ in } A_n \text{ for } n \leq N\}.$$ 
We have 
$$\bigcup_{N=1}^{\infty} U_N = \{0\}.$$ 
A basis of neighborhoods of $a \in \mathbb{A}$ is 
$$\{a + U_N\}.$$ 

Proof of Theorem 30.4. We will prove sequential compactness. Let \(\{x_n\}\) be a sequence in $\mathbb{A}$. We have to show there is a convergent subsequence. There are only finitely many $a_1 \in A_1$, and $\mathbb{A} = \bigcup_{a_1 \in A_1} a_1 + U_1$. So $a_1 + U_1$ contains infinitely many $x_n$ for some $a_1$. Suppose we have $a_n \in A_n$, defined where there are infinitely many $x_n$ in $a_n + U_n$. Then $a_n + U_n$ is the union of $a_{n+1} + U_{n+1}$ where $a_{n+1}$ projects to $a_n$. Since there are only finitely many $a_{n+1}$, one of them $a_{n+1} + U_{n+1}$ has infinitely many $x_n$ in it. That defines $a = (a_n) \in \mathbb{A}$ where $a_n + U_n$ contains infinitely many $x_n$'s. Then there are $n_1 < n_2 < n_3 < \cdots$ such that $x_{n_j} \in a_j + U_j$ for all $j$. Then by definition $\lim_{j \to \infty} x_{n_j} = a$. 

Since $\mathfrak{o} \cong \varprojlim_n \mathfrak{o}/p^n$, that proves $\mathfrak{o}$ is compact.

Remark 30.5. Infinite Galois groups are projective limits. Suppose $K^{sep}$ is the field of all algebraic numbers which are separable over $K$. Then 
$$K^{sep} = \bigcup_{L/K \text{ finite separable}} L = \varprojlim_{L/K \text{ finite separable}} L \quad \text{(direct limit)}.$$ 
Then 
$$\text{Gal}(K^{sep}/K) = \varprojlim_{L/K \text{ finite separable}} \text{Gal}(L/K)$$ 
since for $K \subset L_1 \subset L_2$ we have 
$$\text{Gal}(L_2/K) \to \text{Gal}(L_1/K)$$
forms a projective system of groups. With the projective topology, $\text{Gal}(K^{sep}/K)$ is a compact group. This suggests a relationship between $\text{Gal}(K^{sep}/K)$ and groups like $\mathbb{Z}_p$. Iwasawa Theory is the study of $\mathbb{Z}_p$-Galois extensions over $\mathbb{Q}$.

31 Hensel’s Lemma (10/31)

Theorem 31.1 (Hensel’s Lemma). Let $K$ be a complete field with nonarchimedean absolute value $|\cdot| = |\cdot|_v$, $\mathfrak{o} = \{x \in K : |x| \leq 1\}$, $\mathfrak{p} = \{x \in K : |x| < 1\}$, $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$. Suppose $f(x) \in \mathfrak{o}[x]$. If there is an $a_0 \in \mathfrak{o}$ with 
$$\left| \frac{f(a_0)}{f'(a_0)^2} \right| < 1,$$
then there is a root $\alpha \in \mathfrak{o}$ with $f(\alpha) = 0$ and $|\alpha - a_0| < 1$. 

47
Proof. For $f(x) \in \mathfrak{o}[x]$, $f(x) = \sum_{m=0}^{N} c_m x^m$ where $c_m \in \mathfrak{o}$. Then

$$f(x + \pi^j y) = \sum_{m=0}^{N} c_m (x + \pi^j m)^m$$

$$= \sum_{m=0}^{N} c_m \sum_{k=0}^{m} \binom{m}{k} x^{m-k}(\pi^j y)^k$$

$$= \sum_{k=0}^{N} (\pi^j y)^k \sum_{m=k}^{N} c_m \binom{m}{k} x^{m-k}.$$  

Note that

$$\sum_{m=k}^{N} c_m \binom{m}{k} x^{m-k} = \frac{f^{(k)}(x)}{k!} \in \mathfrak{o}[x].$$

So

$$f(x + \pi^j y) = f(x) + (\pi^j y) f'(x) + (\pi^j y)^2 h(x, \pi y)$$

where $h(x, \pi y) \in \mathfrak{o}[x, y]$. At the beginning we have $\alpha_0$ with

$$|f(\alpha_0)| < |f'(\alpha_0)|^2 \leq 1.$$

If $v(f'(\alpha_0)) = c \geq 0$, then $v(f'(\alpha_0)) = n + c$ for some $n \geq c$ (because $f'(\alpha_0) \in \pi^c \mathfrak{o}^*$ and $f'(\alpha_0) \in \pi^{2c+1} \mathfrak{o}$). Let $\alpha_1 = \alpha_0 + y\pi^n$ for some $y \in \mathfrak{o}$. Then

$$f(\alpha_1) = f(\alpha_0 + y\pi^n) \equiv f(\alpha_0) + f'(\alpha_0)\pi^n y \pmod{p^{2n}}.$$

Choose

$$y = \frac{-f(\alpha_0)}{\pi^n f'(\alpha_0)}.$$  

Then

$$|y| = \frac{|f(\alpha_0)|}{|\pi^n f'(\alpha_0)|} = \frac{|\pi^{n+1}|}{|\pi^{n+1}|} = 1.$$

Then $y \in \mathfrak{o}^*$. Then for that $y$,

$$f(\alpha_1) \equiv 0 \pmod{p^{2n}}.$$

That proves

$$v(f(\alpha_1)) \geq 2n.$$

Since $n > c$,

$$v(f'(\alpha_1)) = v(f'(\alpha_0)) = c.$$

Repeat the process from $\alpha_1$ to get $\alpha_2$, then $\alpha_3$ and so on, and we get

$$v(f(\alpha_0)) < v(f(\alpha_1)) < v(f(\alpha_2)) \cdots$$
and
\[ v(f'(\alpha_n)) = v(f'(\alpha_1)), \quad \forall n. \]

Also
\[ v(\alpha_{n+1} - \alpha_n) > v(\alpha_n - \alpha_{n-1}), \]
which implies \( \{\alpha_n\} \) is Cauchy. So \( \lim_{n \to \infty} \alpha_n = \alpha \) exists in \( \mathfrak{o} \). Since \( v(f(\alpha_n)) \to \infty \), by
continuity \( \lim_{n \to \infty} f(\alpha_n) = 0 = f(\alpha). \)

\[ \square \]

**Example 32.2.** Consider \( f(x) = x^2 + 1 \) in \( \mathbb{Q}_5 \) and \( \alpha_0 = 2 \). We have \( f(\alpha_0) = 5 \), so \( |f(\alpha_0)|_5 < 1 \). Also \( f'(\alpha_0) = 2 \times 2 = 4 \), so \( |f'(\alpha_0)| = 1 \). Then by Hensel’s Lemma, there
exists \( \alpha \in \mathbb{Z}_5 \) with \( \alpha \equiv 2 \pmod{5} \) and \( \alpha^2 + 1 = 0 \).

### 32. Teichmüller Units (11/03)

Let \( K \) be a complete field with nonarchimedean absolute value \( | \cdot | = | \cdot |_v \), \( \mathfrak{o} = \{ x \in K : |x| \leq 1 \} \) the valuation ring of \( K \), \( \mathfrak{p} = \{ x \in K : |x| < 1 \} \) the maximal ideal of \( \mathfrak{o} \). Assume
\( k = \mathfrak{o}/\mathfrak{p} \) is a finite field of order \( q = p^f \) for a prime \( p \).

**Theorem 32.1.** For each \( a \in \mathfrak{o}/\mathfrak{p} \) with \( a \neq 0 \), there exists \( \hat{a} \in \mathfrak{o} \) with \( \hat{a}^q - 1 = 1 \) and \( \hat{a} \equiv a \pmod{\mathfrak{p}} \).

**Proof.** Pick \( x_0 \in \mathfrak{o} \) with \( x_0 \equiv a \pmod{\mathfrak{p}} \). Since \( a^{q-1} = 1 \) in \( (\mathfrak{o}/\mathfrak{p})^* \), then \( x_0^{q-1} \equiv 1 \pmod{\mathfrak{p}} \). So for \( f(x) = x^{q-1} - 1 \), we have \( |f(x_0)| < 1 \). Next, \( f'(x_0) = (q-1)x_0^{q-2} \). Since \( x_0^{q-2} \equiv 1 \pmod{\mathfrak{p}} \), \( |x_0| = 1 \). Also, since \( p\#(\mathfrak{o}/\mathfrak{p}) \), we have \( p \equiv 0 \pmod{\mathfrak{p}} \) and so \( q = p^f \equiv 0 \pmod{\mathfrak{p}} \). So \( |q - 1| = 1 \). So \( |f'(x_0)| = |q - 1| \cdot |x_0|^{q-2} = 1 \). Then \( |f(x_0)| < 1 = |f'(x_0)|^2 \). Then by Hensel’s Lemma, there exists root \( \hat{a} \) with \( f(\hat{a}) = (\hat{a})^q - 1 = 0 \) and \( \hat{a} \equiv x_0 \pmod{\mathfrak{p}} \).

\[ \square \]

**Remark 32.2.** It is common to use \( R = \{ 0, \hat{a} \} \) as “digits” in \( p \)-adic series expansion.

Next we consider when \( x_0 \) is a square in \( \mathbb{Z}_p^* \)

**Theorem 32.3.** If \( x_0 \in \mathbb{Z}_p^* \), then \( x_0 = a^2 \) for some \( a \in \mathbb{Z}_p^* \) if and only if

\[
\begin{cases}
  x_0 \equiv a^2 \pmod{p} & \text{if } p > 2, \\
  x_0 \equiv 1 \pmod{8} & \text{if } p = 2.
\end{cases}
\]

**Proof.** We look at \( f(x) = x^2 - x_0 \).

For \( p > 2 \), \( |f(a)|_p < 1 \) and \( |f'(a)|_p = |2a|_p = 1 \). By Hensel’s Lemma, we are done.

For \( p = 2 \), we need \( x_0 \equiv 1 \pmod{8} \). Then \( |f(1)|_2 = |1^2 - x_0|_2 \leq |8|_2 = 2 \) and \( |f'(1)|_2 = |2 \cdot 1|_2 = |2|_2 \). Hence \( |8|_2 < |f'(1)|_2^2 = |2|_2^2 = |4|_2 \). By Hensel’s Lemma, there exists a root \( x \) with \( f(x) = 0 \) and so \( x_0 = x^2 \). Conversely, if \( x_0 = a^2 \) for some \( a \in \mathbb{Z}_2^* \), then \( a = 1 + 2b \) for some \( b \in \mathbb{Z}_2 \). Then \( a^2 = (1 + 2b)^2 = 1 + 4b(b + 1) \equiv 1 \pmod{8} \).

\[ \square \]

49
33 Adeles and Ideles I (11/05)

A good reference for this part is the book *Basic Number Theory* by Weil.

Let \( K/\mathbb{Q} \) be a number field of degree \( n \). Let \( M = M_K \) be the set of inequivalent absolute values on \( K \) (places of \( K \)), \( M_\infty \) be the set of archimedean places (infinite places), \( M_\mathbb{R} \) be the set real places, \( M_\mathbb{C} \) be the set complex places. Let \( r_1, r_2 \) be the number of real places and complex places respectively. So \( r_1 + 2r_2 = n \). Let \( M_0 \) be the set of nonarchimedean places of \( K \). For each \( v \in M \), let \( K_v \) be the completion of \( K \) with respect to \( v \). For \( v \in M_0 \), let

\[
\begin{align*}
on_v &= \{ x \in K_v : |x|_v \leq 1 \}, \\
p_v &= \{ x \in K_v : |x|_v < 1 \}, \\
\pi_v &\in p_v \setminus p_v^2, \\
U_v &= \{ x \in K_v : |x|_v = 1 \} = \text{units of} \, o_v.
\end{align*}
\]

The ring of *adeles* of \( K \) is

\[
K_\mathbb{A} = K_K = \prod'_{v \in M} K_v
\]

where the direct product is restricted to \( (x_v)_{v \in M} \) where for all but finitely many \( v \in M_0 \) we have \( |x_v|_v \leq 1 \) (or \( x_v \in o_v \)).

A basis of open sets in \( K_\mathbb{A} \) consists of

\[
U \times \prod_{v \notin S} o_v
\]

where \( S \) is a finite set \( S \subset M \), \( S \supset M_\infty \), and \( U \) is an open subset of \( \prod_{v \in S} K_v \).

**Theorem 33.1** (Tychonoff’s Theorem). A countable direct product of compact sets is compact.

Tychonoff’s Theorem implies that \( \prod_{v \in M_0} o_v \) is compact, and hence \( K_\mathbb{A} \) is locally compact.

We use direct product laws of addition and multiplication on \( K_\mathbb{A} \).

**Theorem 33.2** (Theorem of Haar). Every Hausdorff locally compact topological group \( G \) has an invariant measure \( \mu \) on open subsets of \( G \), satisfying

(i) \( \mu(U) \geq 0 \) for all open subsets \( U \),
(ii) \( \mu(U) < \infty \) if \( \overline{U} \) is compact,
(iii) \( \mu \left( \bigcup_{n=1}^\infty U_n \right) = \sum_{n=1}^\infty \mu(U_n) \) for disjoint union \( \bigcup_{n=1}^\infty U_n \),
(iv) \( \mu(aU) = a\mu(U) \) for all \( a \in G \).

The Haar measure \( \mu \) is unique, determined up to a nonzero constant multiplier. For additive group \( G \), (iv) in Theorem of Haar becomes \( \mu(a + U) = \mu(U) \) for all \( a \in G \).
\( K_v \) is locally compact topological group under addition, so it has a Haar measure. If \( K_v \cong \mathbb{R} \), then \( \mu((a, b)) = b - a \) up to a constant is the usual Lebesgue measure. If \( K_v \cong \mathbb{C} \), then \( \mu(\{ |z| \leq r \}) = \pi r^2 \) up to a constant multiplier. If \( v \) is nonarchimedean, it is normal to normalize \( \mu \) by \( \mu(\mathcal{o}_v) = 1 \).

If \( \mu \) is a Haar measure on \( K_v \), for any \( a \in K_v^* \), define
\[
\mu_a(U) = \mu(aU).
\]
Then \( \mu_a(U) \) is also a Haar measure. So \( \mu_a(U) = \text{mod}_{K_v}(a) \cdot \mu(U) \). \( \text{mod}_{K_v}(a) \) is called the *modulus* of \( a \) in \( K_v \). \( \text{mod}_{K_v}(a) = |a|_\mathbb{R} \) if \( K_v \cong \mathbb{R} \), \( \text{mod}_{K_v}(a) = |a|^2 \) if \( K_v \cong \mathbb{C} \).

In general, there is a constant \( A \) such that
\[
\text{mod}_{K_v}(x + y) \leq A (\text{mod}_{K_v}(x) + \text{mod}_{K_v}(y))
\]
for any \( x, y \in K_v \). For example, for \( K_v = \mathbb{C} \), \( \text{mod}_{\mathbb{C}}(z) = |z|^2 \) where \( |\cdot| \) is the ordinary absolute value, we have \( \text{mod}_{\mathbb{C}}(z + w) \leq 2(\text{mod}_{\mathbb{C}}(z) + \text{mod}_{\mathbb{C}}(w)) \).

If \( v \) is nonarchimedean with \( \mathcal{o}_v / \mathfrak{p}_v \) finite, then
\[
\mathcal{o}_v = \prod_{a \in \mathcal{o}_v / \mathfrak{p}_v} (a + \pi \mathcal{o}_v)
\]
for any \( \pi \in \mathfrak{p}_v \setminus \mathfrak{p}_v^2 \). So
\[
\mu(\mathcal{o}_v) = \sum_{a \in \mathcal{o}_v / \mathfrak{p}_v} \mu(a + \pi \mathcal{o}_v)
= \sum_{a \in \mathcal{o}_v / \mathfrak{p}_v} \mu(\pi \mathcal{o}_v)
= \text{mod}_{K_v}(\pi) \sum_{a \in \mathcal{o}_v / \mathfrak{p}_v} 1
= \frac{1}{|\mathcal{o}_v / \mathfrak{p}_v|} \cdot \sum_{a \in \mathcal{o}_v / \mathfrak{p}_v} 1.
\]

### 34 Adeles and Ideles (II) (11/07)

Now let \( K/\mathbb{Q} \) be a finite extension. Let \( K_\mathbb{A} = \prod_{v \in \mathfrak{M}} K_v \). \( K_\mathbb{A} \) is locally compact and has a Haar measure defined by
\[
\mu(U) = \int_U |dx|_\mathbb{A} = \int_U d\mu_\mathbb{A}(x).
\]
One common normalization is to put
\[
\mu \left( \prod_{v \in \mathfrak{M}} \{ x_v : |x_v|_v \leq 1 \} \right) = \prod_{v \in \mathfrak{M}_\mathbb{R}} \int_{-1}^1 dx \cdot \int_{|x| \leq 1} dx \cdot \int_{|x| \leq 1} \mu(\mathcal{o}_v)
= 2^{r_1} (2\pi)^{r_2}.
\]

51
The group of ideles of $K$ is the restricted direct product

$$K_A^* = \prod_{v \in \mathfrak{N}} K_v^*$$

where $(x_v)_v$ must satisfy $x_v \in \mathfrak{o}_v^*$ for almost all finite places $v$. $K_A^*$ has the direct product multiplicative law and the restricted direct product topology. $K_A^*$ is locally compact. $K_A^*$ acts continuously on $K^A$ by $a \in K_A^*$ and $x \in K^A$ going to $ax \in K^A$.

The normalize Haar measure on $K_A^*$ is

$$\mu \left( \prod_{v \in \mathfrak{N}_{\infty}} \{1 \leq |x|_v \leq N\} \times \prod_{v \in \mathfrak{N}_{\infty}} \mathfrak{o}_v^* \right) = \left( 2 \int_1^N \frac{dt}{t} \right)^r_1 \cdot \left( \int_{1 \leq |x|_v \leq N} \frac{|dx \wedge dx|}{|x|_v} \right)^{r_2} \cdot 1$$

$$= 2^{r_1} \cdot (\log N)^{r_1}(2\pi \cdot 2\log(\sqrt{N}))^{r_2}$$

$$= 2^{r_1} \cdot (2\pi)^{r_2} \cdot (\log N)^{r_1+r_2}.$$

If $\mu$ is a Haar measure on $K_A^*$ and $a \in K_A^*$, then $\mu(aU)$ for any open $U \subset K_A^*$ defines another Haar measure on $K_A^*$. So $\mu(aU) = \text{mod}_A(a)\mu(U)$. Another common notation is $|a|_A = \text{mod}_A(a)$. From the product structure of $K_A$ and $K_A^*$, we can prove $|a|_A = \prod_{v \in \mathfrak{N}} |a_v|_v$. (This is the product formula for ideles.)

### 35 Module Theory over Dedekind Domain (11/10)

Let $\mathfrak{o}$ be an integral domain and $M$ a module over $\mathfrak{o}$. Then $x \in M$ is torsion if there exists $r \in \mathfrak{o}$ such that $r \neq 0$ and $rx = 0$. $tM$, the set of torsion elements in $M$, is a submodule of $M$ and is called the torsion submodule of $M$. $M$ is torsion-free if $tM = 0$. $M/tM$ is torsion-free for any module $M$ over $\mathfrak{o}$.

Let $\mathfrak{o}$ be Noetherian, $K$ be the field of fractions of $\mathfrak{o}$.

**Theorem 35.1.** Let $M$ be a finitely generated $\mathfrak{o}$-module. The following are equivalent:

(i) $M$ is torsion-free.

(ii) $M$ is isomorphic to a submodule of a free $\mathfrak{o}$-module of finite rank.

(iii) $M$ is isomorphic to an $\mathfrak{o}$-submodule of a finite dimensional $K$-vector space.

(iv) The map $M \to M \otimes_\mathfrak{o} K$ defined by $m \mapsto m \otimes_\mathfrak{o} 1$ is injective.

$$\dim_K(M \otimes_\mathfrak{o} K) = \text{rk}_\mathfrak{o}(M)$$ is the $\mathfrak{o}$-rank of $M$.

**Theorem 35.2.** If $\mathfrak{o}$ is a PID, any finitely-generated torsion-free module is free.

**Theorem 35.3.** If $\mathfrak{o}$ is an integral domain containing a single prime ideal $\mathfrak{p} \neq 0$ and if $M = tM$ is a torsion module, then

$$M \cong \bigoplus_{i=1}^t (\mathfrak{o}/\mathfrak{p}^{n_i})$$

for uniquely determined $n_1 \leq n_2 \leq \cdots \leq n_t$. 52
Theorem 35.4. Let $\mathfrak{a}$ be an Dedekind domain.
(i) Every fractional $\mathfrak{a}$-ideal is a projective $\mathfrak{a}$-module.
(ii) Every torsion-free finitely generated $\mathfrak{a}$-module $M$ is isomorphic as a $\mathfrak{a}$-module to $F \oplus \mathfrak{a}$ for some free $\mathfrak{a}$-module $F$ and a fractional $\mathfrak{a}$-ideal $\mathfrak{a}$.

Remark 35.5. The $\mathfrak{a}$-rank of $F$ and the ideal class of $\mathfrak{a}$ are uniquely determined. The ideal class of $\mathfrak{a}$ is denoted only on $M$ is denoted as $c(M)$ and is called the Steinitz invariant of $M$. $M$ is free if and only if $c(M) = 1$ in $cL(K) = cL(\mathfrak{a})$.

Suppose $K$ is a finite extension of $\mathbb{Q}$, and $L/K$ is a finite extension. Then the ring $\mathfrak{a}_L$ of integers in $L$ is a finitely generated torsion free $\mathfrak{a}_K$-module. $\mathfrak{a}_L$ is free if and only if $c(\mathfrak{a}_L) = 1$.

Theorem 36.1. There is a unique absolute value $| \cdot |_w$ on $E$ such that $|x|_w = |x|_v$ for all $x \in K$. Furthermore, for $a \in E$, we have $|a|_{E/K} = |N_{E/K}(a)|_v$.

Proof. (Existence) If $K = \mathbb{R}$, then $E = \mathbb{R}$ or $\mathbb{C}$; if $K = \mathbb{C}$, then $E = \mathbb{C}$. In both cases, existence is clear. For the ordinary absolute value $| \cdot |$ on $\mathbb{C}$, $|z|^2 = |z \cdot \overline{z}| = |N_{\mathbb{C}/\mathbb{R}}(z)|_\mathbb{R}$.

If $K$ is a nonarchimedean field with valuation $v$ and maximal compact subring $\mathfrak{a}_K$, prime ideal $\mathfrak{p}_K$, then the integral closure $\mathfrak{a}_E$ of $\mathfrak{a}_K$ in $E$ is a discrete valuation domain with unique prime ideal $\mathfrak{p}_E$ satisfying $\mathfrak{p}_E \cap \mathfrak{a}_K = \mathfrak{p}_K$. Let $\pi = \pi_K \in \mathfrak{p}_K \setminus \mathfrak{p}_K^2$ and $\pi_E \in \mathfrak{p}_E \setminus \mathfrak{p}_E^2$. Then $\pi \mathfrak{a}_E = \mathfrak{p}_E^e$ for some integer $e \geq 1$. If $|\pi|_v = \lambda < 1$, define $|\pi_E|_w = \lambda^{1/e} < 1$. We can show that $| \cdot |_w$ defines an absolute value on $E$ satisfying $|\pi|_w = |\pi_E|_w = (\lambda^{1/e})^e = \lambda = |\pi|_v$.

(Uniqueness) Suppose $w, w'$ are two extensions of $v$ to $E$ over $K$. We want to prove that $w, w'$ are equivalent. Earlier we saw that this follows from

\[ \{ x \in E : |x|_w < 1 \} \subset \{ x \in E : |x|_{w'} < 1 \}. \]

If so then $|x|_{w'} = |x|_{w'}^c$ for some $c > 0$. Since $|x|_w = |x|_v = |x|_{w'}$ for $x \in K$, we have $c = 1$. It suffices to show (36.1) which is dealt with in Lemma 36.2.
Lemma 36.2. For any sequence \( \{x_n\} \subset E \), if we have
\[
\text{if } \lim_{n \to \infty} |x_n|_w = 0, \text{ then } \lim_{n \to \infty} |x_n|_{w'} = 0,
\]
then 36.1 is true.

Proof. Suppose 36.1 is not true, then there exists \( y \in E \) with \( |y|_w < 1 \) and \( |y|_{w'} \geq 1 \). Then
\[
\lim_{n \to \infty} |y^n|_w = 0 \text{ and } \lim_{n \to \infty} |y^n|_{w'} \geq 1,
\]
a contradiction. \( \square \)

To finish the proof of Theorem 36.1, we need to prove the limit connection 36.2.

37 Extensions II (11/14)

Both \(|\cdot|_w \) and \(|\cdot|_{w'} \) define \( v \)-norms on \( E \) as a vector space over \( K \). Recall that \( ||\cdot|| : E \to [0, \infty) \) is a \( v \)-norm if
(i) \( ||x|| = 0 \) if and only if \( x = 0 \).
(ii) \( ||\lambda x|| = |\lambda|_v \cdot ||x|| \) for all \( \lambda \in K, x \in E \).
(iii) \( ||x + y|| \leq ||x|| + ||y|| \) for all \( x, y \in E \).

Lemma 37.1. Let \( \{x_n\} \) be a sequence in \( E \). Let \( ||\cdot|| \) be a \( v \)-norm on \( E \) over \( K \). Let \( \{z_1, \cdots, z_n\} \) be a basis of \( E \) over \( K \). Let
\[
x_m = \lambda_{m_1} z_1 + \cdots + \lambda_{m_n} z_n
\]
for \( \lambda_{m_j} \in K \). Then
\[
\lim_{m \to \infty} ||x_m|| = 0 \text{ if and only if } \lim_{m \to \infty} ||\lambda_m||_v = 0 \text{ for all } 1 \leq j \leq n.
\]

Since 37.1 is independent of \( ||\cdot|| \), this shows the following corollary.

Corollary 37.2. For any two \( v \)-norms \( ||\cdot||, ||\cdot||' \) on \( E \) over \( K \), we have
\[
\lim_{m \to \infty} ||x_m|| = 0 \text{ if and only if } \lim_{m \to \infty} ||x_m||' = 0.
\]

Proof of Lemma 37.1 \( \iff \) Assume \( \lim_{m \to \infty} ||\lambda_{m_j}||_v = 0 \) for all \( j \). Then
\[
0 \leq ||x_m|| \leq ||\lambda_{m_1}||_v \cdot ||z_1|| + \cdots + ||\lambda_{m_n}||_v \cdot ||z_n||.
\]
By the Squeeze Theorem, \( \lim_{m \to \infty} ||x_m|| = 0 \).
\( \implies \) We prove this direction by induction. For \( n = 1, ||x_m|| = ||\lambda_{m_1}||_v \cdot ||z_1|| \) and since \( ||z_1|| \neq 0 \), this statement is clear.
Assume it is true for some \( n \geq 1 \) and let \( \dim(E/K) = n + 1 \), with basis \( \{ z_1, \cdots, z_{n+1} \} \). Let \( U = \text{span}(z_1) \) and consider the quotient space \( E/U \) which has dimension \( n \). Define

\[
\| \cdot \|_0 : E/U \to [0, \infty) \\
x + U \mapsto \inf_{z \in U} ||x + z|| = \inf_{\lambda \in K} ||x + \lambda z_1||.
\]

We will check that \( || \cdot \|_0 \) is a norm on \( E/U \).

(i) If \( ||x + U||_0 = 0 = \inf_{z \in U} ||x + z|| \), then there is a sequence \( z_m \in U \) such that \( \lim_{m \to \infty} ||x - z_m|| = 0 \). Then \( \lim_{m \to \infty} z_m = x \). All finite-dimensional subspaces of a finite-dimensional normed vector space are closed. So \( x \in U \).

(ii) For any \( \lambda \in U \),

\[
||\lambda (x + U)||_0 = \inf_{z \in U} ||\lambda(x + z)|| \\
= \inf_{z \in U} ||\lambda x + \lambda z|| \\
= |\lambda|_v \cdot \inf_{z \in U} ||x + z|| \\
= |\lambda|_v \cdot ||x + U||_0.
\]

(iii)

\[
||(x + U) + (y + U)||_0 = \inf_{z, z' \in U} ||x + y + z + z'|| \\
= \inf_{z, z' \in U} ||x + y + z + z'|| \\
\leq \inf_{z, z' \in U} (||x + z|| + ||y + z'||) \quad \text{(by Triangle Inequality)} \\
\leq \inf_{z \in U} ||x + z|| + \inf_{z' \in U} ||x + z'|| \\
= ||x + U||_0 + ||y + U||_0.
\]

Take a sequence

\[
x_m = \lambda_{m_1} z_1 + \cdots + \lambda_{m_{n+1}} z_{n+1}
\]

with \( \lim_{m \to \infty} ||x_m|| = 0 \). Let

\[
y_m = \lambda_{m_2} z_2 + \cdots + \lambda_{m_{n+1}} z_{n+1} + U \in E/U.
\]

Then

\[
||y_m + U||_0 \leq ||x_m||.
\]

So \( \lim_{m \to \infty} ||y_m + U||_0 = 0 \). Since \( z_2 + U, \cdots, z_{n+1} + U \) is a basis of \( E/U \), by the induction assumption for \( n \), this implies

\[
\lim_{m \to \infty} |\lambda_{m_j}|_v = 0, \quad \forall 2 \leq j \leq n + 1.
\]

55
Repeat the whole argument with $U = \text{span}(z_i)$ for any $i \neq 1$, then we get
$$\lim_{m \to \infty} |\lambda_{mj}|_v = 0, \ \forall j \neq i, 1 \leq j \leq n + 1.$$ Then we proved
$$\lim_{m \to \infty} |\lambda_{mj}|_v = 0, \ \forall 1 \leq j \leq n + 1. \quad \square$$

38 Correspondence Between Prime Ideals and Absolute Values (11/17)

Let $K$ be a field with a valuation $v$, $K_v$ be its completion, and $L/K$ be a finite separable extension. Then $L \otimes_K K_v \cong \prod_{i=1}^n L_i$ and $L_i$ is a finite separable extension of $K_v$. $v$ has a unique extension $w_i$ to $L_i$. Every extension of $v$ to $L$ is one of the $w_i$’s. The $w_i$’s are inequivalent absolute values on $L$.

Corollary 38.1. $L$ is dense under the embedding $L \to L \otimes_K K_v$ defined by $\alpha \mapsto \alpha \otimes 1$ by the Weak Approximation Theorem.

We will write
$$L \otimes_K K_v \cong \prod_{w \mid v} L_w$$
where $w \mid v$ means $w$ is an extension of $v$.

Let $v$ be a discrete valuation. Let $\mathfrak{o}_{K_v} = \mathfrak{o}_v = \{x \in K_v : |x|_v \leq 1\}$ be the maximal compact subring of $K_v$, $\mathfrak{p}_v$ the maximal ideal of $\mathfrak{o}_v$, $\mathfrak{o}_{L_w} = \{x \in L_w : |x|_w \leq 1\}$ the maximal compact subring of $L_w$, $\mathcal{P}_w$ the maximal ideal of $\mathfrak{o}_{L_w}$. We have proved $\mathcal{P}_w \cap \mathfrak{o}_{K_v} = \mathfrak{p}_v$. Then the ramification order $e = e(w \mid v)$ is defined by
$$\mathfrak{p}_v \mathfrak{o}_{L_w} = \mathcal{P}_w^e.$$
If $e = 1$, $w$ is unramified over $v$. Define the residue degree of $w$ over $v$ to be
$$f = f(w \mid v) = (\mathfrak{o}_{L_w}/\mathfrak{p}_v : \mathfrak{o}_{K_v}/\mathfrak{p}_v).$$

Theorem 38.2. $(L_w : K_v) = e(w \mid v)f(w \mid v)$.

Proof. We sketch the idea of the proof. Choose $\pi_w \in \mathcal{P}_w \setminus \mathcal{P}_w^2$. List a basis of $\mathfrak{o}_{L_w}/\mathcal{P}_w$ over $\mathfrak{o}_{K_v}/\mathfrak{p}_v$ to $\{\alpha_1, \cdots, \alpha_f\}$. Then $\{\alpha_i \pi_w^j\}_{1 \leq i \leq f, 0 \leq j \leq e-1}$ is a basis of $L_w/K_v$. \quad \square

Suppose $\mathfrak{o}_K$ is a Dedekind domain, $K$ is its field of fractions, $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}_K$, $L/K$ is a finite separable extension, $\mathcal{O}_L$ is the integral closure of $\mathfrak{o}_K$ in $L$, $\mathcal{P}$ is a prime
ideal of $O_L$ lying over $p$. So $P \cap o_K = p$. Let $v$ be the valuation corresponding to $p$ on $K$, $w$ the valuation of $L$ corresponding to $P$. In the Dedekind domain $o_L$,

$$pO_L = P_1^{e_1} \cdots P_t^{e_t}$$

for distinct prime ideals $P_j$ in $O_L$. The $P_j$ corresponds to all the inequivalent absolute values $w$ extending $v$ from $K$ to $L$. Each $P_j$ corresponds to some $w_j|v$ and $L_{P_j} = L_{w_j}$, and $e_j = e(w_j|v)$. That describes the correspondence between the prime ideals over $p$ and the direct sum components in $L \otimes_K K_v = \prod_{w|v} L_w$.

Inside $L \otimes_K K_v$ we have a ring $O_L \otimes_{o_K} o_{K_v}$. Since $o_{K_v}$ is a PID, $O_L \otimes_{o_K} o_{K_v}$ is a free $o_{K_v}$-module of rank $(L : K)$. Also

$$O_L \otimes_{o_K} o_{K_v} \cong \prod_{w|v} o_{L_w}.$$ 

The mapping $\alpha \in L \rightarrow \alpha \otimes 1 \rightarrow (\alpha)$ is dense because the absolute values $w$ are inequivalent, by the Weak Approximation Theorem. Also, since $o_{K_v}$ is closed, $O_L \otimes_{o_K} o_{K_v}$ is closed as a submodule. So the mapping is onto.

**Theorem 38.3 (Tower Laws).** Suppose

$$K \hookrightarrow L \hookrightarrow N$$

are finite separable extensions with prime ideals

$$p \rightarrow P \rightarrow Q$$

in each of them. Then

$$e(Q|p) = e(Q|P)e(P|p),$$

$$f(Q|p) = f(Q|P)f(P|p),$$


### 39 Galois Extensions I (11/19)

Let $L/K$ be a finite separable extension, $K$ be the field of fractions of a Dedekind domain $o$, $O_L$ be the integral closure of $o$ in $L$. Any prime ideal $p$ in $o$ lifts to an ideal $pO_L$ with factors as

$$pO_L = P_1^{e_1} \cdots P_t^{e_t}$$

for all distinct prime ideals $P_j$ lying over $p$ and $P_j \cap o_K = p$. The primes $P_j$ correspond to the inequivalent valuations $w_j$ extending the valuation on $K$ corresponding to $p$ to $L$. With regard to completions, $L_{P_j} = L_{w_j}$. If we omit the $j$, the prime ideal in $L_w$ $P_w$ satisfies $P_w \cap O_L = p$.

Suppose $L/K$ is a Galois extension with $G = \text{Gal}(L/K)$. 

57
Theorem 39.1. $G$ acts transitively on the prime divisors $P_j$ of $p\mathcal{O}_L$. So all $e_j = e$ and all $f_j = f$ and so $[L : K] = ef r$.

The decomposition group (Zerlegungsgruppe in German) of $P$ lying over $p$ is defined as

$$Z(P) = \{ \sigma \in G : \sigma(P) = P \}.$$ 

We have $[G : Z] = r$ and $Z(P_i)$ is conjugate to $Z(P_j)$ in $G$. The inertia group (Trägungsgruppe in German) is defined as

$$T(P) = \{ \sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{P} \text{ for all } \alpha \in \mathcal{O}_L \} = \{ \sigma \in G : \sigma \text{ acts as the identity in } \mathcal{O}_L/P \}.$$

$T(P)$ is a normal subgroup of $Z(P)$ and

$$Z(P)/T(P) = \text{Gal}((\mathcal{O}_L/P)/(\mathfrak{o}_K/p)).$$

If $\mathfrak{o}_K/p$ is a finite field of order $q$, then $\mathcal{O}_L/P$ has order $q^f$, and is cyclic generated by Frobenius $\varphi(x) = x^q$. The class of $\varphi$ in $Z/T$ is called the Frobenius symbol $\left[ \frac{L/K}{P} \right] \in G$.

If $G$ is abelian, then $Z(P)$ is the same for all $P|p$, and then we write

$$\left[ \frac{L/K}{P} \right] = \left( \frac{L/K}{p} \right)$$

and the second one is the Artin symbol. $p$ is ramified ($e > 1$) if and only if $T \neq 1$. If $T = 1$, then $\left( \frac{L/K}{p} \right) \in G$ is a well-defined element.

40 Galois Extensions II (11/21)

Suppose $L/K$ is Galois with $\text{Gal}(L/K) = G$. For any prime ideal $p$ in $\mathfrak{o}_K$, let $P$ be a prime ideal lying over $p$ in $\mathcal{O}_L$. We have defined

$$Z(P) = \{ \sigma \in G : \sigma(P) = P \},$$

$$T(P) = \{ \sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{P} \text{ for all } \alpha \in \mathcal{O}_L \}.$$

This implies that $\text{Gal}((\mathcal{O}_L/P)/(\mathfrak{o}_K/p)) \cong Z(P)/T(P)$. $Z(P) \cong \text{Gal}(L_P/K_p)$ where $L_P$ is the completion of $L$ relative to the valuation determined by $P$ and $K_p$ is the completion of $K$ relative to the valuation determined by $p$. Suppose we have a tower of extension $K_p \hookrightarrow F \hookrightarrow L_P$ where $\text{Gal}(F/K_p) = Z/T$, $\text{Gal}(L_P/F) = T$, then the extension $F/K_p$ is unramified, and the extension $L_P/F$ is totally ramified.

Suppose $K$ is a finite extension of $\mathbb{Q}$, $(K : \mathbb{Q}) = n$, and $\mathcal{O}_K$ is the the ring of integers of $K$. Suppose $\alpha \in \mathcal{O}_K$ satisfies an Eisenstein polynomial for the prime $p$

$$f(\alpha) = \alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$$

58
where $p|c_j$ for $1 \leq j \leq n$ and $p^2 \nmid c_n$. Then $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and $p$ is totally ramified in $K$ ($e = n, f = 1, r = 1$). (Recall $\text{Disc}(f) = \text{Disc}(\mathcal{O}_K) \cdot ([\mathcal{O}_K : \mathbb{Z}[\alpha]])^2$).

Here is an example for $K = \mathbb{Q}(w)$ where $w = e^{2\pi i/p}$, $p \geq 3$. $f(x) = x^n - 1$. We have $\text{Disc}(f) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$ (by midterm problem). So $D_K = \text{Disc}(\mathcal{O}_K) | (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$.

Notice that $p - 1$ satisfies an Eisenstein polynomial for $p$, so $w - 1$ satisfies an Eisenstein polynomial for $p$. Then $p \nmid [\mathcal{O}_K : \mathbb{Z}[w - 1]] = [\mathcal{O}_K : \mathbb{Z}[w]]$. That proves $[\mathcal{O}_K : \mathbb{Z}[w]] = 1$. That proves $D_K = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$

is square of Vandermonde determinant

with entries equal to power of $w$.

Then $D_K$ is a square in $K$. So $\sqrt{D_K} \in K$. Since $p$ is odd, $p - 2$ is odd. Then $F = \mathbb{Q}(\sqrt{D_K}) = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) \subset K$.

Let $q$ be a prime different from $p$. $q$ splits in $F/\mathbb{Q}$ if $q\mathfrak{P}_F = \mathfrak{P}_q$ for some prime ideal $q$. By earlier lemma, $q = (q, \alpha)$ for some $\alpha = a + b\sqrt{D}$. Then $q\mathfrak{P}_F = (q, a - b\sqrt{D})(q, a + b\sqrt{D})$. This proves $q|a^2 - b^2D$. So $D$ is a square mod $q$. So $(-1)^{\frac{p-1}{2}} \cdot p$ is a square mod $q$. $\text{Gal}(\mathbb{Q}(w)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^* \equiv \{1^\cdot\}_{l \in (\mathbb{Z}/p\mathbb{Z})^*}$. By Galois theory, $K^H = F$. $q$ splits in $F$ if and only if the decomposition group of any prime ideal $Q$ lying over $p$ satisfies $Z(Q) \subset H$. $Z_K(Q) \cong \text{Gal}(\mathcal{O}_K/(\mathbb{Z}/q\mathbb{Z}))$ is generated by the Frobenius map $x \mapsto x^q$. This map must be in $H$. So $q$ is a square mod $p$. This yields another proof of the Law of Quadratic Reciprocity: for odd primes $p, q$,

$(-1)^{\frac{p-1}{2}} \cdot p \equiv \square \pmod{q}$ iff $q \equiv \square \pmod{p}$.

41 Galois Extensions III (11/24)

Lemma 41.1. Let $K$ be a finite extension of $\mathbb{Q}$, $(K : \mathbb{Q}) = n$, and $\mathcal{O}_K$ is the ring of integers of $K$. Suppose $\alpha \in \mathcal{O}_K$ satisfies an Eisenstein polynomial

$$f(\alpha) = \alpha^n + c_1\alpha^{n-1} + \cdots + c_n$$

where $p|c_j$ for $1 \leq j \leq n$ and $p^2 \nmid c_n$, then $p \nmid [\mathcal{O}_K : \mathbb{Z}[[\alpha]]]$.
Let \( q_0 \in \pi \) where \( \pi \) is the maximal compact subring.

Theorem 41.3.

\[ \alpha \in \mathbb{Z}[\alpha], \beta \notin \mathbb{Z}[\alpha]. \]

Let \( p \) be the smallest index such that \( p \mid b_j \). Then \( p \mid b_i \) for \( 0 \leq i < j \). Let \( \gamma \in \mathcal{O}_K \) be

\[ \gamma = \beta - \frac{b_0 + b_1 \alpha + \cdots + b_{j-1} \alpha^{j-1}}{p} = b_j \frac{\alpha^j + \cdots + b_{n-1} \alpha^{n-1}}{p}. \]

Then

\[ \gamma \alpha^{n-j-1} = \frac{b_j \alpha^{n-1}}{p} + \frac{\alpha^n}{p} \delta \]

for some \( \delta \in \mathbb{Z}[\alpha] \). Since \( \frac{\alpha^n}{p} \delta \in \mathcal{O}_K \), \( \frac{b_j \alpha^{n-1}}{p} \in \mathcal{O}_K \). So

\[ N_{K/Q} \left( \frac{b_j \alpha^{n-1}}{p} \right) = \frac{b_j \cdot N_{K/Q}(\alpha)^{n-1}}{p^n} = \pm \frac{b_j^n \alpha^{n-1}}{p^n} \in \mathbb{Z}. \]

Since \( p \mid c_n, p^{n-1} \mid c_n^{n-1} \), hence \( p \mid b_j^n \) and so \( p \mid b_j \). This is a contradiction. \( \square \)

Remark 41.2. If \( | \cdot |_v \) on \( K \) is the extension of \( | \cdot |_p \) on \( \mathbb{Q} \), then

\[ |\alpha^n|_v = | - c_1 \alpha^{n-1} - \cdots - c_n |_v \leq \max (| - c_1 \alpha^{n-1}|_v, \ldots, | - c_n |_v). \]

By the Eisenstein condition, \( p | c_1, \ldots, c_n \). So \( |c_j|_v = |c_j|_p \leq |p|_p < 1 \). Then \( |\alpha|_v < 1 \). Since \( | - c_j \alpha^{n-j}|_v = |c_j|_p |\alpha^{n-j}|_v < |p|_p \) for all \( 1 \leq j \leq n-1 \) and \( | - c_n |_v = |p|_p \), then \( |\alpha^n|_v = |p|_p \). That means that \( K_v \) is totally ramified over \( \mathbb{Q}_p \). Also, \( (\alpha \mathcal{O}_K)^n = p \mathcal{O}_K \) and so \( e(p^n) = n = (K : \mathbb{Q}) \). Conversely, if \( K/Q \) is totally ramified at \( p \), then there is an \( \alpha \in K \) that satisfies an Eisenstein polynomial at \( p \).

Theorem 41.3. Let \( K \) be a nonarchimedean complete field with absolute value \( | \cdot |_v \), maximal compact subring \( \mathfrak{o} \), prime ideal \( \mathfrak{p} \), with finite residue field \( k = \mathfrak{o}/\mathfrak{p} \) of order \( q = p^f \). Let \( \pi \) be a generator of \( \mathfrak{p} \). A finite separable extension \( L/K \) is totally ramified \( e = (L:K), f = 1 \) if and only if \( L = K(\alpha) \) where \( \alpha \) has a minimal polynomial

\[ \alpha^n + c_1 \alpha^{n-1} + \cdots + c_n = 0, \quad n = (L:K) \]

where \( \pi^j \) for \( 1 \leq j \leq n, \pi^2 \mid c_n \).

Theorem 41.4. Let \( K \) be a nonarchimedean complete field with absolute value \( | \cdot |_v \), maximal compact subring \( \mathfrak{o}, \) prime ideal \( \mathfrak{p} \), with finite residue field \( k = \mathfrak{o}/\mathfrak{p} \) of order \( q = p^f \). Let \( \pi \) be a generator of \( \mathfrak{p} \). A finite separable extension \( L/K \) is unramified \( e = 1, f = (L:K) = n \) if and only if \( L = K(\alpha) \) where \( \alpha \) is a \((q^n - 1)\)-th root of unity in \( L \).
Proof. Earlier we showed that there is an isomorphism
\[ (\mathcal{O}_L/P)^* \hookrightarrow L^* \]
that maps onto the \((q^n - 1)\)-th root of unity, (the Teichmüller units) proved by Hensel’s Lemma. Thus, these roots of unity generate \(L/K\).

**Theorem 41.5.** Every finite separable extension \(L/K\) of complete nonarchimedean number fields has a unique intermediate field
\[ L \supset F \supset K \]
such that \(F/K\) is unramified and \(L/F\) is totally ramified.

**Corollary 41.6.** Every Galois extension \(L/K\) of complete nonarchimedean number fields has solvable Galois group.

### 42 Finiteness of the Class Group I (12/01)

Let \(K/\mathbb{Q}\) be a finite extension with ring of integers \(\mathcal{O}_K\). The class group is
\[ C_K = \text{cl}(\mathcal{O}_K) = I_{\mathcal{O}_K}/P_{\mathcal{O}_K}. \]
The absolute norm of an ideal \(a \subset \mathcal{O}_K\) is
\[ N(a) = |\mathcal{O}_K : a|. \]

If \(p\) is a prime ideal lying over \(p\) in \(\mathbb{Q}\), then \((\mathcal{O}_K/p)\) is an extension of \((\mathbb{Z}/p\mathbb{Z})\) of degree \(f(p|p)\). So \(N(p) = p^f\).

**Lemma 42.1.** For any \(X > 0\), there are finitely many ideals \(a \subset \mathcal{O}_K\) with \(N(a) \leq X\).

**Proof.** By Dedekind Theorem, every ideal has a prime factorization \(a = p_1^{e_1} \cdots p_r^{e_r}\). The Chinese Remainder Theorem says that
\[ N(a) = |\mathcal{O}_K/a| = N(p_1)^{e_1} \cdots N(p_r)^{e_r}. \]

There are only finitely many ideals \(p\) in \(\mathcal{O}_K\) that lie over a given ordinary prime \(p \in \mathbb{Z}\). For \(n \leq X\), if \(n = p_1^{k_1} \cdots p_r^{k_r}\) in \(\mathbb{Z}\) then each \(p_j\) has only finitely many prime ideals \(p\) lying over \(p\) and \(N(p) = p_j^{f_j}\). So if \(N(a) = n\), and if \(p^e\|a\) then \(p^e = N(p^e) \leq N(a) = n\). That proves that
\[ e \leq \frac{\log(n)}{f \log(p)}. \]

For a given \(n\), that allows only finitely many prime ideals \(p\) and only finitely many exponents \(e\). That means there are finitely many \(a\) such that \(N(a) = n\). \(\square\)
We will show that there is a constant $A$ depending on $K/Q$ such that every ideal class contains an ideal $b \subset \mathcal{O}_K$ with $N(b) \leq A$.

Let $v_1, \cdots, v_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Pick some ideal $a$ in the inverse ideal class $C_{K}^{-1}$. Then let

$$\mathcal{L} = \{ s = \sum_{j=1}^{n} m_j v_j, 0 \leq m_j < (N(a))^{1/n} + 1 \}.$$

Then

$$\#\mathcal{L} \geq \prod_{j=1}^{n} (N(a))^{1/n} + 1 \geq N(a) + 1.$$

By Pigeonhole Principle, there exists $a, b \in \mathcal{L}$ with $a \neq b$ and $a \equiv b \pmod{a}$. (there are only $N(a) = |\mathcal{O}_K/a|$ congruence classes.) So $a - b \neq 0$ and $a - b = ab$ for some $\mathcal{O}_K$-ideal $b$. Notice since $(a - b)$ is principal, $b$ belongs to the ideal class $C_{K}$. Let

$$A = \prod_{j=1}^{n} \sum_{i=1}^{n} |v_i^{\sigma_j}|$$

where $\sigma_j$ ranges over the embeddings $\sigma_j : K \hookrightarrow \mathbb{C}$ over $\mathbb{Q}$. Now

$$N(a)N(b) = |N_{K/Q}(a - b)| = |N(\sum_{i=1}^{n} p_i v_i)| \leq \prod_{j=1}^{n} \left( \sum_{i=1}^{n} |p_i| |v_i^{\sigma_j}| \right)$$

for some integers $p_i \in \mathbb{Z}$ and $|p_i| \leq N(a)^{1/n} + 1$. So

$$N(a)N(b) \leq \left( N(a)^{1/n} + 1 \right)^n A$$

and hence

$$N(b) \leq \left( \frac{N(a)^{1/n} + 1}{N(a)^{1/n}} \right)^n A = \left( 1 + \frac{1}{N(a)^{1/n}} \right)^n A.$$

$a$ was arbitrary chosen in $C_{K}^{-1}$. Replace $a$ by $M^a$ for any $M \geq 1$. In the limit, as $M \to \infty$, we get $N(b) \leq A$.

**Theorem 42.2.** Let $K/Q$ be a finite extension, $(K : \mathbb{Q}) = n$, and $d_K$ be the discriminant of $K/Q$. Let $a$ be a non-zero fractional ideal in $\mathcal{O}_K$. There is a non-zero $y \in a$ such that

$$1 \leq |N_{K/Q}(y)| \leq \left( \frac{4}{\pi} \right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d_K|^{1/2} N(a)$$

where $r_1$ be the number of real embeddings $K \hookrightarrow \mathbb{R}$ over $\mathbb{Q}$, $r_2$ be the number of conjugate pairs of nonreal embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{R}$ over $\mathbb{Q}$.
We postpone the proof of Theorem 42.2 to next lecture, but see the consequences of it first.

**Theorem 42.3** (Minkowski Bound). Given a class \( c \in C_K \), there exists an \( \mathcal{O}_K \)-ideal \( b \in c \) such that

\[
N(b) \leq \left( \frac{4}{\pi} \right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d_K|^{1/2}.
\]

**Proof.** Choose an \( \mathcal{O}_K \)-ideal \( a \neq 0 \) in \( c^{-1} \). By Theorem 42.2, there exists \( x \neq 0 \) in \( a \) such that

\[
|N_{K/Q}(x)| \leq \left( \frac{4}{\pi} \right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d_K|^{1/2} N(a).
\]

Since \( x \in a \), \( x \neq 0 \), \( (x) = ab \) for some \( \mathcal{O}_K \)-ideal \( b \). Then \( b \) is in class \( c \). Then

\[
N(a)N(b) = |N_{K/Q}(x)| \leq \left( \frac{4}{\pi} \right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d_K|^{1/2} N(a).
\]

Then cancel \( N(a) \).

**Remark 42.4.** Theorem 42.3 implies that there are only finitely many ideal classes.

**Theorem 42.5.** For \( n \geq 2 \),

\[
|d_K| \geq \left( \left( \frac{\pi}{4} \right)^{r_2} \cdot \frac{n^n}{n!} \right)^2 > 1.
\]

**Proof.** Choose \( a = \mathcal{O}_K \) in Theorem 42.2. Then \( |N_{K/Q}(y)| \geq 1 \) and \( N(a) = N(\mathcal{O}_K) = 1 \).

**Remark 42.6.** The worst case for the bound in Theorem 42.5 is when \( r_2 = \frac{n}{2} \). Then

\[
\left( \frac{\pi}{4} \right)^{n/2} \cdot \frac{n^n}{n!} > 1.
\]

This can be proved by induction. If \( n = 2 \), then \( \frac{\pi}{4} \cdot \frac{2^2}{2!} = \frac{\pi}{2} > 1 \). Now consider the ratio of \( n+1 \)-term to the \( n \)-term:

\[
\frac{\left( \frac{\pi}{4} \right)^{(n+1)/2} \cdot \frac{(n+1)^{n+1}}{(n+1)!}}{\left( \frac{\pi}{4} \right)^{n/2} \cdot \frac{n^n}{n!}} = \left( \frac{\pi}{4} \right)^{1/2} \cdot \frac{(n+1)^{n+1}}{(n+1) \cdot n^n} = \left( \frac{\pi}{4} \right)^{1/2} \cdot \frac{n+1}{n}.
\]
Note that \((1 + \frac{1}{n})^n\) is an increasing sequence for \(n \geq 2\) (converges to \(e\)). The minimal ratio is when \(n = 2\), which is
\[
\left(\frac{\pi}{4}\right)^{1/2} \cdot \left(1 + \frac{1}{2}\right)^2 \approx 1.99 > 1.
\]

### 43 Finiteness of the Class Group II (12/03)

Let \(K/\mathbb{Q}\) be a finite extension, \((K : \mathbb{Q}) = n\), and \(d_K\) be the discriminant of \(K/\mathbb{Q}\). Let \(r_1\) be the number of real embeddings \(K \hookrightarrow \mathbb{R}\) over \(\mathbb{Q}\), \(r_2\) be the number of conjugate pairs of nonreal embeddings \(\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{R}\) over \(\mathbb{Q}\). So \(K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}\) and \(n = r_1 + 2r_2\).

Number the embeddings \(\sigma_1, \cdots, \sigma_n\) such that
\[
\sigma_j : K \hookrightarrow \mathbb{R} \text{ for } 1 \leq j \leq r_1,
\]
\[
\sigma_j : K \hookrightarrow \mathbb{C} \text{ for } r_1 + 1 \leq j \leq r_1 + r_2.
\]

and
\[
\sigma_{j+r_2} = \overline{\sigma_j} \text{ for } r_1 + 1 \leq j \leq r_1 + r_2.
\]

Each \(\sigma_j\) induces an \(\mathbb{R}\)-linear map
\[
f_j = \sigma_j \otimes \text{id} : K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}
\]
\[
x \otimes r \mapsto r(x^{\sigma_j}).
\]

Set \(V = K \otimes_{\mathbb{Q}} \mathbb{R}\) which is a \(n\)-dimensional \(\mathbb{R}\)-vector space. Let \(a\) be a fractional ideal of \(\mathcal{O}_K\). Let \(a_1, \cdots, a_n\) be a \(\mathbb{Z}\)-basis of \(a\). Then \(\{a_j \otimes a\}_{1 \leq j \leq n}\) is an \(\mathbb{R}\)-basis of \(V\). The general point \(x\) in \(V\) can be written as
\[
x = \sum_{j=1}^{n} a_j \otimes x_j
\]
for \(x_j \in \mathbb{R}\).

Let
\[
R_d = \{\vec{x} \in \mathbb{R}^n : \sum_{j=1}^{r_1} |x_j| + 2 \sum_{j=r_1+1}^{r_1+r_2} \sqrt{x_j^2 + x_{j+r_2}^2} \leq d\}.
\]

Then \(R_d\) is symmetric (\(\vec{x} \in R_d \Rightarrow -\vec{x} \in R_d\)), compact, convex. Moreover,
\[
\text{vol}(R_d) = \int_{R_d} d\vec{x} = \frac{2^{r_1} (\pi)^{r_2}}{n!} d^n.
\]

For a fractional ideal \(a \subset \mathcal{O}_K\), choose a \(\mathbb{Z}\)-basis \(a_1, \cdots, a_n\) of \(a\) over \(\mathbb{Q}\) and map
\[
\sum_{j=1}^{n} a_j \otimes y_j \text{ to }
\begin{bmatrix}
    x_1 \\
    \vdots \\
    x_{r_1+1} \\
    \vdots \\
    x_{r_1+r_2} \\
    \vdots \\
    x_n
\end{bmatrix}
= \begin{bmatrix}
    \sigma_1(a_1) & \cdots & \sigma_1(a_n) \\
    \text{Re}(\sigma_{r_1+1}(a_1)) & \cdots & \text{Re}(\sigma_{r_1+1}(a_n)) \\
    \text{Re}(\sigma_{r_1+r_2}(a_1)) & \cdots & \text{Re}(\sigma_{r_1+r_2}(a_n)) \\
    \text{Im}(\sigma_{r_1+1}(a_1)) & \cdots & \text{Im}(\sigma_{r_1+1}(a_n)) \\
    \text{Im}(\sigma_{r_1+r_2}(a_1)) & \cdots & \text{Im}(\sigma_{r_1+r_2}(a_n))
\end{bmatrix}
\begin{bmatrix}
    y_1 \\
    \vdots \\
    y_{r_1+1} \\
    \vdots \\
    y_{r_1+r_2} \\
    \vdots \\
    y_n
\end{bmatrix}
= J
\begin{bmatrix}
    y_1 \\
    \vdots \\
    y_{r_1+1} \\
    \vdots \\
    y_{r_1+r_2} \\
    \vdots \\
    y_n
\end{bmatrix}.
\]

Then
\[
\det(J) = \left|2^{-r_2}\det(\sigma_j(a_k))\right| = 2^{-r_2}|d_K|^{1/2}N(a).
\]

The image \(\Lambda = JD^\mathbb{Z}^n\) is a lattice in \(R^n\): a free \(\mathbb{Z}\)-module of rank \(n\) such that \(R^n/\Lambda\) has finite volume.

\[
\text{vol}(\mathbb{R}^n/\Lambda) = |\det(J)|\text{vol}(\mathbb{R}^n/\mathbb{Z}^n)
\]
(by the multivariable change-of-variables theorem)
\[
= |\det(J)|
\]
\[
= 2^{-r_2}|d_K|^{1/2}N(a).
\]

**Lemma 43.1** (Minkowski-Blichfeldt Lemma). Let \(\Lambda\) be a lattice in \(\mathbb{R}^n\) and \(S\) a compact, symmetric, convex subset of \(\mathbb{R}^n\). If \(\text{vol}(S) \geq 2^n \text{vol}(\mathbb{R}^n/\Lambda)\), then \(S\) contains a non-zero point in \(\Lambda\).

**Proof of Theorem 42.2** Choose \(d\) so that
\[
\text{vol}(R_d) = \int_{R_d} d\vec{x} = \frac{2^{r_1}\pi^{r_2}d^n}{n!} \geq 2^n 2^{-r_2}|d_K|^{1/2}N(a).
\]

Then there exists \(y \in \mathbb{Z}^n, y \neq 0\) such that \(Jy \in R_d\). Let \(y = \sum_{j=1}^{n} y_j a_j \in \mathfrak{a}\). The setup implies that
\[
\sum_{j=1}^{r_1} |y^{\sigma_j}| + 2\sum_{j=r_1+1}^{r_1+r_2} |y^{\sigma_j}| \leq d.
\]

65
Then
\[ |N(y)| = \prod_{j=1}^{r_1} |y^{\sigma_j}| \]
\[ \leq \left( \frac{\sum_{j=1}^{n} |y^{\sigma_j}|}{n} \right)^n \]
(Arithmetic-Geometry Mean Inequality)
\[ \leq d^n \]
Get \( d \) to be the smallest of all such values that work, then we have
\[ |N(y)| \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{r_2} |d_K|^{1/2} N(a) \]

44 Dirichlet’s Unit Theorem (12/05)

Let \( U_K = \mathcal{O}_K^\times \) be the group of units of \( \mathcal{O}_K \), \( \mu_K = \{ x \in U_K : x^m = 1 \text{ for some } m \in \mathbb{Z} \} \) be the subgroup of roots of unity in \( U_K \). Since \( (\mathbb{Q}(e^{2\pi i/m}) : \mathbb{Q}) = \varphi(m) \to \infty \) as \( \varphi \to \infty \) and \( (K : \mathbb{Q}) \) is finite, there exists \( m \) such that \( \mu_K =< e^{2\pi i/m} > \) and \( \varphi(m) < (K : \mathbb{Q}) \). \( U_K \) is a multiplicative \( \mathbb{Z} \)-module ( \( l \in \mathbb{Z} \) acts on \( u \in U_K \) by \( u^l \) ). \( \mu_K \) is a torsion submodule. The torsion-free quotient is \( U_K = U_K/\mu_K \).

Lemma 44.1. \( u \in \mathcal{O}_K \) is a unit if and only if \( |N_K/\mathbb{Q}(u)| = 1 \).

Theorem 44.2 (Dirichlet’s Unit Theorem).

\[ U_K \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1} \]

A basis of the free part \( U_K \) is called a system of fundamental units.

Define a map
\[ \psi : K^\times \to W = \mathbb{R}^{r_1+r_2} \]
\[ u \mapsto (\log |u^{\sigma_j}|_{1 \leq j \leq r_1}, 2 \log |u^{\sigma_j}|_{r_1+1 \leq j \leq r_1+r_2}) \]

So if \( \vec{c} = (1, 1, \cdots, 1) \in \mathbb{R}^{r_1+r_2} \), then
\[ \psi(u) \cdot \vec{c} = \log(N(u)) \]

So \( \psi \) maps \( U_K \) into the hyperplane \( H = \{ \vec{w} \in W : \vec{w} \cdot \vec{c} = 0 \} = \vec{c}^\perp \). Note that \( \dim_{\mathbb{R}} H = r_1+r_2-1 \). Our goal is to show that \( \psi(U_K) \) is a lattice of rank \( r_1+r_2-1 \) in \( H \).
Lemma 44.3. \( \{ a \in \mathcal{O}_K : |a^{\sigma_j}| \leq \beta \text{ for all } j = 1, \cdots, n \} \) is a finite set.

Proof. The coefficients of
\[
f(x) = \prod_{\sigma} (x - a^\sigma) = x^n + c_1 x^{n-1} + \cdots + c_n
\]
satisfies \( |c_j| \leq \binom{n}{j} \beta^j \). This allows at most finitely many \( f(x) \in \mathbb{Z}[x] \), each of which has finitely many roots. \( \square \)

Corollary 44.4. This proves \( \psi(U_K) \) is discrete in \( W \).

Corollary 44.5. \( \ker(\psi) = \mu_K \).

Proof. By Lemma 44.3, \( \ker(\psi) \) is a finite subgroup of \( \{ a \in K^* : |a^{\sigma_j}| = 1 \text{ for all } j \} \subset K^* \). Hence, \( \ker(\psi) \) is cyclic and thus \( \ker(\psi) = \mu_K \). \( \square \)

We will next prove

Theorem 44.6. \( \psi(U_K) \) spans \( H \).

Then we will use a geometry theorem.

Theorem 44.7. If \( \wedge \) is a discrete subgroup of a real vector space \( \mathbb{R}^n \) that spans \( \mathbb{R}^n \), then \( \wedge \) is a free \( \mathbb{Z} \)-module of rank \( n \) and \( \text{vol}(\mathbb{R}^n/\wedge) < \infty \).

Corollary 44.8. \( \psi(U_K) \) is a free \( \mathbb{Z} \)-module of rank \( r_1 + r_2 - 1 \).

Proof of Theorem 44.7. Suppose \( \psi(U_K) \) does not span \( H = \overrightarrow{e} \). Then there is another hyperplane \( \mathcal{H}_2 = \overrightarrow{b} \perp \) with \( \overrightarrow{b} \neq 0, \overrightarrow{b} \in W \), \( \overrightarrow{b} \) is not any scalar multiple of \( \overrightarrow{e} \), such that \( \psi(U_K) \subset \mathcal{H}_2 \). By orthogonalization of \( \overrightarrow{b} \) relative to \( \overrightarrow{e} \), we may assume \( \overrightarrow{b} \cdot \overrightarrow{e} = 0 \). We will show that there exists \( u \in U_K \) with \( \psi(u) \cdot \overrightarrow{b} \neq 0 \).

Consider the map
\[
h : K \rightarrow V = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},
\]
\[
\alpha \mapsto (\alpha^{\sigma_j}).
\]

We have seen that \( h(\mathcal{O}_K) \) is a lattice in \( V \) of rank \( n \). Let \( \mathcal{L} \) be a symmetric, compact, convex region in \( V \). The Minkowski-Blichfeldt Lemma says that there is a constant \( A > 0 \) such that if \( \text{vol}(\mathcal{L}) \geq A \) then \( \mathcal{L} \) contains a non-zero point \( h(\alpha) \), \( \alpha \in \mathcal{O}_K \setminus \{0\} \). Let
\[
\mathcal{L} = \{ \overrightarrow{x} \in V : |x_j| \leq \rho_j, 1 \leq j \leq r_1 + r_2 \} \subset V.
\]

Then
\[
\text{vol}(\mathcal{L}) = \left( \prod_{1 \leq j \leq r_1} 2\rho_j \right) \left( \prod_{r_1 + 1 \leq j \leq r_1 + r_2} \pi \rho_j^2 \right) = 2^{r_1} \pi^{r_2} \rho_1 \cdots \rho_r \rho_{r_1 + 1}^2 \cdots \rho_{r_1 + r_2}^2.
\]
Choose $\rho$’s so that this equals $A$. Then for $\alpha \in \mathcal{O}_K$ with $\alpha \neq 0$, $h(\alpha) \in \mathcal{L}$, we have
\[
|N_{K/Q}(\alpha)| \leq \rho_1 \cdots \rho_{r_1} \rho_{r_1+1}^2 \cdots \rho_{r_1+r_2}^2 = \frac{A}{2^r_1 \pi^{r_2}} = A'.
\]
Also $|N_{K/Q}(\alpha)| \geq 1$. There are finitely many principal ideals $(\beta_j) \subset \mathcal{O}_K$ with $|N(\beta_j)| \leq A'$. Let
\[
B = \max_j |\psi(\beta_j) \cdot \bar{b}|.
\]
Claim: There is a vector $\vec{r} \subset V$ such that $\vec{r} \cdot \vec{e} = \log A'$, and $\vec{r} \cdot \vec{b} > B + (\log A') \sum |b_j|$. Actually
\[
\vec{r} = \frac{\log A'}{\vec{e} \cdot \vec{e}} \vec{e} + \frac{B + 1}{\vec{b} \cdot \vec{b}} \vec{b}
\]
works.

Define the $\rho_j$’s by
\[
\log \rho_j = j\text{-th coordinate of } \vec{r}, \quad 1 \leq j \leq r_1,
\]
\[
2 \log \rho_j = j\text{-th coordinate of } \vec{r}, \quad r_1 + 1 \leq j \leq r_1 + r_2.
\]
Then $\vec{r} \cdot \vec{e} = \log A'$ implies
\[
\rho_1 \cdots \rho_{r_1} \rho_{r_1+1}^2 \cdots \rho_{r_1+r_2}^2 = A'.
\]
So we have $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$ with $|\alpha^\sigma_j| \leq \rho_j$ for all $j$. So
\[
|\alpha^\sigma_j| = \frac{1}{|\prod_{i \neq j} \alpha^\sigma_i|} \geq \frac{1}{\prod_{i \neq j} \rho_i} = \frac{\rho_j}{A'}.
\]
So
\[
\frac{\rho_j}{A'} \leq |\alpha^\sigma_j| \leq \rho_j.
\]
So
\[
\log \rho_j - \log A' \leq \log |\alpha^\sigma_j| \leq \log \rho_j.
\]
Since $|N(\alpha)| \leq A'$, there is a $j$ such that $(\alpha) = (\beta_j)$. Then $u = \frac{\alpha}{\beta_j} \in U_K$. Hence,
\[
\psi(\alpha) \cdot \bar{b} = (\psi(\alpha) - \psi(\beta_j)) \cdot \bar{b}
\]
\[
\geq \psi(\alpha) \cdot \bar{b} - B
\]
\[
\geq \vec{r} \cdot \vec{b} - \sum_{j=1}^{r_1+r_2} (\log A')|b_j| - B
\]
\[
> 0 \text{ (by the choice of } \vec{r}).
\]
That proves $\vec{u} \not\in H_2$ and hence finishes the proof.
Index

absolute norm, 25, 31
absolute value, 36
adeles, 50
algebraic integer, 4
algebraic number, 4
Cauchy sequence, 41
Chinese Remainder Theorem for Dedekind Domains, 25
Chinese Remainder Theorem for Rings, 23
decomposition group, 58
derivation, 11
Dirichlet’s Unit Theorem, 66
discriminant, 12
dual module, 26
equivalent absolute values, 36
Fermat’s Two Square Theorem, 4
field algebra, 9
fractional ideal, 20, 21
greatest common divisor, 23
group ring, 9
Hensel’s Lemma, 47
Hilbert Basis Theorem, 19
Hilbert Class Field, 26
ideles, 52
idempotent, 16
inertia group, 58
inverse limit, 44
inverse of a fractional ideal, 21
Kable-Wright, 2006, 53
Law of Quadratic Reciprocity, 5
least common multiple, 23
lift, 26
Minkowski Bound, 63
Minkowski-Blichfeldt Lemma, 65
norm, 14
Ostrowski’s Theorem, 37
perfect field, 12
place, 38
Primitive Element Theorem, 13
primitive idempotent, 16
Principal Ideal Theorem, 26
radical, 16
ramification order, 56
relatively prime, 23
separable extensions, 13
Steinitz invariant, 53
Stickelberger-Schur Theorem, 29
tensor product, 10
Theorem of Haar, 50
torsion element, 52
Tower Laws, 15, 57
trace, 14
Tychonoff’s Theorem, 50
Weak Approximation Theorem, 39