Algebraic Number Theory

Fall 2014

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)

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 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. $S \subset R$ is a subring if: 1) S is closed under multiplication and addition; 2) 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 $\mathrm{im} f = \ker f$. The diagram

$$\begin{tikzcd} B \arrow[dr, "g"] & \\ A \arrow[u, "f"] \arrow[r, "h"] & C \end{tikzcd}$$

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., $\mathbb{Z}[x] = \{p(x) = c_0 x^n + c_1 x_{n-1} + \cdots + c_n : c_0, c_1, \cdots, c_n \in \mathbb{Z}\}$. ($\mathbb{Z}$ 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, π. e^π 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 transcentental) 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 or $2 \pmod 4$. 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 $\mathbb{N}(x + iy) = x^2 + y^2$. 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 $\mathbb{N}(p) \geq 9$ while $\mathbb{N}(2i) = 2i(-2i) = 4$. 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 $\mathbb{N}(p) = p^2 = (x^2 + y^2)(x'^2 + y'^2)$, 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 $x, y \in \mathbb{Z}$ iff $p \equiv \pm 1 \pmod 8$.*

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. (⇒) 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, $p = x^2 - 2y^2 \equiv 1 - 2 \cdot \{0, 1, 4\} \pmod 8 \equiv 1, -1 \pmod 8$.

(⇐) 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 $\mathbb{N}(p) = p^2$ divides $\mathbb{N}(2\sqrt{2}) = (2\sqrt{2}) \cdot (-2\sqrt{2}) = -8$. 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 $\mathbb{N}((x + \sqrt{2}y)(1 + \sqrt{2})) = (x^2 - 2y^2) \cdot (1 - 2) = -(x^2 - 2y^2) = p$. □

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. (⇒) If $p = x^2 + 6y^2$, then $x^2 \equiv -6y^2 \pmod p$, hence $-6 \equiv m^2 \pmod p$ since $x, y \not\equiv 0 \pmod p$. Therefore, $(\frac{-6}{p}) = 1$ since $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ (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 $(\frac{-6}{p}) = (\frac{-1}{p}) \cdot (\frac{2}{p}) \cdot (\frac{3}{p})$. We have

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

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

(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 $(\frac{3}{p}) = (\frac{-1}{p})(\frac{p}{3})$. So $(\frac{-6}{p}) = (\frac{-1}{p})(\frac{2}{p})(\frac{-1}{p})(\frac{p}{3}) = (\frac{2}{p})(\frac{p}{3})$. Then

$$\begin{aligned}(\frac{-6}{p}) = 1 &\Leftrightarrow (\frac{2}{p}) = (\frac{p}{3}) = 1 \text{ or } (\frac{2}{p}) = (\frac{p}{3}) = -1 \\ &\Leftrightarrow p \equiv \pm 1 \pmod 8, p \equiv 1 \pmod 3 \text{ or } p \equiv \pm 3 \pmod 8, p \equiv 2 \pmod 3\end{aligned}$$

The Chinese Remainder Theorem implies

$$(\frac{-6}{p}) = 1 \Leftrightarrow p \equiv 1, 5, 7, 11 \pmod{24}.$$

($\Leftarrow$) 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 $(p) = \mathfrak{p}\overline{\mathfrak{p}}$. $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ happens for $p \equiv 1, 5, 7, 11 \pmod{24}$. In addition, $\mathfrak{p} = (x + y\sqrt{-6})$ is a principal ideal iff $p \equiv 1, 7 \pmod{24}$. $\square$

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 $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ are equivalent if there exists $\alpha, \beta \in \mathcal{O}_K \backslash \{0\}$ such that

$$\alpha\mathfrak{a} = \beta\mathfrak{b}.$$

Under multiplication $\mathfrak{ab}$ of ideals, the equivalence classes form a group, called the class group of K. $\mathfrak{a}$ is principal iff $\mathfrak{a} \sim (1) = \mathcal{O}_K$. 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 $\mathrm{Re}(s) > 0$. It has a meromorphic continution to the whole complex plane $\mathbb{C}$ which is holomorphic except for a single pole at $s = 1$ with residue $\mathrm{Res}_{s=1}\zeta(s) = 1$. If $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\,dt$, then $\Lambda(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ 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):

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

for $x > 0$.

All the zeroes ρ of $\zeta(s)$ are either

$$\rho = -2, -4, -6, \cdots$$

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

$$\pi(x) = \sum_{p<x} 1 \sim \mathrm{li}(x) = \int_2^\infty \frac{dt}{\ln(t)}$$

was derived by proving all the nontrivial zeroes are in $0 < \mathrm{Re}(\rho) < 1$. The Riemann Hypothesis is that all nontrivial zeroes have $\mathrm{Re}(\rho) = \frac{1}{2}$. 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

$$\zeta_K(s) = \prod_{\text{prime ideals } \mathfrak{p} \text{ in } \mathcal{O}_K} (1 - (N\mathfrak{p})^{-s})^{-1}$$

where $N\mathfrak{p} = [\mathcal{O}_K : \mathfrak{p}]$ is the absolute norm of ideal $\mathfrak{p}$.

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

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |d_K|^{\frac{1}{2}}}$$

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

$$\left(\sum x_g g\right) + \left(\sum y_g g\right) = \sum \left(x_g + y_g\right) g$$

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

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \text{ where } ij = k = -ji, i^2 = j^2 = -1,$$

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

$$\begin{aligned} \mathbb{R}[Q_8] &\to \mathbb{R}[Q_8] \\ q &\mapsto q + (-1)q \end{aligned}$$

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 $\oplus_{i=1}^t L_i$ 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

$$\begin{aligned} M \times N &\xrightarrow{\varphi} P \\ (m,n) &\mapsto \varphi(m,n) \end{aligned}$$

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

$$\begin{aligned} M \times N &\xrightarrow{c} M \otimes_R N \xrightarrow{h} P \\ (m,n) &\mapsto m \otimes n \end{aligned}$$

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

If K/F is a finite separable field field extension, then $K = F(\alpha)$ for a root α 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 $(K : F) = \sum (L_i : L)$. $\square$

Example 5.6. For $d \in \mathbb{Z}$, d is square-free, $\mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} \mathbb{R} = \oplus_{i=1}^t L_i$ 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 $\sqrt{d} \in \mathbb{R}$.

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

Remark 6.1. *Here is another application of tensor products. Consider the following tensor product*

$$\mathbb{Z}[\sqrt{d}] \otimes_{\mathbb{Z}} (\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}[\sqrt{d}]/7\mathbb{Z}[\sqrt{d}].$$

Even though $\mathbb{Z}/7\mathbb{Z}$ is a field, this tensor product is not always a field. For example, for $d = 2$, $\mathbb{Z}[\sqrt{2}]/7\mathbb{Z}[\sqrt{2}]$ has zero divisors

$$(3+\sqrt{2})(3-\sqrt{2}) = 7 = 0.$$

$F[x]$ is a F-vector space with basis $\{1, x, x^2, \cdots, \}$. 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:*

$$D(x^m x^n) = D(x^m)x^n + x^m D(x^n).$$

If char$(F) = 0$, then $D(f) = f' = 0$ if and only if f is constant. If char$(F) = p$, $D(\sum a_n x^n) = \sum a_n n x^{n-1} = 0$ if and only if $p|n$ or $a_n = 0$ if and only if $f(x) = \sum b_n x^{p^n} = g(x^p)$.

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

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

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

Proof. (i)⇒(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, α'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)⇒(iii) If $g = (f, f') \neq 1$, then $g(\alpha_j) = 0$ for some root α_j of f. Since $g|f'$, that implies $f'(\alpha_j) = 0$, contrary to (ii).

(iii)⇒(i) Suppose f is not separable. Then $\alpha_i = \alpha_j$ for some $i \neq j$. Then $f = (x-\alpha_i)^2 g(x)$ for some $g(x)$. Then $f'(x) = 2(x-\alpha_i)g(x) + (x-\alpha_i)^2 g'(x)$ is divisible by $x - \alpha_i$, so $(f, f') \neq 1$. □

7 Discriminant, Separable Extensions (09/03)

Definition 7.1. Let $f(x) = (x - \alpha^{\sigma_1}) \cdots (x - \alpha^{\sigma_n})$ be an irreducible polynomial of α over F and $E = F(\alpha)$. Then the *discriminant* of f is defined as

$$\begin{aligned}\mathrm{Disc}(f) &= \prod_{1 \le i < j \le n} (\alpha^{\sigma_j} - \alpha^{\sigma_i}) \\ &= (-1)^{\frac{n(n-1)}{2}} \cdot f'(\alpha^{\sigma_1}) \cdots f'(\alpha^{\sigma_n}).\end{aligned}$$

Corollary 7.2. *f is separable iff Disc$(f) \neq 0$.*

Remark 7.3. *The Vandermonde determinant of $T_1, T_2, \cdots, T_n$ is*

$$V(T_1, \cdots, T_n) = \det \begin{bmatrix} 1 & T_1 & \cdots & T_1^{n-1} \\ 1 & T_2 & \cdots & T_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & T_n & \cdots & T_n^{n-1} \end{bmatrix} = \prod_{1 \le i < j \le n} (T_j - T_i).$$

Hence, Disc$(f) = V(\alpha^{\sigma_1}, \cdots, \alpha^{\sigma_n})^2$.

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) char$(F) = 0$ or (ii) 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 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

$$\begin{aligned} g(x^p) &= (g_1(x))^p \\ &= (c_0 + c_1 x + \cdots + c_l x^l)^p \\ &= c_0^p + c_1^p x^p + \cdots c_l^p x^{lp}. \end{aligned}$$

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 $f'(x) = px^{p-1} - 0 = 0$, $(f, f') \neq 1$, and so f is inseparable. Let $F = K(T)$, and let α 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 $r \geq 1$ iff $r = p$. If $(x-\alpha)^r \in F[x]$, then $(-\alpha)^r$ (where $x = 0$) is in F. So $\alpha^r \in F$ and $\alpha^p \in F$. 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 $K[T]$. □

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

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* $\Leftrightarrow$ *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* α *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

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

Theorem 8.1.

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

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

$$[u_j^{\sigma_i}]\overrightarrow{l} = \overrightarrow{0}.$$

Then for each i,

$$\sum_{j=1}^{n} u_i^{\sigma_j} l_j = 0.$$

For any $c_1, \cdots, c_n \in F$,

$$\sum_{i=1}^{n} c_i \sum_{j=1}^{n} u_i^{\sigma_j} l_j = 0.$$

Hence,

$$\sum_{j=1}^{n} (\sum_{i=1}^{n} c_i u_i)^{\sigma_j} l_j = 0$$

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. □

If $(w_1, \cdots, w_n)$ 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,

$$V^*(w_1, \cdots, w_n) = \det([c_{ij}]) V^*(u_1, \cdots, u_n).$$

Example 8.2. If $E = F(\alpha)$, α is separable over F, $\sigma_i \in \mathrm{Gal}(E/F)$ and we take the basis to be $(1, \alpha, \cdots, \alpha^{n-1})$, then

$$\begin{aligned} V^*(1, \alpha, \cdots, \alpha^{n-1}) &= V(\alpha^{\sigma_1}, \cdots, \alpha^{\sigma_n}) \text{ (Vandermonde determinant)} \\ &= \prod_{1 \leq i < j \leq n} (\alpha^{\sigma_i} - \alpha^{\sigma_j}) \\ &\neq 0. \end{aligned}$$

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 $E = F(\alpha), H = F(\alpha^{\sigma_1}, \cdots, \alpha^{\sigma_n})$), $\mathrm{Gal}(H/F)$ fixes $t_{E/F}(\alpha), N_{E/F}(\alpha)$. Hence they are in F.

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

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

So

$$[t_{E/F}(u_i u_j)] = [u_i^{\sigma_k}][u_i^{\sigma_k}]^T,$$

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

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

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 $(v_1, \cdots, v_n)$ 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 $(v_1, \cdots, v_n)$.

$$\mathrm{Trace}(l_a) = \sum_{i=1}^{n} c_{ii} = t_{A/F}(a),$$

$$\mathrm{Norm}(l_a) = \det[c_{ij}] = N_{A/F}(a).$$

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* Ae *is a subalgebra of* A *since* $(ae)(be) = (ab)e^2 = (ab)e$*.* Ae *is a vector space over* F*, and* $1 \leq \dim_F Ae \leq \dim_F A$*.*

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* $A = \oplus_{i=1}^n Ae_i$*.*

Remark 9.6. *(i)* e *is primitive iff* Ae *is indecomposible, meaning* Ae *cannot be written as* $B \oplus C$ *for nonzero algebras* B, C*.*
(ii) If $A = \oplus_{i=1}^n A_i = \prod_{i=1}^n A_i$ *where* $A_i = Ae_i$*, 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

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

Theorem 9.8. *Rad*(A) *is an ideal of* A*.*

Proof. Clearly $0 \in \mathrm{Rad}(A)$. 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 $\overline{A} = A/Rad(A)$, then $Rad(\overline{A}) = 0$.*

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 $a \in \text{Rad}(A)$. □

Theorem 9.10. *If A is an indecomposible finite F-algebra and $Rad(A) = 0$, 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) $Rad(A) = 0$.
(ii) $A = \oplus_{i=1}^t A_i$ where each A_i is a field extension of F.
Moreover, if F is perfect, then (i), (ii) are equivalent to (iii), (iv):
(iii) $d(v_1, \cdots, v_n) \neq 0$ for some basis $v_1, \cdots, v_n$ of A over F.
(iv) $d(v_1, \cdots, v_n) \neq 0$ for all basis $v_1, \cdots, v_n$ 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 $v_1, \cdots, v_n$ is a basis of A over F, then $av_i = \sum_{i=1}^n c_{ij} v_j$ for $c_i j \in F$. So $[c_{ij}]$ is the matrix of l_a with respect to $v_1, \cdots, v_n$. Let $p(x) = \det(xI_n - [c_{ij}]) = x^n + u_1 x^{n-1} + \cdots + u_n$. By Cayley-Hamilton Theorem, $A = [c_{ij}]$ satisfies $p(A) = A^n + u_1 A^{n-1} + \cdots + u_n I = 0$. Since $a^m = 0$ for some $m \geq 1$, then $l_a^m(b) = 0$ for all b, and $[c_{ij}]^m = 0$. Also, all the eigenvalues of $[c_{ij}]$ are 0 in some algebraic closure $\overline{F}$ 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 $t_{A/F}(a) = 0$. □

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 $a \in \mathfrak{R} \subset \mathcal{O}$ where $\mathfrak{R}$ is a subring of $\mathcal{O}$ containing $\mathfrak{o}$ and is a finitely generated $\mathfrak{o}-$module.*

Proof. ($\Rightarrow$) By Theorem 10.1, $\mathfrak{R} = \mathfrak{o}[a]$ is a subring that works.
($\Leftarrow$) Suppose $\mathfrak{R} = (r_1, \cdots, r_n)\mathfrak{o} = r_1\mathfrak{o} + \cdots + r_n\mathfrak{o}$. Then

$$ar_i = \sum_{j=1}^n c_{ij} r_j$$

for some $c_{ij} \in \mathfrak{o}$. Then $p(x) = \det(xI_n - [c_{ij}]) = x^n +$ 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 $\mathfrak{o}$. $\square$

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^{σ_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 $\mathfrak{o} \subset K$. Then $p(x) = \prod_{j=1}^n (x - a^{\sigma_j})$. so a^{σ_j} is integral over $\mathfrak{o}$. $\square$

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 $N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq M$ 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 ($\Leftrightarrow$ 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 $d = \max(\deg(f_i))$. 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 $0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{m} \subsetneq R$.

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 $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_l$ in $\mathfrak{o}$.

Theorem 12.4. *Every nonzero ideal $\mathfrak{a}$ of a Dedekind domain may be written as a product of prime ideals $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_\mathfrak{n}$ 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

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0 \tag{12.1}$$

for $c_i \in R$. Suppose $\alpha = a/b$ for $a, b \in K$ and a, b have no non-unit common divisor. Substituting α with a/b in equation (12.1) and multiplying each side by b^n, we get

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1ab^{n-1} + c_0b^n = 0 \tag{12.2}$$

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 $(p) \subsetneq (m) \subsetneq \mathfrak{o}$. Then $p = mx$ for some $x \in \mathfrak{o}, x \notin \mathfrak{o}^*$ (x is not a unit). Since $(m) \subsetneq \mathfrak{o}$, $m \notin \mathfrak{o}^*$. 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 $\mathfrak{b} \subset K$ is a *fractional ideal* if there exists $c \in K^*$ and a nonzero ideal $\mathfrak{a} \subset \mathfrak{o}$ such that $\mathfrak{b} = c\mathfrak{a}$.

Theorem 12.8 (D1). *Suppose $\mathfrak{o}$ is Noetherian and integrally closed, and $\mathfrak{a}$ is any fractional ideal of $\mathfrak{o}$, then*

$$\{x \in K | x\mathfrak{a} \subset \mathfrak{a}\} = \mathfrak{o}.$$

Proof. Clearly $\mathfrak{o} \subset \{x \in K | x\mathfrak{a} \subset \mathfrak{a}\}$, since $\mathfrak{a}$ is fractional ideal of $\mathfrak{o}$. For the reverse inclusion, since $\mathfrak{o}$ is Noetherian, $\mathfrak{a} = (c_1, c_2, \cdots, c_m)\mathfrak{o}$. If $b\mathfrak{a} \subset \mathfrak{a}$, 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, $\mathfrak{a} \subset K$ 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 $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$ for nonzero prime ideals $\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_n$, then $\mathfrak{p} = \mathfrak{p}_j$ for some j.*

Proof. By induction on n. For $n = 1$, if $\mathfrak{p} \supset \mathfrak{p}_1$, then since prime ideals are maximal, we have $\mathfrak{p} = \mathfrak{p}_1$.

Assume the theorem is true for $n-1$. Suppose $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$ and $\mathfrak{p} \neq \mathfrak{p}_n$. Then there exists $c \in \mathfrak{p}_n \backslash \mathfrak{p}$. (Again since prime ideals are maximal) Let $b \in \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}$. Then $bc \in \mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{p}$. Since $c \notin \mathfrak{p}$, we must have $b \in \mathfrak{p}$, since $\mathfrak{p}$ is prime. Thus $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}$ and by the induction assumption $\mathfrak{p} = \mathfrak{p}_j$ for some $1 \leq j \leq n-1$. $\square$

Let $\mathfrak{a}$ be a (nonzero) fractional ideal of $\mathfrak{o}$. Define the *inverse of a fractional ideal* to be

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subset \mathfrak{o}\}.$$

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

For any fractional ideals $\mathfrak{a}, \mathfrak{b}$, $\mathfrak{a}\mathfrak{b} \stackrel{\text{def}}{=} \{\sum_{i=1}^{t} a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ is also a fractional ideal.

Definition 12.11. $\mathfrak{a}$ is invertible iff $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}$.

Theorem 12.12. *Every fractional ideal in a Dedekind domain $\mathfrak{o}$ is invertible.*

Remark 12.13. *If $\mathfrak{o}$ is a field, there are only two ideals: 0 and $\mathfrak{o}$.*

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

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

Proof. Suppose $ab \in \mathfrak{m}$ and $a \in \mathfrak{o} \backslash \mathfrak{m}$ and $b \in \mathfrak{o}$. Consider $\mathfrak{m} + a\mathfrak{o} \supsetneq \mathfrak{m}$. Since $\mathfrak{m} \subset S$, $\exists c \in K \backslash \mathfrak{o}$ such that $c\mathfrak{m} \subset \mathfrak{o}$. Then $c(\mathfrak{m} + a\mathfrak{o}) = c\mathfrak{m} + ca\mathfrak{o}$. $\mathfrak{m} + a\mathfrak{o}$ can not be in S because $\mathfrak{m}$ is maximal in S. So $ca \notin \mathfrak{o}$. Now consider $\mathfrak{m} + b\mathfrak{o} \supseteq \mathfrak{m}$ ($b\mathfrak{o} \subset \mathfrak{o}$). Then $ac(\mathfrak{m} + b\mathfrak{o}) = ac\mathfrak{m} + c(ab)\mathfrak{m} \subset \mathfrak{o}$ ($c\mathfrak{m} \in \mathfrak{o}$, $ab \in \mathfrak{m}$). By maximality, $\mathfrak{m} + b\mathfrak{o}$ is in S and contains $\mathfrak{m}$ and so $\mathfrak{m} + b\mathfrak{o} = \mathfrak{m}$. So $b \in \mathfrak{m}$. That proves $\mathfrak{m}$ is prime.

$\mathfrak{m}$ is maximal by definition of Dedekind domain. Then $\mathfrak{m}\mathfrak{m}^{-1}$ is an ideal containing $\mathfrak{m}$ and so $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ or $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{o}$. If $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$, then by theorem 12.8 that $\{x \in K | x\mathfrak{a} \subset \mathfrak{a}\} = \mathfrak{o}$ then we'd have $\mathfrak{m}^{-1} \subset \mathfrak{o}$. Since $\mathfrak{m} \subset S$, there is a $c \in \mathfrak{m}^{-1} \backslash \mathfrak{o}$. That contradiction proves $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{o}$. $\square$

13 Dedekind Domains II (09/17)

Theorem 13.1 (D4)**.** *Let $\mathfrak{o}$ be a Dedekind domain. A nonzero ideal $\mathfrak{a}$ in $\mathfrak{o}$ is invertible iff $\mathfrak{a} = \mathfrak{m}_1 \cdots \mathfrak{m}_r$ for some invertible prime ideals $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$.*

Proof. ($\Leftarrow$) Ideal multiplication is associative and commutative:

$$\mathfrak{ab} = \mathfrak{ba}, \ (\mathfrak{ab})\mathfrak{c} = \mathfrak{c}(\mathfrak{bc}).$$

Hence,

$$(\mathfrak{m}_1^{-1} \cdots \mathfrak{m}_r^{-1})(\mathfrak{m}_1 \cdots \mathfrak{m}_r) = (\mathfrak{m}_1^{-1}\mathfrak{m}_1) \cdots (\mathfrak{m}_r^{-1}\mathfrak{m}_r) = \mathfrak{o}.$$

Thus, $\mathfrak{a}^{-1} = \mathfrak{m}_1^{-1} \cdots \mathfrak{m}_r^{-1}$ satisfies $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$.

($\Rightarrow$) Assume $\mathfrak{a} \neq 0$ is a proper invertible ideal. Then $\mathfrak{a} \subset \mathfrak{o}\backslash\mathfrak{o}^*$. Since $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$, there are $a_1, \cdots, a_n \in \mathfrak{a}$ and $b_1, \cdots, b_m \in \mathfrak{a}^{-1}$ such that $a_1b_1 + \cdots + a_nb_n = 1$. Some b_j is not in $\mathfrak{o}$ (otherwise $1 \in \mathfrak{a}$). Thus $\mathfrak{a}^{-1} \neq \mathfrak{o}$ and $\mathfrak{o}$ belongs to the family of ideals S. Then there is a maximal $\mathfrak{m}_1$ in S such that $\mathfrak{a} \subset \mathfrak{m}_1$. Since $\mathfrak{m}_1$ is invertible by Theorem 12.14, we have $\mathfrak{m}_1^{-1}\mathfrak{a} \subset \mathfrak{o}$ and $\mathfrak{a} \subset \mathfrak{m}_1^{-1}\mathfrak{a}$. If $\mathfrak{m}_1^{-1}\mathfrak{a} = \mathfrak{o}$, then $\mathfrak{m}_1(\mathfrak{m}_1^{-1}\mathfrak{a}) = \mathfrak{a} = \mathfrak{m}_1$. Otherwise repeat the process with the nonzero proper ideal $\mathfrak{m}_1^{-1}\mathfrak{a}$ to produce another $\mathfrak{m}_2$ and so on. Then we get a sequence

$$\mathfrak{a} \subset \mathfrak{m}_1^{-1}\mathfrak{a} \subset \mathfrak{m}_1^{-1}\mathfrak{m}_2^{-1}\mathfrak{a} \subset \cdots \subset \mathfrak{o}.$$

Since $\mathfrak{o}$ is Noetherian, this ascending sequence must terminate with $\mathfrak{a} = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_r$. □

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

Proof. Pick $a \in \mathfrak{p}\backslash\{0\}$. Then $a\mathfrak{o}$ is invertible because $(a\mathfrak{o})^{-1} = \frac{1}{a}\mathfrak{o}$ and $(a\mathfrak{o})(a\mathfrak{o})^{-1} = \mathfrak{o}$. By Theorem 13.1, $a\mathfrak{o} = \mathfrak{m}_1 \cdots \mathfrak{m}_r$ where $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ are invertible prime ideals. So $\mathfrak{p} \supset a\mathfrak{o} = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. So by Theorem 12.10, $\mathfrak{p} = \mathfrak{m}_j$ for some j. □

Theorem 13.3 (D6). *Every nonzero ideal* $\mathfrak{a}$ *in a Dedekind domain* $\mathfrak{o}$ *is a product of prime ideals* $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Proof. If $\mathfrak{a} = \mathfrak{o}$, then we are donw with $r = 1$. If $\mathfrak{a} \subsetneq \mathfrak{o}$, then $\mathfrak{a}$ is contained in a maximal (hence prime) ideal $\mathfrak{a} \subset \mathfrak{p}_1 \subset \mathfrak{o}$. Then $\mathfrak{a} \subset \mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathfrak{o}$. If $\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{o}$, then $\mathfrak{a} = \mathfrak{p}_1(\mathfrak{p}_1^{-1}\mathfrak{a}) = \mathfrak{p}_1$. Otherwise, repeat the process for $\mathfrak{a} \subset \mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\mathfrak{a} \subset \cdots$. Since $\mathfrak{o}$ is Noetherian, we must have $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$ at some point. □

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

Proof. Suppose $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ for prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{q}_1 \cdots \mathfrak{q}_s$ with $r \geq 0$ as small as possible. Then by Theorem 12.10 $\mathfrak{p}_1 = \mathfrak{q}_j$ for some j. Renumber so that $j = 1$ and $\mathfrak{p}_1 = \mathfrak{q}_1$. Then by Theorem 13.2, $\mathfrak{p}_1^{-1}(\mathfrak{p}_1 \cdots \mathfrak{p}_r) = \mathfrak{q}_1^{-1}(\mathfrak{q}_1 \cdots \mathfrak{q}_s)$ reduces to $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. That contradicts r being minimal. □

Corollary 13.5. *In a Dedekind domain, every fractional ideal* $\mathfrak{a}$ *can be uniquely written as* $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ *for distinct prime ideals* $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ *and nonzero integers* $a_1, \cdots, a_r$ *up to rearrangement.*

14 Dedekind Domains III (09/19)

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 $\mathfrak{a}|\mathfrak{b}$ if there is an ideal $\mathfrak{c} \subset \mathfrak{o}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Proposition 14.3. $\mathfrak{a}|\mathfrak{b} \Leftrightarrow \mathfrak{a} \supset \mathfrak{b}$.

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

Remark 14.5. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$.

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

Remark 14.7. *$lcm(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$.*

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

15 Chinese Remainder Theorem for Rings(09/22)

Theorem 15.1 (Chinese Remainder Theorem for Rings)**.** *Let R be a ring with 1. Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be two-sided ideals in R such that $\mathfrak{a}_i + \mathfrak{a}_j = \mathfrak{o}$ for any $i \neq j$. Then the map*

$$R/(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) \to \prod_{i=1}^{n} R/\mathfrak{a}_i$$

defined by

$$x + (\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) \mapsto (x + \mathfrak{a}_i)$$

is an R-module isomorphism.

Proof. This map is clearly well-defined and a module homomorphism. It is injective since if $x \in \mathfrak{a}_i$ for all i, then $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. To prove surjectivity, we use induction on n, and then it suffices to prove the theorem for $n = 2$ ideals. Since $\mathfrak{a}_1 + \mathfrak{a}_2 = R$, there are $a_1 \in \mathfrak{a}_1$ and $a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. Suppose we are given $(y_1 + \mathfrak{a}_1, y_2 + \mathfrak{a}_2) \in R/\mathfrak{a}_1 \times R/\mathfrak{a}_2$. Let $x = y_2 a_1 + y_1 a_2$. Then

$$x = y_2 a_1 + y_1(1 - a_1) = y_1 - y_1 a_1 + y_2 a_1 \equiv y_1 \pmod{\mathfrak{a}},$$

and

$$x = y_2(1-a_2) + y_1 a_2 = y_2 - y_2 a_2 + y_1 a_2 \equiv y_2 \pmod{\mathfrak{a}_2}.$$

For $n > 2$ assume the theorem is true for $n-1$ ideals, since it is true for 2 ideals, we can say

$$R/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \cong (R/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1}) \times R/\mathfrak{a}_n$$

if $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} + \mathfrak{a}_n = R$. Since $\mathfrak{a}_i + \mathfrak{a}_n = R$ for $1 \le i \le n-1$, then $u_i + v_i = 1$ for some $u_i \in \mathfrak{a}_i, v_i \in \mathfrak{a}_n$. So $1 = (u_1 + v_1) \cdots (u_n + v_n) = u_1 u_2 \cdots u_n +$ multiple of v's $\in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} + \mathfrak{a}_n$. $\square$

Theorem 15.2. *For every proper prime ideal $\mathfrak{p}$ in a Dedekind domain $\mathfrak{o}$, $\mathfrak{o} \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \mathfrak{p}^3 \supsetneq \cdots$.*

Proof. The inequalities follow from unique factorization into prime ideals. $\square$

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

Proof. Let $\mathfrak{b} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_t^{m_t}$. For each j, suppose $\mathfrak{p}_j^{n_j}$ exactly divides $\mathfrak{a}$. Pick $\alpha_j \in \mathfrak{p}_j^{n_j} \backslash \mathfrak{p}_j^{n_{j+1}}$. Pick $\alpha \equiv \alpha_j \pmod{\mathfrak{p}_j^{n_{j+1}}}$ for all j, by Chinese Remainder Theorem. Then $\alpha \in \mathfrak{p}_j^{n_j}$ for all j. Hence, $\alpha \in \prod_{j=1}^k \mathfrak{p}_j^{n_j}$, then $\alpha\mathfrak{o} = \left(\prod_{j=1}^k \mathfrak{p}_j^{n_j}\right)$ is a product of primes $\mathfrak{q} \neq$ any $\mathfrak{p}_j$. Since $\alpha\mathfrak{o} \subset \mathfrak{a}$, $\mathfrak{a} | \alpha\mathfrak{o}$, and together with the assumption that $\mathfrak{p}_j^{n_j}$ exactly divides $\mathfrak{a}$, $(\alpha\mathfrak{o})\mathfrak{a}^{-1} = \alpha\mathfrak{a}^{-1}$ is a product of primes $\mathfrak{q} \neq$ any $\mathfrak{p}_j$. So $\alpha\mathfrak{a}^{-1}$ is relatively prime to $\mathfrak{b}$, and so $\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{o}$. $\square$

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

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

16 Valuation (09/24)

Definition 16.1. For a prime $\mathfrak{p}$ and an ideal $\mathfrak{a} \neq 0$, we define the $\mathfrak{p}$-*adic valuation* of $\mathfrak{a}$ to be

$$v_{\mathfrak{p}}(\mathfrak{a}) = \text{exponent of } \mathfrak{p} \text{ in the prime factorization of } \mathfrak{a}.$$

Remark 16.2. *Properties of valuation:*
(i) $v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$.
(ii) If $\mathfrak{a}|\mathfrak{b}$, *then* $v_{\mathfrak{p}}(\mathfrak{a}) \le v_{\mathfrak{p}}(\mathfrak{b})$.
(iii) $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$.
(iv) $v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$.
(v) $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) + v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$.
(vi) $\mathfrak{a} + \mathfrak{b} = \mathfrak{o} \Leftrightarrow \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

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

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

Remark 16.5. *Properties of absolute value:*
(i) $|\alpha\beta|_{\mathfrak{p}}=|\alpha|_{\mathfrak{p}}|\beta|_{\mathfrak{p}}$.
(ii) $|\alpha+\beta|_{\mathfrak{p}}\leq \max(|\alpha|_{\mathfrak{p}},|\beta|_{\mathfrak{p}})\leq|\alpha|_{\mathfrak{p}}+|\beta|_{\mathfrak{p}}$.

$|\cdot|_{\mathfrak{p}}$ is a $\mathfrak{p}$-adic absolute value. Extend $|\cdot|_{\mathfrak{p}}$ to $|0|_{\mathfrak{p}}=0$, $|\cdot|_{\mathfrak{p}}$ defines a metric on K. The completion of K relative to this metric is $K_{\mathfrak{p}}$ (the field of $\mathfrak{p}$-adic numbers).

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

Proof. Define an isomorphism

$$f:\mathfrak{o}/\mathfrak{p}\to\mathfrak{p}^n/\mathfrak{p}^{n+1}.$$

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

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

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

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

Theorem 16.7 (Chinese Remainder Theorem for Dedekind Domains)**.** *For an ideal $\mathfrak{a}$ in a Dedekind domain $\mathfrak{o}$ with prime factorization $\mathfrak{a}=\mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}$ where each $\mathfrak{p}_j$ is distinct. Then $\mathfrak{o}/\mathfrak{a}\cong\prod_{i=1}^r\mathfrak{o}/\mathfrak{p}_j^{m_j}$.*

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

$$N(\mathfrak{p})=[\mathfrak{o}:\mathfrak{p}].$$

Remark 16.9. $N(\mathfrak{a})=[\mathfrak{o}:\mathfrak{a}]=\prod_{j=1}^r N(\mathfrak{p}_j)^{m_j}$ *for* $\mathfrak{a}=\mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}$.

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

Let $I_{\mathfrak{o}}$ be the group of fractional ideals $\mathfrak{a}$ in the Dedekind domain $\mathfrak{o}$, $P_{\mathfrak{o}}$ be the subgroup of principal ideals $(\alpha)=\alpha\mathfrak{o}$, $\mathrm{Cl}(\mathfrak{o})=I_{\mathfrak{o}}\backslash P_{\mathfrak{o}}$ be the class group. Then $1\to\mathfrak{o}^*\hookrightarrow K^*\to I_{\mathfrak{o}}\to\mathrm{Cl}(\mathfrak{o})\to 1$ is exact.

Corollary 17.1. *$Cl(\mathfrak{o}) = 1$ if and only if $\mathfrak{o}$ is a PID.*

If L is a finite separable extension of K, $\mathfrak{o}$ is the ring of integers of K, and $\mathcal{O}_L$ is the integral closure of $\mathfrak{o}$ in L, then for any ideal $\mathfrak{a} \subset \mathfrak{o}$, $\mathfrak{a}\mathcal{O}_L$ is an ideal in $\mathcal{O}_L$. $\mathfrak{a}\mathcal{O}_L$ is called the *lift* of $\mathfrak{a}$ to $\mathcal{O}_L$.

Theorem 17.2 (Principal Ideal Theorem (Furtwungler, 1929))**.** *For any algebraic number field $K/\mathbb{Q}$, there is a finite extension L/K such that every ideal $\mathfrak{a}$ in $\mathfrak{o}_K$ lifts to a principal ideal in $\mathcal{O}_L$. The smallest degree extension H_K with this property is uniquely determined, it's Galois over K, and $\mathrm{Gal}(H/K) \cong Cl(\mathfrak{o}_K)$. 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 $p|u^2 + 6v^2$, the ideal $\mathfrak{p} = (p, u + \sqrt{-6}v)$ is principal. It will turn out that $Cl(\mathbb{Q}(\sqrt{-6})) \cong C_2$. $\mathfrak{p}$ is 1 in $Cl(\mathbb{Q}(\sqrt{-6}))$ if and only if $p \equiv 1, 7 \pmod{24}$.*

18 Extensions of Dedekind Domain I (09/29)

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. Consider the trace

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

We have $t_{L/K}(x) \subset \mathfrak{o}$. This is because the embeddings σ 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 σ. So $t_{L/K}(x)$ is invariant under $\mathrm{Gal}(N/K)$. So $t_{L/K}(x) \in K$ for all $x \in L$. Each x^{σ_i} is an algebraic integer. So $t_{L/K}(x) \in K \cap \mathcal{O}_L = \mathfrak{o}$ since $\mathfrak{o}$ is integrally closed.

Definition 18.1. For any $\mathfrak{o}$-submodule $X \subseteq L$, the *dual module* of X is defined as

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

Remark 18.2. *(i) $(X^D)^D = X$.*
(ii) If $X \subset Y$, then $Y^D \subset X^D$.
(iii) $t_{L/K}(\mathcal{O}_L) \subset \mathfrak{o}$ implies that ${\mathcal{O}_L}^D \supseteq \mathcal{O}_L$.

Proposition 18.3. *Suppose $\{x_1, \cdots, x_n\}$ is a basis of L/K. Let $X = x_1\mathfrak{o} + \cdots + x_n\mathfrak{o}$ be a free $\mathfrak{o}$-submodule of L. For every j, $\exists\ y_i \in L$ with $t_{L/K}(x_i y_j) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases}$*

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

$(L : K) = n$, $\dim_K L = n = \dim_K(K^n)$. Since the kernel is 0, the map is surjective. So there is some y_i such that

$$\big(t_{N/L}(x_i y_j)\big)_{i=1}^{n} = \vec{e_j} = \begin{bmatrix} 0 \\ \cdots \\ 1 \\ \cdots \\ 0 \end{bmatrix}$$

$\square$

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 $t_{L/K}(yx_i) = c_i \in \mathfrak{o}$ for all i. $\square$

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

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

Since $t_{L/K}\left(x + y\sqrt{-6}\right) = 2x$, $t_{L/K}\big((x + y\sqrt{-6})\sqrt{-6}\big) = -12y$, then $\mathcal{O}_L^D = \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{\sqrt{-6}}{12}$, 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 $ac_1x_1, \cdots, ac_nx_n$ 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 $\mathcal{P} \cap \mathfrak{o} = \mathfrak{p}$ is a prime ideal in $\mathfrak{o}$. $\mathfrak{p}\mathcal{O}_L$ is an ideal in $\mathcal{O}_L$.

We claim that $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. In K, we know that $\mathfrak{p}^{-1} \supsetneq \mathfrak{o}$ because $\mathfrak{o}$ is a Dedekind domain. Then $\mathfrak{p}^{-1} \not\supseteq \mathcal{O}_L$ because $\mathcal{O}_L \cap K = \mathfrak{o}$ by integral closure. Then $\mathfrak{p}\mathcal{O}_L \not\subset \mathcal{O}_L$.

Then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{A}$ is a commutative algebra over $\mathfrak{o}/\mathfrak{p} = k$. Since $\mathcal{O}_L$ 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 decomposable algebra. $\mathcal{A}_i$ is a field iff $\operatorname{Rad}(\mathcal{A}_i) = 0$. The radical is an ideal and if $\overline{\mathcal{A}} = \mathcal{A}/\operatorname{Rad}(\mathcal{A})$ then $\operatorname{Rad}(\overline{\mathcal{A}}) = 0$. Also $\overline{\mathcal{A}} = \prod_{i=1}^t \overline{\mathcal{A}}_i$ with $\overline{\mathcal{A}}_i = \mathcal{A}_i/\operatorname{Rad}(\mathcal{A}_i)$. So each $\overline{\mathcal{A}}_i$ is a field. The maximal ideals in $\overline{\mathcal{A}}_i$ are

$$\overline{J}_i = \prod_{j=1, j\neq i}^{t} \overline{\mathcal{A}}_j.$$

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

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

From the map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{A}$ the inverse images of the J_i's are all the maximal ideals $\mathcal{P}_i$ that contain $\mathfrak{p}\mathcal{O}_L$. This proves there are only finitely many maximal ideals containing $\mathfrak{p}\mathcal{O}_L$.

If $\mathcal{P}$ is a prime ideal in $\mathcal{O}_L$ that contains $\mathfrak{p}\mathcal{O}_L$, then $\mathcal{O}_L/\mathcal{P}$ is a finite dimensional commutative k-algebra ($k = \mathfrak{o}/\mathfrak{p}$) and $\mathcal{O}_L/\mathcal{P}$ is an integral domain. That means that $\mathcal{O}_L/\mathcal{P}$ 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 $\operatorname{Rad}(\mathcal{O}_L/\mathcal{P}) = \mathfrak{o}$. Then $\mathcal{O}_L/\mathcal{P}$ 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 $L/\mathbb{Q}$, $\mathcal{O}_L$ is a Dedekind domain. Because $\mathbb{Z}$ is a PID, $\mathcal{O}_L$ is a free $\mathbb{Z}$-module. Since $\mathcal{O}_L$ spans L over $\mathbb{Q}$, $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of rank n, and has an integral basis

$$\{w_1, \cdots, w_n\}.$$

The discriminant is

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

where $\sigma_1, \cdots, \sigma_n$ are the distinct embeddings $L \hookrightarrow \overline{\mathbb{Q}}$. Suppose $\{u_1, \cdots, u_n\}$ is another basis of $\mathcal{O}_L$. Then there exists integers $a_{ij}, b_{ij} \in \mathbb{Z}$ such that

$$w_i = \sum_{j=1}^{n} a_{ij} u_i, \ u_i = \sum_{j=1}^{n} b_{ij} w_i.$$

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, $\det([w_i^{\sigma_j}]) = \pm \det([u_i^{\sigma_j}])$. 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:

$$\begin{aligned} \det(w_i^{\sigma_j}) &= \sum_{\pi \in S_n} \operatorname{sign}(\pi) w_1^{\sigma_{\pi(1)}} \cdots w_n^{\sigma_{\pi(n)}} \\ &= \sum_{\pi \text{ even}} w_1^{\sigma_{\pi(1)}} \cdots w_n^{\sigma_{\pi(n)}} - \sum_{\pi \text{ odd}} w_1^{\sigma_{\pi(1)}} \cdots w_n^{\sigma_{\pi(n)}} \\ &= E - O. \end{aligned}$$

If we apply any embedding σ to these terms,

$$(w_j^{\sigma_{\pi(j)}})^\sigma = w_j^{\sigma_{\lambda\pi(j)}}$$

for some permutation $\lambda \in S_n$ determined by σ. So either

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

or

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

Then $(E+O)^\sigma = E+O$ for all σ. 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

$$d_L = (E+O)^2 - 4EO \equiv 0, 1 \pmod 4.$$

□

20 Extensions of Dedekind Domain III (10/03)

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

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] \text{ if } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \text{ if } m \equiv 1 \pmod 4. \end{cases}$$

Also, the fundamental discriminant is

$$d_K = \begin{cases} 4m \text{ if } m \equiv 2,3 \pmod 4, \\ m \text{ if } m \equiv 1 \pmod 4. \end{cases}$$

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

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

$$\alpha \in \mathcal{O}_K \Leftrightarrow t_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \text{ and } N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}.$$

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

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

$$\det([u_i^{\sigma_j}])^2 = \det([a_{ij}])^2 \cdot \det([w_i^{\sigma_j}])^2,$$

so

$$d(u_1, \cdots, u_n) = [\mathcal{O}_K : \wedge] \cdot d_K.$$

In our quadratic case, $u_1 = 1, u_2 = \sqrt{m}$, because $\mathbb{Z}[\sqrt{m}] \subset \mathcal{O}_K$.

$$d(\sqrt{m}) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m$$

and $d(\mathcal{O}_K) \cdot l^2 = d(\sqrt{m})$, we have $l^2 | 4m$. 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 $m \equiv 1 \pmod 4$. □

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 $[\mathfrak{o} : \mathfrak{a}] = \prod_{j=1}^r [\mathfrak{o} : \mathfrak{p}_\mathrm{j}]^{m_j}$. □

Definition 20.3. 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 $N : I_{\mathfrak{o}} \to \mathbb{Q}^*$:

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

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 $\mathfrak{p}$ in $\mathfrak{o}$, 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 $xx^{-1} = 1$, $v(x)+v(-x) = v(1) = 0$. Since if $x \in \mathfrak{o}_v^*$, 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 $\mathfrak{a} = \mathcal{P}_v^m = (\pi^m)$. 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 $\mathfrak{a} \subset (\pi^m)$. By similar reasoning, $v(a\pi^{-m}) = 0$, and so $a\pi^{-m} \in \mathfrak{o}_v^*$. So $\pi^{-m} \in \mathfrak{a}$. $\square$

For a general Dedekind domain, we had an exact sequence

$$1 \to \mathfrak{o}^* \to K^* \to I_{\mathfrak{o}} \to \mathrm{Cl}(\mathfrak{o}) \to 1.$$

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

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

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

$$\mathfrak{o}_v^* \supseteq U_K^{(1)} \supseteq U_K^{(2)} \supseteq U_K^{(3)} \cdots$$

and

$$\mathfrak{o}_v^*/U_K^{(1)} \cong (\mathfrak{o}_v/\mathcal{P}_v)^*,$$

$$U_K^{(n)}/U_K^{(n+1)} \cong \mathcal{P}_v^n/\mathcal{P}_v^{n+1} \cong \mathfrak{o}_v/\mathcal{P}_v = k_v.$$

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 $1 + \mathcal{P}_v = U_K^{(1)}$, so $\mathfrak{o}_v^*/U_K^{(1)} \cong (\mathfrak{o}_v/\mathcal{P}_v)^*$. $U_K^{(n)} = 1 + \mathcal{P}_v^n = 1 + \pi^n \mathfrak{o}_v = 1 + \pi^n(a + \pi\mathfrak{o}_v)$ for some $a \in \mathfrak{o}_v$. Consider the map $U_K^{(n)} \to \mathfrak{o}_v/\mathcal{P}_v : 1 + \pi^n a + \pi^{n+1} b \mapsto a + \mathcal{P}_v$. 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 $(1 + \mathcal{P}_v^n)/(1 + \mathcal{P}_v^{n+1}) \cong \mathfrak{o}_v/\mathcal{P}_v$.

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 $n \in \mathbb{N}$,

$$v(n) = v(1 + 1 + \cdots + 1) \geq \min(v(1), v(1), \cdots, v(1)) = 0.$$

For negative $n \in \mathbb{N}$,

$$v(n) = v(-1 - 1 - \cdots - 1) \geq \min(v(-1), v(-1), \cdots, v(-1)) = 0.$$

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

$$\begin{aligned} v(x^n) = nv(x) &\geq \min_{1 \leq j \leq n} (v(a_j) + (n-j)v(x)) \\ &\geq \min_{1 \leq j \leq n} ((n-j)v(x)). \end{aligned}$$

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, $\mathfrak{o} \subset \mathfrak{o}_v$. □

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) $\mathfrak{p}_v = \mathcal{P}_v \cap \mathfrak{o}$ is a prime ideal in $\mathfrak{o}$,
(ii) $\mathfrak{p}_v \mathfrak{o}_v = \mathcal{P}_v$,
(iii) $\mathfrak{o}/\mathfrak{p}_v \cong \mathfrak{o}_v/\mathcal{P}_v$.

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

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

$$\mathcal{P}_v = \{\text{all fractions } \frac{r}{s} \text{ where } p \nmid s, p|r\},$$

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

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

$$\begin{aligned} v_\infty : & K^* \to \mathbb{Z} \\ & \frac{f(x)}{g(x)} \mapsto -\deg(f) + \deg(g) \end{aligned}$$

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

$$\begin{aligned} v_\infty\left(\frac{f(x)}{g(x)} \cdot \frac{r(x)}{s(x)}\right) &= -\deg(f(x)) - \deg(r(x)) + \deg(g(x)) + \deg(s(x)) \\ &= v_\infty\left(\frac{f(x)}{g(x)}\right) + v_\infty\left(\frac{r(x)}{s(x)}\right), \end{aligned}$$

$$\begin{aligned} v_\infty\left(\frac{f(x)}{g(x)} + \frac{r(x)}{s(x)}\right) &= v_\infty\left(\frac{f(x)s(x) + r(x)g(x)}{g(x)s(x)}\right) \\ &= -\deg\left(f(x)s(x) + r(x)g(x)\right) + \deg(g(x)) + \deg(s(x)) \\ &\geq -\max\left\{\deg(f(x)s(x)), \deg(r(x)g(x))\right\} \\ &= \min\left\{-\deg(f(x)) + \deg(g(x)), -\deg(r(x)) + \deg(s(x))\right\} \\ &= \min\left\{v_\infty\left(\frac{f(x)}{g(x)}\right), v_\infty\left(\frac{r(x)}{s(x)}\right)\right\}. \end{aligned}$$

Note that $\deg(x) = -1, \deg(\frac{1}{x}) = 1$, and $\frac{1}{x} \notin \mathfrak{o}$. Moreover, we have the following sum formula

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

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 $\mathfrak{o}_v$ is 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 $v_{\mathfrak{p}_v} : K^* \to \mathbb{Z}$ by $v_{\mathfrak{p}_v}(x) = n$ where $x\mathfrak{o}$ is a product of $\mathfrak{p}_v^n$ and other prime ideal powers. $v_{\mathfrak{p}_v}$ is surjective on $\mathbb{Z}$ because $\mathfrak{p}_v^n \neq \mathfrak{p}_v^{n+1}$.

We claim that for $z \in K^*$, if $v_{\mathfrak{p}_v}(z) = 0$, then $v(z) = 0$. Here is the proof. Write $z = \frac{a}{b}$ for some $a, b \in \mathfrak{o}$. Then $a\mathfrak{o} = \mathfrak{p}_v^l\mathfrak{a}$ and $b\mathfrak{o} = \mathfrak{p}_v^l\mathfrak{b}$ for some ideal $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{p}_v \nmid \mathfrak{a}$, $\mathfrak{p}_v \nmid \mathfrak{b}$. The same power occurs because $v_{\mathfrak{p}_v}(z) = 0 = v_{\mathfrak{p}_v}(a) - v_{\mathfrak{p}_v}(b)$. Pick $c \in \mathfrak{p}_v^{-l}\backslash\mathfrak{p}_v^{-l+1}$. Then $ca \in (\mathfrak{p}_v^{-l}\mathfrak{p}_v^l\mathfrak{a})\backslash(\mathfrak{p}_v^{1-l}\mathfrak{p}_v^l\mathfrak{a}) = \mathfrak{a}\backslash(\mathfrak{p}_v\mathfrak{a})$. That proves $v_{\mathfrak{p}_v}(ca) = 0$. Similarly, $v_{\mathfrak{p}_v}(cb) = 0$. Since $z = \frac{a}{b} = \frac{ca}{cb}$, so we proved that we can assume $z = \frac{a}{b}$ with $v_{\mathfrak{p}_v}(a) = v_{\mathfrak{p}_v}(b) = 0$. So $a, b \in \mathfrak{o}\backslash\mathfrak{p}_v$. Then $a, b \in \mathfrak{o}_v\backslash\mathcal{P}_v$ (if not, $a \in \mathcal{P}_v$ implies $a \in \mathfrak{o} \cap \mathcal{P}_v = \mathfrak{p}_v$). Then $v(a) = v(b) = 0$ and so $v(z) = 0$.

Now pick $x \in \mathfrak{o}, x \neq 0$. Then $v_{\mathfrak{p}_v}(x) = l \geq 0$. Then $x\mathfrak{o} = \mathfrak{p}_v^l\mathfrak{a}$ for some ideal $\mathfrak{a}$ with $\mathfrak{p}_v \nmid \mathfrak{a}$. So there exists $\alpha \in \mathfrak{a}$, $\alpha \notin \mathfrak{p}_v, \alpha \in \mathfrak{o}$. By the previous claim, $v(\alpha) = 0$. Then $\alpha\mathfrak{o}_v = \mathfrak{o}_v$, then $\mathfrak{a}\mathfrak{o}_v = \mathfrak{o}_v$. So $x\mathfrak{o}_v = \mathfrak{p}_v^l\mathfrak{a}\mathfrak{o}_v = \mathfrak{p}_v^l\mathfrak{o}_v = (\mathfrak{p}_v\mathfrak{o}_v)^l = (\mathcal{P}_v^e)^l = \mathcal{P}_v^{ef}$. That proves $v(x) = el = ev_{\mathfrak{p}_v}(x)$. 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 $bc = 1 \pmod{\mathfrak{p}_v}$. 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_∞ 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 $1 + \frac{b}{a} \in 1 + \mathcal{P}_v \subset \mathfrak{o}_v \backslash \mathcal{P}_v = \mathfrak{o}_v^*$. 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

$$v\left(\frac{f(x)}{g(x)}\right) = (-\deg(f) + \deg(g))\,\alpha \in \alpha\mathbb{Z}.$$

Since v maps K^* onto $\mathbb{Z}$, we have $\alpha = -1$. Thus $v(\frac{f(x)}{g(x)}) = -\deg(f) + \deg(g)$. □

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 λ 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*

$$\{x \in K : |x| > 1\} \subset \{x \in K : |x|' > 1\}.$$

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

$$\left|x^n x_0^{-m}\right|' < 1.$$

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

$$\left|x^n x_0^{-m}\right| > 1.$$

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 $x \in K^*$. □

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

$$1 = |mp^a + nq^b| \leq |m||p|^a + |n||p|^b < 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1.$$

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 $x \in \mathbb{Q}^*$. Since $|p| < 1$, $|p| = p^{-a}$ for some $a > 0$. Then $|x| = |x|_p^a$.

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

$$\begin{aligned}
|m| &\leq \sum_{j=0}^{k} |c_j||n^j| \leq \sum_{j=0}^{k} c_j n^{j\alpha} \\
&\leq (n-1) \sum_{j=0}^{k} n^{j\alpha} = (n-1) \cdot \frac{n^{(k+1)\alpha} - 1}{n^\alpha - 1}.
\end{aligned}$$

Only k depends on m. That proves

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

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 $|m| \leq c^{\frac{1}{r}} \cdot m^{\alpha}$. Then $\lim_{r\to\infty} c^{\frac{1}{r}} = 1$. 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 $0 \leq c_j < n$, $0 \leq j < k$, 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

$$\begin{aligned} |m| &\leq |n^{k+1}| - |b| \leq n^{(k+1)\alpha} - (n^{k+1} - n^k)^{\alpha} \\ &= n^{(k+1)\alpha}\left(1 - (1 - \frac{1}{n})^{\alpha}\right) \\ &\geq c' \cdot n^{(k+1)\alpha} \\ &\geq c' \cdot m^{\alpha} \end{aligned}$$

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 $\mathfrak{p}$-adic absolute value for a unique prime ideal $\mathfrak{p}$ 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 topoloty 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 an $\in \overline{\mathbb{Z}}$, where $\overline{\mathbb{Z}}$ 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,

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

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,

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

□

27 Weak Approximation Theorem (10/20)

Theorem 27.1 (Weak Approximation Theorem). *Let $|\cdot|_1, \cdots, |\cdot|_n$ 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 $\mathfrak{p}_i$ 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 $x \equiv y_j \pmod{\mathfrak{p}_j^M}$, that's equivalent saying $|x - y_j|_j \leq (N_{\mathfrak{p}_j})^{-M}$. So if we choose M large enough so that $(N_{\mathfrak{p}_j})^{-M} < \varepsilon$, 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 $2 \leq i \leq n$.*

Proof. We prove by induction on n.

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

$$\{|x|_1 < 1\} \not\subset \{|x|_2 < 1\}$$

and

$$\{|x|_2 < 1\} \not\subset \{|x|_1 < 1\}.$$

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 $|b|_1 > 1, |b|_i < 1$ for $i = 2, \cdots, n$. 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 $2 \leq i \leq n$,

$$|cb^r|_i = |c|_i |b|_i^r < 1$$

which we can do because $|b|_i < 1$. Also

$$|cb^r|_1 = |c|_1 \cdot |b|_1^r > 1,$$

$$|cb^r|_{n+1} = |c|_{n+1} \cdot |b|_{n+1}^r = |c|_{n+1} < 1.$$

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

$$|a|_1 = \frac{|c|_1 |b|_1^r}{|1 + b|_1^r} \geq \frac{|c|_1 |b|_1^r}{1 + |b|_1^r}.$$

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

$$|a|_i \leq \frac{|c|_i |b|_i^r}{1 - |b|_i^r}$$

because $|b|_i < 1$, and

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

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

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

and

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

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

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

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

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

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

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

Corollary 27.5. *Suppose $K/\mathbb{Q}$ is a finite extension. Suppose $|\cdot|_1, \cdots, |\cdot|_m$ 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 ± 1. Then there exists $x \in K$ such that 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 $|\cdot|$. 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 $n > m \geq N$.

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 sequence forms a commutative ring R with a $1 = \{1\}$ with operations:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\},$$
$$\{a_n\}\{b_n\} = \{a_n b_n\}.$$

The set $\mathfrak{N}$ of null sequences forms an ideal in R. If $\{a_n\} \in R\backslash\mathfrak{N}$, 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

$$\begin{aligned} |a_n| &= |a_n - a_N + a_N| \\ &\geq |a_N| - |a_n - a_N| \\ &\geq \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2} \end{aligned}$$

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 $\{a_n\} \in R\backslash\mathfrak{N}$ to $\mathfrak{N}$, then $1 = \{1\} \in \mathfrak{N}$.) Then $\overline{K} = R\backslash\mathfrak{N}$ 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

$$\begin{aligned} &K \hookrightarrow \overline{K} \\ &\alpha \mapsto \{\alpha\} + \mathfrak{N} \end{aligned}$$

satisfying $\|\{\alpha\}\| = |\alpha|$.
(iv) The image of K is dense in $\overline{K}$.
(v) If $\overline{\overline{K}}$ is a complete field containing K as a dense subset, then $\overline{\overline{K}}$ is isomorphic to $\overline{K}$, with K mapping to 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 $|x^\sigma|_{\mathbb{R}}$ is isomorphic to $\mathbb{R}$. For $\sigma : K \hookrightarrow \mathbb{C}$ which are nonreal, the completion of K relative to $|x^\sigma|_{\mathbb{C}}$ is always isomorphic to $\mathbb{C}$.

Suppose $\mathfrak{o}$ is a Dedekind domain and not a field, K is its field of fractions, $\mathfrak{p}$ is a nonzero prime ideal of $\mathfrak{o}$. Define $|x|_{\mathfrak{p}} = \lambda^{v_{\mathfrak{p}}}$ with some $0 < \lambda < 1$. $|\cdot|_{\mathfrak{p}}$ is an absolute value on K. Then $K_{\mathfrak{p}}$ is the completion of K relative to $|\cdot|_{\mathfrak{p}}$ ($\mathfrak{p}$-adic field). The valuation $v_{\mathfrak{p}}$ extends to

$K_\mathfrak{p}$ so that $|x|_\mathfrak{p} = \lambda^{v_\mathfrak{p}(x)}$. Then for any Cauchy sequence $\{a_n\}$ in K, $\lim_{n\to\infty} |a_n|_\mathfrak{p}$ exists. $\{|x|_\mathfrak{p}$ for $x \in K\} \subset \{\lambda^n | n \in \mathbb{Z}\} \cup \{0\}$ and since this is a discrete subset of $(0, \infty)$, the only possible limits of sequence of these are $\{\lambda^n | n \in \mathbb{Z}\} \cup \{0\}$. Then $\lim_{n\to\infty} |a_n| = 0$ or λ^m for some integer $m \in \mathbb{Z}$. Then if $x \neq 0$, define $v_\mathfrak{p}(x) = m$. Then $v_\mathfrak{p}$ is a valuation on $\overline{K}$. Then denote $K_\mathfrak{p}$ as K_v, and $\mathfrak{o}_v = \{x \in K_v : |x|_v \leq 1\}$ 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 $\mathfrak{o}$, 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

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

Then $L_1 - L_0 < \varepsilon$ 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 $|x|_v = \lambda^{v(x)}$ for some $0 < \lambda < 1$. Since $\{\lambda^n | n \in \mathbb{Z}\}$, then $\lim_{n\to\infty} |a_n|_v = 0$ or λ^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 $\{\lambda^n | n \in \mathbb{Z}\}$. The only limit point of that set not in the set is 0. Then $\lim_{n\to\infty} |a_n|_v = \lambda^m$ 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

$$\begin{aligned} \mathfrak{o}_v &= \text{valuation ring of } v \text{ in } K_v \\ &= \{x \in K_v : |x|_v \leq 1\} \\ &= \text{closure of } \mathfrak{o} \text{ in } K_v \end{aligned}$$

and

$$\begin{aligned} \mathcal{P}_v &= \text{unique prime ideal in } \mathfrak{o}_v \\ &= \{x \in K_v : |x|_v < 1\} \\ &= \{x \in K_v : |x|_v \leq \lambda\} \\ &= \text{closure of } \mathfrak{p} \text{ in } K_v. \end{aligned}$$

Theorem 29.1.

$$\mathfrak{o}_v / {\mathcal{P}_v}^r \cong \mathfrak{o}/\mathfrak{p}^r$$

for $r \geq 1$.

Proof. Consider the map

$$\mathfrak{o}/\mathfrak{p}^r \to \mathfrak{o}_v/{\mathcal{P}_v}^r$$
$$x + \mathfrak{p}^r \mapsto x + {\mathcal{P}_v}^r.$$

Since $|\cdot|_v$ is discrete in K_v,

$${\mathcal{P}_v}^r = \{x \in K_v : |x|_v \leq \lambda^r\}.$$

Since v is an extension of the valuation on K, $\mathfrak{p}^r \subset {\mathcal{P}_v}^r$. So the map is well-defined. Suppose $x \in \mathfrak{o} \cap {\mathcal{P}_v}^r$, then $x \in \mathfrak{p}^r$. 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 $n >> 0$. Choose $0 < \varepsilon < \lambda^r$. Then there exists $N > 0$ such that for $n \geq N$

$$|a_n - x|_v < \varepsilon < \lambda^r.$$

Then $a_N - x \in {\mathcal{P}_v}^r$. So $a_N + \mathfrak{p}^r$ maps to $x + {\mathcal{P}_v}^r$. That proves the map is surjective. $\square$

Example 29.2. $\mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}_p/p^r\mathbb{Z}_p$.

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

Proof. Since $\mathfrak{q} \subset \mathfrak{o}$, $\mathfrak{q}\mathfrak{o}_v \subset \mathfrak{o}_v$. Then $\mathfrak{q}\mathfrak{o}_v = {\mathcal{P}_v}^r$ for some $r \geq 0$. Since $\mathfrak{q} \neq \mathfrak{p}$, there exists $\alpha \in \mathfrak{q}\backslash\mathfrak{p}$. Then $|\alpha|_v = 1$ and hence $r = 0$. $\square$

Now we come to the Inverse Limits.

Suppose we have a sequence of commutative groups: for $n \geq 1$

$$A_n = \mathfrak{o}/\mathfrak{p}^n$$

with homomorphisms

$$\alpha_m^n : A_n \to A_m$$

for all $n \geq m \geq 1$, satisfying for $n \geq m \geq r \geq 1$

$$\alpha_r^n = \alpha_r^m \circ \alpha_m^n$$

where

$$\alpha_m^n\,(x + \mathfrak{p}^n) = x + \mathfrak{p}^m$$

which is well-defined because since $n \geq m, \mathfrak{p}^n \subset \mathfrak{p}^m$. To any such inverse system $\{A_n\}$, there is associated an *inverse limit*

$$\overline{A} = \varprojlim_n A_n = \left\{ (x_n) \in \prod_{n=1}^{\infty} A_n : \alpha_m^n(x_n) = x_m \text{ for } n \geq m \geq 1 \right\}$$

with natural surjective homomorphisms

$$\beta_n : \overline{A} \to A_n$$

such that for $n \geq m \geq 1$, $\beta_m = \alpha_m^n \circ \beta_n$.

Theorem 29.4.
$$\varprojlim_n \mathfrak{o}/\mathfrak{p}^n \cong \mathfrak{o}_v.$$

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

Choose $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$. So $|\pi|_v = \lambda$. Let R be any set of representatives in $\mathfrak{o}$ for the residue field $k = \mathfrak{o}/\mathfrak{p}$. Let $x \in K_v, x \neq 0$. Then $|x|_v = \lambda^{n_1} = |\pi|_v{}^{n_1}$ for some $n_1 \in \mathbb{Z}$. Then $|x\pi^{-n_1}|_v = 1$. Then $x\pi^{-n_1} \in \mathfrak{o}_v$. Choose $a_1 \in R$ with $x\pi^{-n_1} = a_1 \pmod{\mathfrak{p}}$. Either $|x^{-n_1} - a_1|_v = 0$ or $|x^{-n_1} - a_1|_v = \lambda^{n_2} = |\pi|_v{}^{n_2}$ for some $n_2 \geq 1$. Then $|(x\pi^{-n_1} - a_1)\pi^{-n_2}|_v = 1$. Choose $a_2 \in R$ with $(x\pi^{-n_1} - a_1)\pi^{-n_2} = a_2 \pmod{\mathfrak{p}}$. 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 $\left((1+x)^{\frac{1}{2}}\right)^2 = 1+x$. Note

$$\begin{aligned}
\binom{\frac{1}{2}}{n} &= \frac{\frac{1}{2}\cdot(\frac{1}{2}-1)\cdots(\frac{1}{2}-(n-1))}{n!} \\
&= \frac{1}{2^n}\cdot\frac{(-1)^{n-1}(2n-3)(2n-1)\cdots 3\cdot 1}{n!} \\
&= \frac{(-1)^{n-1}}{2^n}\cdot\frac{(2n-2)(2n-3)(2n-1)(2n)\cdots 3\cdot 2\cdot 1}{n!(2n-2)(2n-4)\cdots 2} \\
&= \frac{(-1)^{n-1}}{2^{2n-2}}\cdot\frac{(2n-2)!}{n!\cdot(n-1)!} \\
&= \frac{(-1)^{n-1}}{2^{2n-2}}\cdot\binom{2n-2}{n-1}\cdot\frac{1}{n} \\
&\in \frac{\mathbb{Z}}{2^{2n-1}n}.
\end{aligned}$$

So

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

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

$$v_p\left(\binom{\frac{1}{2}}{n}x^n\right) \geq n - c\log(n) \to \infty \text{ as } n\to\infty.$$

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

Let K be a complete field with a nonarchimedean absolute value $|\cdot|$. 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 $v = v_{\mathfrak{p}}$ 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 $\varprojlim_n A_n = \overline{A}$ is compact with respect to the projective topology.*

A basis of neighborhoods of 0 in $\overline{A}$ 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 $a \in \overline{A}$ is $\{a + U_N\}$.

Proof of Theorem 30.4. We will prove sequential compactness. Let $\{x_n\}$ be a sequence in $\overline{A}$. We have to show there is a convergent subsequence. There are only finitely many $a_1 \in A_1$, and $\overline{A} = \bigcup_{a_1 \in A_1} a_1 + U_1$. 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 $a = (a_n) \in \overline{A}$ 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 $\lim_{j \to \infty} x_{n_j} = a$. $\square$

Since $\mathfrak{o} \cong \varprojlim_n \mathfrak{o}/\mathfrak{p}^n$, 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*

$$K^{sep} = \bigcup_{L/K \text{ finite separable}} L = \varinjlim_{L/K \text{ finite separable}} L \quad \textit{(direct limit).}$$

Then

$$\mathrm{Gal}(K^{sep}/K) = \varprojlim_{L/K \text{ finite separable}} \mathrm{Gal}(L/K)$$

since for $K \subset L_1 \subset L_2$ we have

$$\mathrm{Gal}(L_2/K) \twoheadrightarrow \mathrm{Gal}(L_1/K)$$

forms a projective system of groups. With the projective topology, $\mathrm{Gal}(K^{sep}/K)$ *is a compact group. This suggests a relationship between* $\mathrm{Gal}(K^{sep}/K)$ *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 $\alpha_0 \in \mathfrak{o}$ with*

$$\left| \frac{f(\alpha_0)}{f'(\alpha_0)^2} \right| < 1,$$

then there is a root $\alpha \in \mathfrak{o}$ with $f(\alpha) = 0$ and $|\alpha - \alpha_0| < 1$.

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

$$\begin{aligned} f(x + \pi^l y) &= \sum_{m=0}^{N} c_m (x + \pi^l m)^m \\ &= \sum_{m=0}^{N} c_m \sum_{k=0}^{m} \binom{m}{k} x^{m-k} (\pi^l y)^k \\ &= \sum_{k=0}^{N} (\pi^l y)^k \sum_{m=k}^{N} c_m \binom{m}{k} x^{m-k}. \end{aligned}$$

Note that

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

So

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

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

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

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,

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

That proves

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

Since $n > c$,

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

Repeat the process from α_1 to get α_2, then α_3 and so on, and we get

$$v(f(\alpha_0)) < v(f(\alpha_1)) < v(f(\alpha_2)) \cdots$$

and

$$v(f'(\alpha_n)) = v(f'(\alpha_1)),\ \forall n.$$

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 31.2. 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 $x_o \equiv a \pmod{\mathfrak{p}}$. 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 $x_0^{q-1} \equiv 1 \pmod{\mathfrak{p}}$, $|x| = 1$. 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 $f(\hat{a}) = (\hat{a})^{q-1} - 1 = 0$ 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 $|f(1)|_2 = |1^2 - x_0|_2 \leq |8|_2$ 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 $a^2 = (1+2b)^2 = 1 + 4b(b+1) \equiv 1 \pmod 8$. $\square$

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 $\mathfrak{M} = \mathfrak{M}_K$ be the set of inequivalent absolute values on K (places of K), $\mathfrak{M}_\infty$ be the set of archimedean places (infinite places), $\mathfrak{M}_\mathbb{R}$ be the set real places, $\mathfrak{M}_\mathbb{C}$ 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 $\mathfrak{M}_0$ be the set of nonarchimedean places of K. For each $v \in \mathfrak{M}$, let K_v be the completion of K with respect to v. For $v \in \mathfrak{M}_0$, let

$$\begin{aligned}
&\mathfrak{o}_v = \{x \in K_v : |x|_v \le 1\}, \\
&\mathfrak{p}_v = \{x \in K_v : |x|_v < 1\}, \\
&\pi_v \in \mathfrak{p}_v \backslash \mathfrak{p}_v^2, \\
&U_v = \mathfrak{o}_v^* = \{x \in K_v : |x|_v = 1\} = \text{ units of } \mathfrak{o}_v.
\end{aligned}$$

The ring of *adeles* of K is

$$K_\mathbb{A} = \mathbb{A}_K = \prod_{v \in \mathfrak{M}}{}' K_v$$

where the direct product is restricted to $(x_v)_{v \in \mathfrak{M}}$ where for all but finitely many $v \in \mathfrak{M}_0$ we have $|x_v|_v \le 1$ (or $x_v \in \mathfrak{o}_v$).

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

$$U \times \prod_{v \notin S} \mathfrak{o}_v$$

where S is a finite set $S \subset \mathfrak{M}$, $S \supset \mathfrak{M}_\infty$, 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 $\prod_{v \in \mathfrak{M}_0} \mathfrak{o}_v$ 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 μ on open subsets of G, satisfying*
(i) $\mu(U) \ge 0$ for all open subsets U,
(ii) $\mu(U) < \infty$ if $\overline{U}$ is compact,
(iii) $\mu\left(\coprod_{n=1}^\infty U_n\right) = \sum_{n=1}^\infty \mu(U_n)$ for disjoint union $\coprod_{n=1}^\infty U_n$,
(iv) $\mu(aU) = a\mu(U)$ for all $a \in G$.

The Haar measure μ 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 $\mu(\{|z| \le r\}) = \pi r^2$ up to a constant multiplier. If v is nonarchimedean, it is normal to normalize μ by $\mu(\mathfrak{o}_v) = 1$.

If μ 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 $\mu_a(U) = \mathrm{mod}_{K_v}(a) \cdot \mu(U)$. $\mathrm{mod}_{K_v}(a)$ is called the *modulus* of a in K_v. $\mathrm{mod}_{K_v}(a) = |a|_{\mathbb{R}}$ if $K_v \cong \mathbb{R}$, $\mathrm{mod}_{K_v}(a) = |a|^2$ if $K_v \cong \mathbb{C}$.

In general, there is a constant A such that

$$\mathrm{mod}_{K_v}(x+y) \le A\left(\mathrm{mod}_{K_v}(x) + \mathrm{mod}_{K_v}(y)\right)$$

for any $x, y \in K_v$. For example, for $K_v = \mathbb{C}$, $\mathrm{mod}_{\mathbb{C}}(z) = |z|^2$ where $|\cdot|$ is the ordinary absolute value, we have $\mathrm{mod}_{\mathbb{C}}(z+w) \le 2(\mathrm{mod}_{\mathbb{C}}(z) + \mathrm{mod}_{\mathbb{C}}(w))$.

If v is nonarchimedean with $\mathfrak{o}_v/\mathfrak{p}_v$ finite,

$$\mathfrak{o}_v = \coprod_{a \in \mathfrak{o}_v/\mathfrak{p}_v} (a + \pi\mathfrak{o}_v)$$

for any $\pi \in \mathfrak{p}_v \backslash \mathfrak{p}_v^2$. So

$$\begin{aligned}
\mu(\mathfrak{o}_v) &= \sum_{a \in \mathfrak{o}_v/\mathfrak{p}_v} \mu(a + \pi\mathfrak{o}_v) \\
&= \sum_{a \in \mathfrak{o}_v/\mathfrak{p}_v} \mu(\pi\mathfrak{o}_v) \\
&= \mathrm{mod}_{K_v}(\pi) \sum_{a \in \mathfrak{o}_v/\mathfrak{p}_v} 1 \\
&= \frac{1}{|\mathfrak{o}_v/\mathfrak{p}_v|} \cdot \sum_{a \in \mathfrak{o}_v/\mathfrak{p}_v} 1.
\end{aligned}$$

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

$$\begin{aligned}
\mu\left(\prod_{v \in \mathfrak{M}} \{x_v : |x_v|_v \le 1\}\right) &= \prod_{v \in \mathfrak{M}_{\mathbb{R}}} \int_{-1}^{1} dx \cdot \int_{v \in \mathfrak{M}_{\mathbb{C}}} \int_{|x| \le 1} |dx \wedge d\overline{x}| \cdot \prod_{v \in \mathfrak{M}_0} \mu(\mathfrak{o}_v) \\
&= 2^{r_1}(2\pi)^{r_2}.
\end{aligned}$$

The group of *ideles* of K is the restricted direct product

$$K_{\mathbb{A}}^* = \prod_{v\in\mathfrak{M}}' K_v^*$$

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

The normalize Haar measure on $K_{\mathbb{A}}^*$ is

$$\begin{aligned}\mu\left(\prod_{v\in\mathfrak{M}_\infty}\{1 \le |x|_v \le N\} \times \prod_{v\in\mathfrak{M}_0}\mathfrak{o}_v^*\right) &= \left(2\int_1^N \frac{dt}{t}\right)_1^r \cdot \left(\int_{1\le|x|_v\le N}\frac{|dx\wedge d\overline{x}|}{|x|_v}\right)^{r_2} \cdot 1 \\ &= 2^{r_1}\cdot(\log N)^{r_1}(2\pi\cdot 2\log(\sqrt{N}))^{r_2} \\ &= 2^{r_1}\cdot(2\pi)^{r_2}\cdot(\log N)^{r_1+r_2}.\end{aligned}$$

If μ is a Haar measure on $K_{\mathbb{A}}$ and $a \in K_{\mathbb{A}}^*$, then $\mu(aU)$ for any open $U \subset K_{\mathbb{A}}$ defines another Haar measure on $K_{\mathbb{A}}$. So $\mu(aU) = \mathrm{mod}_{\mathbb{A}}(a)\mu(U)$. Another common notation is $|a|_{\mathbb{A}} = \mathrm{mod}_{\mathbb{A}}(a)$. From the product structure of $K_{\mathbb{A}}$ and $K_{\mathbb{A}}^*$, we can prove $|a|_{\mathbb{A}} = \prod_{v\in\mathfrak{M}}|a_v|_v$. (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.

$\dim_K(M \otimes_{\mathfrak{o}} K) = \mathrm{rk}_{\mathfrak{o}}(M)$ 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*

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

for uniquely determined $n_1 \le n_2 \le \cdots \le n_t$.

Theorem 35.4. *Let $\mathfrak{o}$ be an Dedekind domain.*
(i) Every fractional $\mathfrak{o}$-ideal is a projective $\mathfrak{o}$-module.
(ii) Every torsion-free finitely generated $\mathfrak{o}$-module M is isomorphic as a $\mathfrak{o}$-module to $F \oplus \mathfrak{a}$ for some free $\mathfrak{o}$-module F and a fractional $\mathfrak{o}$-ideal $\mathfrak{a}$.

Remark 35.5. *The $\mathfrak{o}$-rank of F and the ideal class of $\mathfrak{a}$ are uniquely determined. The ideal class of $\mathfrak{a}$ is dependent 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 $cl(K) = cl(\mathfrak{o})$.*

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

Theorem 35.6 (Kable-Wright, 2006)**.** *As L/K ranges over all extensions of degree 2 (or 3) by size of discriminant of $L/\mathbb{Q}$, then the Steinitz class of $\mathfrak{o}_L$ as an $\mathfrak{o}_K$-module is equidistributed over all the ideal classes in $cl(\mathfrak{o}_K)$.*

Remark 35.7. *Bhargava and his coauthors laid out distribution of discriminants of degree 4 and 5 relative extensions. One should be able to use this to do this theorem for degree 4 and 5.*

36 Extensions I (11/12)

Let (K, v) be a complete valued field. Let E/K be a finite separable extension.

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 $|a|_w^{(E:K)} = |N_{E/K}(a)|_v$.*

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 $\mathfrak{o}_K$, prime ideal $\mathfrak{p}_K$, then the integral closure $\mathfrak{o}_E$ of $\mathfrak{o}_K$ in E is a discrete valuation domain with unique prime ideal $\mathfrak{p}_E$ satisfying $\mathfrak{p}_E \cap \mathfrak{o}_K = \mathfrak{p}_K$. Let $\pi = \pi_K \in \mathfrak{p}_K \backslash \mathfrak{p}_K^2$ and $\pi_E \in \mathfrak{p}_E \backslash \mathfrak{p}_E^2$. Then $\pi \mathfrak{o}_E = \mathfrak{p}_E^e$ 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

$$|\pi|_w = |\pi_E^e|_w = (\lambda^{1/e})^e = \lambda = |\pi|_v.$$

(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

$$\{x \in E : |x|_w < 1\} \subset \{x \in E : |x|_{w'} < 1\}. \tag{36.1}$$

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. $\square$

Lemma 36.2. *For any sequence $\{x_n\} \subset E$, if we have*

$$\text{(36.2)} \qquad \textit{if } \lim_{n\to\infty} |x_n|_w = 0, \textit{ then } \lim_{n\to\infty} |x_n|_{w'} = 0,$$

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 $\lim_{n\to\infty} |y^n|_w = 0$ and $\lim_{n\to\infty} |y^n|_{w'} \geq 1$, a contradiction. □

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

$$\text{(37.1)} \qquad \lim_{m\to\infty} ||x_m|| = 0 \textit{ if and only if } \lim_{m\to\infty} |\lambda_{m_j}|_v = 0 \textit{ for all } 1 \leq j \leq n.$$

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*

$$\lim_{m\to\infty} ||x_m|| = 0 \textit{ if and only if } \lim_{m\to\infty} ||x_m||' = 0.$$

Proof of Lemma 37.1. ($\Longleftarrow$) 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, $\lim_{m\to\infty} ||x_m|| = 0$.

($\Longrightarrow$) 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

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

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 $\lambda \in U$,

$$\begin{aligned} ||\lambda(x + U)||_0 &= \inf_{z \in U} ||\lambda(x + z)|| \\ &= \inf_{z \in U} ||\lambda x + \lambda z|| \\ &= |\lambda|_v \cdot \inf_{z \in U} ||x + z|| \\ &= |\lambda|_v \cdot ||x + U||_0. \end{aligned}$$

(iii)

$$\begin{aligned} ||(x + U) + (y + U)||_0 &= \inf_{z \in U} ||x + y + z|| \\ &= \inf_{z, z' \in U} ||x + y + z + z'|| \\ &\leq \inf_{z, z' \in U} \big(||x + z|| + ||y + z'||\big) \text{ (by Triangle Inequality)} \\ &\leq \inf_{z \in U} ||x + z|| + \inf_{z' \in U} ||x + z'|| \\ &= ||x + U||_0 + ||y + U||_0. \end{aligned}$$

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

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

Repeat the whole argument with $U = \text{span}(z_i)$ for any $i \neq 1$, then we get

$$\lim_{m\to\infty} |\lambda_{m_j}|_v = 0, \quad \forall j \neq i, 1 \leq j \leq n+1.$$

Then we proved

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

□

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 $L \otimes_K K_v \cong \prod_{i=1}^t L_i$ 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 $\alpha \mapsto \alpha \otimes_K 1$ by the Weak Approximation Theorem.*

We will write

$$L \otimes_K K_v \cong \prod_{w|v} L_w$$

where $w|v$ 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* $e = e(w|v)$ 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

$$f = f(w|v) = (\mathfrak{o}_{L_w}/\mathcal{P}_w : \mathfrak{o}_{K_v}/\mathfrak{p}_v).$$

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

Proof. We sketch the idea of the proof. Choose $\pi_w \in \mathcal{P}_w \backslash \mathcal{P}_w^2$. 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. □

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 $\mathcal{O}_L$ lying over $\mathfrak{p}$. So $\mathcal{P} \cap \mathfrak{o}_K = \mathfrak{p}$. Let v be the valuation corresponding to $\mathfrak{p}$ on K, w the valuation of L corresponding to $\mathcal{P}$. In the Dedekind domain $\mathfrak{o}_L$,

$$\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_t^{e_t}$$

for distinct prime ideals $\mathcal{P}_j$ in $\mathcal{O}_L$. The $\mathcal{P}_j$ corresponds to all the inequivalent absolute values w extending v from K to L. Each $\mathcal{P}_j$ corresponds to some $w_j|v$ and $L_{\mathcal{P}_j} = L_{w_j}$, and $e_j = e(w_j|v)$. That describes the correspondence between the prime ideals over $\mathfrak{p}$ 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 $\mathcal{O}_L \otimes_{\mathfrak{o}_K} \mathfrak{o}_{K_v}$. Since $\mathfrak{o}_{K_v}$ is a PID, $\mathcal{O}_L \otimes_{\mathfrak{o}_K} \mathfrak{o}_{K_v}$ is a free $\mathfrak{o}_{K_v}$-module of rank $(L : K)$. Also

$$\mathcal{O}_L \otimes_{\mathfrak{o}_K} \mathfrak{o}_{K_v} \cong \prod_{w|v} \mathfrak{o}_{L_w}.$$

The mapping $\alpha \in L \to \alpha \otimes 1 \to (\alpha)$ is dense because the absolute values w are inequivalent, by the Weak Approximation Theorem. Also, since $\mathfrak{o}_{K_v}$ is closed, $\mathcal{O}_L \otimes_{\mathfrak{o}_K} \mathfrak{o}_{K_v}$ 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

$$\mathfrak{p} \to \mathcal{P} \to Q$$

in each of them. Then

$$\begin{aligned} e(Q|\mathfrak{p}) &= e(Q|\mathcal{P})e(\mathcal{P}|\mathfrak{p}), \\ f(Q|\mathfrak{p}) &= f(Q|\mathcal{P})f(\mathcal{P}|\mathfrak{p}), \\ (N_Q : K_\mathfrak{p}) &= (N_Q : L_\mathcal{P})(L_\mathcal{P} : K_\mathfrak{p}). \end{aligned}$$

39 Galois Extensions I (11/19)

Let L/K be a finite separable extension, K be the field of fractions of a Dedekind domain $\mathfrak{o}$, $\mathcal{O}_L$ be the integral closure of $\mathfrak{o}$ in L. Any prime ideal $\mathfrak{p}$ in $\mathfrak{o}$ lifts to an ideal $\mathfrak{p}\mathcal{O}_L$ with factors as

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

for all distinct prime ideals $\mathcal{P}_j$ lying over $\mathfrak{p}$ and $\mathcal{P}_j \cap \mathfrak{o}_K = \mathfrak{p}$. The primes $\mathcal{P}_j$ correspond to the inequivalent valuations w_j extending the valuation on K corresponding to $\mathfrak{p}$ to L. With regard to completions, $L_{\mathcal{P}_j} = L_{w_j}$. If we omit the j, the prime ideal in L_w $\mathcal{P}_w$ satisfies $\mathcal{P}_w \cap \mathcal{O}_L = \mathfrak{p}$.

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

Theorem 39.1. *G acts transitively on the prime divisors $\mathcal{P}_j$ of $\mathfrak{p}\mathcal{O}_L$. So all $e_j = e$ and all $f_j = f$ and so $[L : K] = efr$.*

The *decomposition group* (Zerlegungsgruppe in German) of $\mathcal{P}$ lying over $\mathfrak{p}$ is defined as

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

We have $[G : Z] = r$ and $Z(\mathcal{P}_i)$ is conjugate to $Z(\mathcal{P}_j)$ in G. The *inertia group* (Trägnngs in German) is defined as

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

$T(\mathcal{P})$ is a normal subgroup of $Z(\mathcal{P})$ and

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

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

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

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

40 Galois Extensions II (11/21)

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

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

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

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

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

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

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

$$\begin{aligned}(x+1)^p - 1 &= x^p + px^{p-1} + \binom{p}{2} x^{p-2} + \cdots + \binom{p}{p-1} x \\ &= x\left(x^{p-1} + px^{p-2} + \cdots + \binom{p}{p-1}\right)\end{aligned}$$

and $x^{p-1} + px^{p-2} + \cdots + \binom{p}{p-1}$ is 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

$$\begin{aligned}D_K &= (-1)^{\frac{p-1}{2}} \cdot p^{p-2} \\ &= \text{square of Vandermonde determinant} \\ &\quad\ \text{with entries equal to power of } w.\end{aligned}$$

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 $q\mathfrak{o}_F = \mathfrak{q}\bar{\mathfrak{q}}$ for some prime ideal $\mathfrak{q}$. $q \in \mathfrak{q}$. By earlier lemma, $\mathfrak{q} = (q, \alpha)$ for some $\alpha = a + b\sqrt{D}$. Then $q\mathfrak{o}_F = (q, a + b\sqrt{D})(q, a - b\sqrt{D})$. This proves $q|a^2 - b^2 D$. So D is a square mod q. So $(-1)^{\frac{p-1}{2}} \cdot p$ is a square mod q. $\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$. It has a unique subgroup H of order $\frac{p-1}{2}$ and $H = \{l^2 | l \in (\mathbb{Z}/p\mathbb{Z})^*\}$. 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 $Z(Q) \subset H$. $Z_{K/\mathbb{Q}}(q) \cong \mathrm{Gal}\left((\mathcal{O}_K)/(\mathbb{Z}/q\mathbb{Z})\right)$ 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,

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

41 Galois Extensions III (11/24)

Lemma 41.1. *Let 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*

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

where $p|c_j$ for $1 \le j \le n$ and $p^2 \nmid c_n$, then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

Proof. Suppose $p|\ [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then there exists $\beta \in \mathcal{O}_K$ with $p\beta \in \mathbb{Z}[\alpha], \beta \notin \mathbb{Z}[\alpha]$. let

$$p\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

where $b_j \in \mathbb{Z}$ for all $j = 0, \cdots, n-1$ and some b_j is not divisible by p. Let j be the smallest index such that $p \nmid b_j$. Then $p|b_i$ for $0 \le i < j$. Let $\gamma \in \mathcal{O}_K$ be

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

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

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

Since $p||c_n$, $p^{n-1}||c_n^{n-1}$, hence $p|b_j^n$ and so $p|b_j$. This is a contradiction. □

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

$$\begin{aligned} |\alpha^n|_v &= |-c_1\alpha^{n-1} - \cdots - c_n|_v \\ &\le \max\left(|-c_1\alpha^{n-1}|_v, \cdots, |-c_n|_v\right). \end{aligned}$$

By the Eisenstein condition, $p|c_1, \cdots, c_n$. So $|c_j|_v = |c_j|_p \le |p|_p < 1$. Then $|\alpha|_v < 1$. Since $|-c_j\alpha^{n-j}|_v = |c_j|_p|\alpha^{n-j}|_v < |p|_p$ for all $1 \le j \le n-1$ 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 $e(v|p) = n = (K : \mathbb{Q})$. Conversely, if $K/\mathbb{Q}$ 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 $q = p^{f_0}$. Let π 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 α has a minimal polynomial*

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

where $\pi|c_j$ for $1 \le j \le n$, $\pi^2 \nmid c_n$.

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 $q = p^{f_0}$. Let π 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 α is a $(q^n - 1)$-th root of unity in L.*

Proof. Earlier we showed that there is an isomorphism

$$(\mathcal{O}_L/\mathcal{P})^* \hookrightarrow L^*$$

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. $\square$

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

$$C_K = \mathrm{cl}(\mathcal{O}_K) = I_{\mathcal{O}_K}/P_{\mathcal{O}_K}.$$

The absolute norm of an ideal $\mathfrak{a} \subset \mathcal{O}_K$ is

$$N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}].$$

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

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

Proof. By Dedekind Theorem, every ideal has a prime factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. The Chinese Remainder Theorem says that

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}.$$

There are only finitely many ideals $\mathfrak{p}$ 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 $\mathfrak{p}$ lying over p and $N(\mathfrak{p}) = p_j^f$. So if $N(\mathfrak{a}) = n$, and if $\mathfrak{p}^e \| \mathfrak{a}$ then $p^{fe} = N(\mathfrak{p}^e) \leq N(\mathfrak{a}) = n$. That proves that

$$e \leq \frac{\log(n)}{f\log(p)}.$$

For a given n, that allows only finitely many prime ideals $\mathfrak{p}$ and only finitely many exponents e. That means there are finitely many $\mathfrak{a}$ such that $N(\mathfrak{a}) = n$. $\square$

We will show that there is a constant A depending on $K/\mathbb{Q}$ such that every ideal class contains an ideal $\mathfrak{b} \subset \mathcal{O}_K$ with $N(\mathfrak{b}) \leq A$.

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

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

Then

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

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

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

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

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

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

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

and hence

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

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

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

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

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 $\mathfrak{b} \in c$ such that*

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

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

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

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

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

Then cancel $N(\mathfrak{a})$. □

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 $\mathfrak{a} = \mathcal{O}_K$ in Theorem 42.2. Then $|N_{K/\mathbb{Q}}(y)| \geq 1$ and $N(\mathfrak{a}) = N(\mathcal{O}_K) = 1$. □

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:

$$\begin{aligned}
\frac{\left(\frac{\pi}{4}\right)^{(n+1)/2} \cdot \frac{(n+1)^{n+1}}{(n+1)!}}{\left(\frac{\pi}{4}\right)^{n/2} \cdot \frac{n^n}{n!}} &= \left(\frac{\pi}{4}\right)^{1/2} \cdot \frac{(n+1)^{n+1}}{(n+1) \cdot n^n} \\
&= \left(\frac{\pi}{4}\right)^{1/2} \cdot \frac{(n+1)^n}{n^n} \\
&= \left(\frac{\pi}{4}\right)^{1/2} \cdot \left(1 + \frac{1}{n}\right)^n.
\end{aligned}$$

Note that $\left(1+\frac{1}{n}\right)^n$ 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

$$\begin{aligned}&\sigma_j : K \hookrightarrow \mathbb{R} \text{ for } 1 \leq j \leq r_1,\\ &\sigma_j : K \hookrightarrow \mathbb{C} \text{ for } r_1+1 \leq j \leq r_1+r_2,\end{aligned}$$

and

$$\sigma_{j+r_2} = \overline{\sigma}_j \text{ for } r_1+1 \leq j \leq r_1+r_2.$$

Each σ_j induces an $\mathbb{R}$-linear map

$$\begin{aligned}f_j = \sigma_j \otimes \mathrm{id} : K \otimes_{\mathbb{Q}} \mathbb{R} &\to \mathbb{C}\\ x \otimes r &\mapsto r(x^{\sigma_j}).\end{aligned}$$

Set $V = K \otimes_{\mathbb{Q}} \mathbb{R}$ which is a n-dimensional $\mathbb{R}$-vector space. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Let $a_1, \cdots, a_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. 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,

$$\mathrm{vol}(R_d) = \int_{R_d} d\vec{x} = \frac{2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} d^n}{n!}.$$

For a fractional ideal $\mathfrak{a} \subset \mathcal{O}_K$, choose a $\mathbb{Z}$-basis $a_1, \cdots, a_n$ of $\mathfrak{a}$ over $\mathbb{Q}$ and map

$\sum_{j=1}^{n} a_j \otimes y_j$ to

$$\begin{bmatrix} x_1 \\ \vdots \\ x_{r_1+1} \\ \vdots \\ x_{r_1+r_2} \\ x_{r_1+r_2+1} \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sigma_1(a_1) & \cdots & \sigma_1(a_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{r_1+1}(a_1)) & \cdots & \mathrm{Re}(\sigma_{r_1+1}(a_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{r_1+r_2}(a_1)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(a_n)) \\ \mathrm{Im}(\sigma_{r_1+1}(a_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+1}(a_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Im}(\sigma_{r_1+r_2}(a_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(a_n)) \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_{r_1+1} \\ \vdots \\ y_{r_1+r_2} \\ y_{r_1+r_2+1} \\ \vdots \\ y_n \end{bmatrix} = J \begin{bmatrix} y_1 \\ \vdots \\ y_{r_1+1} \\ \vdots \\ y_{r_1+r_2} \\ y_{r_1+r_2+1} \\ \vdots \\ y_n \end{bmatrix}.$$

Then

$$\begin{aligned} \det(J) &= 2^{-r_2}|\det(\sigma_j(a_k))| \\ &= 2^{-r_2}|d_K|^{1/2}N(\mathfrak{a}). \end{aligned}$$

The image $\wedge = J\mathbb{Z}^n$ is a lattice in $\mathbb{R}^n$: a free $\mathbb{Z}$-module of rank n such that $\mathbb{R}^n/\wedge$ has finite volume.

$$\begin{aligned} \mathrm{vol}(\mathbb{R}^n/\wedge) &= |\det(J)|\mathrm{vol}(\mathbb{R}^n/\mathbb{Z}^n) \\ &\quad \text{(by the multivariable change-of-variables theorem)} \\ &= |\det(J)| \\ &= 2^{-r_2}|d_K|^{1/2}N(\mathfrak{a}). \end{aligned}$$

Lemma 43.1 (Minkowski-Blichfeldt Lemma)**.** *Let $\wedge$ be a lattice in $\mathbb{R}^n$ and S a compact, symmetric, convex subset of $\mathbb{R}^n$. If vol$(S) \geq 2^n$vol$(\mathbb{R}^n/\wedge)$, then S contains a non-zero point in $\wedge$.*

Proof of Theorem 42.2. Choose d so that

$$\mathrm{vol}(R_d) = \int_{R_d} d\vec{x} = \frac{2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} d^n}{n!} \geq 2^n 2^{-r_2}|d_K|^{1/2}N(\mathfrak{a}).$$

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

$$\sum_{j=1}^{r_1} |y^{\sigma_j}| + 2\sum_{j=r_1+1}^{r_1+r_2} |y^{\sigma_j}| \leq d.$$

Then

$$\begin{aligned}
|N(y)| &= \prod_{j=1}^{r_1} |y^{\sigma_j}| \\
&\leq \left(\frac{\sum_{j=1}^{n} |y^{\sigma_j}|}{n} \right)^n \\
&\quad \text{(Arithmetic-Geometry Mean Inequality)} \\
&\leq \frac{d^n}{n^n}.
\end{aligned}$$

Take d to be the smallest of all such values that work, then we have

$$\begin{aligned}
|N(y)| &\leq \frac{1}{n^n} \left(\frac{n!}{2^{r_1} (\frac{\pi}{2})^{r_2}} 2^n 2^{-r_2} |d_K|^{1/2} N(\mathfrak{a}) \right) \\
&= \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} |d_K|^{1/2} N(\mathfrak{a}).
\end{aligned}$$

□

44 Dirichlet's Unit Theorem (12/05)

Let $U_K = \mathcal{O}_K^*$ 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.) μ_K is a torsion submodule. The torsion-free quotient is $\mathcal{U}_K = U_K/\mu_K$.

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 $\mathcal{U}_K$ is called a system of fundamental units.

Define a map

$$\begin{aligned}
\psi : K^* &\to W = \mathbb{R}^{r_1+r_2} \\
u &\mapsto \left(\log |u^{\sigma_j}|_{1 \leq j \leq r_1}, 2 \log |u^{\sigma_j}|_{r_1+1 \leq j \leq r_1+r_2}\right).
\end{aligned}$$

So if $\vec{e} = (1, 1, \cdots, 1) \in \mathbb{R}^{r_1+r_2}$, then

$$\psi(u) \cdot \vec{e} = \log(N(u)).$$

So ψ maps U_K into the hyperplane $H = \{\vec{w} \in W : \vec{w} \cdot \vec{e} = 0\} = \vec{e}^{\perp}$. 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. *$\{a \in \mathcal{O}_K : |a^{\sigma_j}| \leq \beta$ 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 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 $H = \vec{e}^{\perp}$. Then there is another hyperplane $H_2 = \vec{b}^{\perp}$ with $\vec{b} \neq 0$, $\vec{b} \in W$, $\vec{b}$ is not any scalar multiple of $\vec{e}$, such that $\psi(U_K) \subset H_2$. By orthogonalization of $\vec{b}$ relative to $\vec{e}$, we may assume $\vec{b} \cdot \vec{e} = 0$. We will show that there exists $u \in U_K$ with $\psi(u) \cdot \vec{b} \neq 0$.

Consider the map

$$\begin{aligned} h : K &\to V = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \alpha &\mapsto (\alpha^{\sigma_j}). \end{aligned}$$

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 vol$(\mathcal{L}) \geq A$ then $\mathcal{L}$ contains a non-zero point $h(\alpha)$, $\alpha \in \mathcal{O}_K \backslash \{0\}$. Let

$$\mathcal{L} = \{\vec{x} \in V : |x_j| \leq \rho_j, 1 \leq j \leq r_1 + r_2\} \subset V.$$

Then

$$\mathrm{vol}(\mathcal{L}) = \left(\prod_{1 \leq j \leq r_1} 2\rho_j\right)\left(\prod_{r_1+1 \leq j \leq r_1+r_2} \pi\rho_j^2\right) = 2^{r_1}\pi^{r_2}\rho_1 \cdots \rho_{r_1}\rho_{r_1+1}^2 \cdots \rho_{r_1+r_2}^2.$$

Choose ρ's so that this equals A. Then for $\alpha \in \mathcal{O}_K$ with $\alpha \neq 0$, $h(\alpha) \in \mathcal{L}$, we have

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \rho_1 \cdots \rho_{r_1} \rho_{r_1+1}^2 \cdots \rho_{r_1+r_2}^2 = \frac{A}{2^{r_1} \pi^{r_2}} = A'.$$

Also $|N_{K/\mathbb{Q}}(\alpha)| \geq 1$. There are finitely many principal ideals $(\beta_j) \subset \mathcal{O}_K$ with $|N(\beta_j)| \leq A'$. Let

$$B = \max_j |\psi(\beta_j) \cdot \vec{b}|.$$

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 ρ_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,

$$\begin{aligned}
\psi(a) \cdot \vec{b} &= (\psi(\alpha) - \psi(\beta_j)) \cdot \vec{b} \\
&\geq \psi(\alpha) \cdot \vec{b} - B \\
&\geq \vec{r} \cdot \vec{b} - \sum_{j=1}^{r_1+r_2} (\log A') |b_j| - B \\
&> 0 \text{ (by the choice of } \vec{r}).
\end{aligned}$$

That proves $\vec{u} \notin H_2$ and hence finishes the proof. $\square$

Index