Algebraic Number Theory

Def An algebraic integer α is the root of a monic polynomial in $\mathbb{Z}[X]$.

Ex: $n \in \mathbb{Z}$ $(X-n)$

i (X^2+1)

$\sqrt{2}$ (X^2-2)

$i+\sqrt{2}$ (X^4-2X^2+9)

$i+\sqrt{2}+\sqrt{3}$?

$(i\cdot\sqrt{2})(i+\sqrt{2}+\sqrt{3})$?

Def An algebraic number field is a finite extension K of $\mathbb{Q}$.

Def The ring of integers $\mathcal{O}_K$ is the set of algebraic integers in K. (it is a ring).

Diophantine problems over $\mathbb{Z}$ quickly lead to questions about $\mathcal{O}_K$!

$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$: PID, UFD, Euclidean, Units $=\{\pm 1\}$.

But, is $\mathcal{O}_K$ a PID?, a UFD?, what are the units?

Example: (Lagrange): p odd prime. Then $p = x^2+y^2$ iff $p \equiv 1 \pmod 4$.

$\Rightarrow$) is easy

$\Leftarrow$) $p \equiv 1\ (4) \Rightarrow 4 \mid |\mathbb{F}_p^*|$ cyclic. $-1 \in \mathbb{F}_p$ is the only element of order 2, and there is an element of order 4 $\Rightarrow \exists m \in \mathbb{Z} : m^2 \equiv -1 \pmod p$.

$\Rightarrow p \mid (m^2+1) = (m-i)(m+i)$ in $\mathbb{Z}[i]$ (Gaussian integers).

Define Norm $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$, $N(x+iy) = x^2+y^2$. It is an euclidean norm (see Rotman §3.6)

$\Rightarrow \mathbb{Z}[i]$ euclidean $\Rightarrow$ PID $\Rightarrow$ UFD. (prime $\Leftrightarrow$ irreducible because PID).

The units are the elements of norm ± 1 $= \{\pm 1, \pm i\}$.

If $p \mid (m+i)$, then $m+i = \alpha p$, so $m+i \equiv \alpha p$ in $\mathbb{F}_p$, and so $p \mid m-i$

Thus $p \mid m+i-(m-i) = 2i$ and $N(p) \mid N(2) \Rightarrow p^2 \mid 4 \Rightarrow !!.$

Conclude that p is not irreducible, so $p = (a+bi)(\alpha+\beta i) \Rightarrow p^2 = \overbrace{(a^2+b^2)}^{\overset{\pm 1}{\cancel{x}}}\overbrace{(\alpha^2+\beta^2)}^{\overset{\pm 1}{\cancel{x}}}$ //

<u>Example 2</u>: $p = x^2 - 2y^2 \Leftrightarrow p \equiv \pm 1 \bmod 8$.

$\Rightarrow$/ easy

$\Leftarrow$/ $p \equiv \pm 1 \bmod 8 \Rightarrow m^2 \equiv 2 \bmod p$ has solutions, so

$$p \mid (m^2 - 2) = (m + \sqrt{2})(m - \sqrt{2}) \text{ in } \mathbb{Z}[\sqrt{2}].$$

$$N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$$
$$x + y\sqrt{2} \mapsto x^2 - 2y^2$$

Euclidean $\Rightarrow$ UFD and repeat the same argument. This has infinitely many solutions, though.

<u>Fact</u>: Unit group in $\mathbb{Z}[\sqrt{2}]$ is $\{\pm(1+\sqrt{2})^n\}_{n \in \mathbb{Z}}$

All solutions to $x^2 - 2y^2 = p$ are $\pm(1+\sqrt{2})^{2n}(x_0 + y_0\sqrt{2})$.

<u>Example 3</u>: For which p have the form $p = x^2 + 6y^2$?

work in the field $\mathbb{Q}(\sqrt{-6})$, ring $\mathbb{Z}[\sqrt{-6}]$

But $\mathbb{Z}[\sqrt{-6}]$ is not a UFD: $N(x + y\sqrt{-6}) = x^2 + 6y^2$.

$$-2 \cdot 3 = -6 = \sqrt{-6} \cdot \sqrt{-6}$$

$N(-2) = 4$, $N(3) = 9$, $N(-6) = 6 \Rightarrow -2, 3, \sqrt{-6}$ are all irreducible.

Also, the units are ± 1, so -2 and $\sqrt{-6}$ are <u>not</u> associate.

<u>Fact</u>: ideals in $\mathcal{O}_K$ can be factored uniquely as a product of prime ideals.

<u>eg</u>: $(-2) = -2\,\mathbb{Z}[\sqrt{-6}] = (-2, \sqrt{-6})^2$

$(3) = (3, \sqrt{-6})^2$

$(\sqrt{-6}) = (\sqrt{-6}, -2)(3, \sqrt{-6})$

$(-6) = (3, \sqrt{-6})^2(-2, \sqrt{-6})^2$.

Def R a ring (commutative, with 1). An R-module is an additive abelian group M with scalar multiplication $R\times M \to M$, $(r,m)\mapsto rm$ such that:

- $(r+r')m = rm + r'm$
- $r(m+m') = rm + rm'$
- $(rr')m = r(r'm)$
- $1m = m$

Examples:

1) $R=k$ is a field, then M is a vector-space.
2) Any abelian group is a $\mathbb{Z}$-module.
3) R is an R-module.
4) Ideals $I\subseteq R$ are also R-modules.

Def N is a submodule of M if it is an additive subgroup s.t. $RN\subseteq N$.

Example: if R is viewed as an R-modules the ideals are submodules (and submodules are ideals).

Def: M is a finitely-generated R-module if $\exists\, m_1,\dots,m_r\in M$ s.t. $M=\sum_{i=1}^{r} Rm_i$

Example: $\zeta = e^{i\frac{2\pi}{p}}$, p prime.

$\mathbb{Z}[\zeta]$ = set of polynomials on ζ with integer coefficients.

We have that $\zeta^{p-1}+\dots+\zeta^2+\zeta+1=0$, so $\mathbb{Z}[\zeta]=\sum_{i=0}^{p-2}\mathbb{Z}\zeta^i$ as a module.

Def $R\subseteq R'$ rings.

a) $b\in R'$ is *integral* over R if $\exists\, f(x)\in R[X]$ monic s.t. $f(b)=0$.

b) the *integral closure* of R in R' is the set of all elements of R' which are integral over R.

Basic situation:

R an integral domain.

K its fraction field $=\{\frac{r}{s} : r,s\in R, s\neq 0\}$.

Def R is <u>integrally closed</u> if every element in $K(R)$ that is integral over R is actually in R (i.e. if R is its own integral closure in K).

<u>Example</u>: $\mathbb{Z}$ is integrally closed (any UFD is):

$x/y \in \mathbb{Q}$ is integral over $\mathbb{Z}$ (assume x/y in lowest terms).

Then $\left(\frac{x}{y}\right)^n + a_{n-1}\left(x/y\right)^{n-1} + \dots + a_1 \frac{x}{y} + a_0 = 0 \Rightarrow x^n = yM$ with $M \in \mathbb{Z}$.

If $p \mid y$, then $p \mid x \Rightarrow !!$ Thus $y = \pm 1$. //

<u>Corollary</u>: The rational numbers that are algebraic integers are exactly the ordinary integers $(\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z})$.

<u>Motivation</u>: $K/\mathbb{Q}$ is a number field, $\mathcal{O}_K$ its ring of integers. (integral closure of $\mathbb{Z}$ in K). We wish to prove that $\mathcal{O}_K$ is a ring. It follows from the following general fact:

<u>Thm</u>: $R \subseteq R'$ rings. Then the integral closure of R in R' is a subring of R' containing R.

<u>Prop</u> If $R \subseteq R'$, then $b \in R'$ is integral over $R \Leftrightarrow R[b]$ is f.gen as R-module.

(eg $R = \mathbb{Z}$, $b = 1/3$, $\mathbb{Z}[1/3]$: no way it is fin gen!).

<u>Pf</u>

$\Rightarrow$) b integral $/R \Rightarrow b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0 \quad (a_i \in R)$.

by induction, $\forall m \geq n$, $b^m \in \sum_{i=0}^{n-1} R b^i \Rightarrow R[b] = \sum_{i=0}^{n-1} R b^i$

$\Leftarrow$) Suppose $R[b] = f_1(b)R + \dots + f_r(b)R \quad (f_i \in R[X])$. Let

$N := \max_i (\deg f_i)$. Then $b^{N+1} \in R[b] \Rightarrow b^{N+1} = \sum_{i \geq 1}^{r} a_i f_i(b)$ //

Prop: With the same setup, $b \in R'$ is integral over R iff b is contained in a subring B of R', with B a fin-gen R-module.

Pf $\Rightarrow$) Take $B = R[b]$.

$\Leftarrow$) Suppose $b \in B$. $B = \sum_{j=1}^{n} Rm_j$, $m_j \in R'$.

Then $bm_i \in B$, so $b \cdot m_i = \sum_{j=1}^{n} r_{ij} m_j$, $r_{ij} \in R$.

Set $A = bI - (r_{ij})$ and $d = \det A$.

Note that $A \cdot \begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix} = 0$.

Let A^* be the adjoint of A, i.e. $A^*A = d \cdot I$, so

$$A^*A \begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix} = 0 \Rightarrow d \begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix} = 0 \Rightarrow dm_i = 0 \ \forall i.$$

Now $\exists \{r_i\}$ s.t. $1 = \sum_{i=1}^{n} r_i m_i$. So $d \cdot 1 = \sum_{i=1}^{n} r_i (dm_i) = 0 \Rightarrow d = 0$

$\Rightarrow$ b is the root of $\det(XI - (r_{ij}))$, which is monic in $R[X]$. //

Recall: $(A^*)_{ij} = (-1)^{i+j} \det A_{ji}$ where A_{ji} is A with deleted j^{th} row and i^{th} col.

Theorem: $R \subseteq R'$ rings. The integral closure of R in R' is a ring.

We need two facts to prove it:

Lemma 1: $R \subseteq S \subseteq T$ rings. If S is a f-gen R-mod, and T is a f-gen S-mod, then T is a f-gen R-module.

Pf exercise.

Lemma 2: If b_1, b_2 are integral over R, then $R[b_1, b_2]$ is a fin-gen R-module.

Pf using Lemma 1, observe first that b_2 is integral over $R[b_1]$ (because $R[b_1] \supseteq R$), so $R[b_1, b_2]$ is f.gen $R[b_1]$-module. //

Rk: Lemma 2 generalises to any (finite) number of elements.

Pf (of theorem):

Take b_1, b_2 integral over R. Then $b_1 b_2,\ b_1 \pm b_2 \in R[b_1, b_2]$

As $R[b_1, b_2]$ is a f.g. R-module, so $b_1 b_2,\ b_1 \pm b_2$ are integral over R. //

Def We say that S is integral over R $\Leftrightarrow$ every element $s \in S$ is.

Prop: If $R \subseteq S \subseteq T$ and S is integral over R, and T is integral over S, then T is integral over R.

Pf $b \in T \Rightarrow b^n + s_{n-1} b^{n-1} + \dots + s_1 b + s_0 = 0$, $s_i \in S$. (*)

Let $B := R[s_0, s_1, \dots, s_{n-1}]$. So B is a f.gen R-module (by Lemma 2).

So (*) implies that $B[b]$ is a fin-gen B-module. As B is f.gen R-mod, b is integral over R by Lemma 1. //

Corollary: if $R \subseteq R'$, then the integral closure of R in R' is integrally closed (in R').

Pf Let S = int closure of R in R', T = int closure of S in R'.

Want to see $T = S$ (in fact, need only $T \subseteq S$).

T integral over S, S is int R, so T is integral over R, so $T \subseteq S$. //

Recall:

$$\begin{tikzcd} K \arrow[d, dash] & \mathcal{O}_K \arrow[d, dash] \\ \mathbb{Q} & \mathbb{Z} \end{tikzcd}$$

$\mathcal{O}_K$ = int. closure of $\mathbb{Z}$ in K.

Know: → $\mathcal{O}_K$ is a ring
→ $\mathcal{O}_K$ is integrally closed in K.

Would like to see that $K = \mathrm{Frac}(\mathcal{O}_K)$. So that then we will say that $\mathcal{O}_K$ is integrally closed.

In fact, we have the more stronger proposition:

__Prop__: if α is an algebraic ~~integer~~, then $\exists N \neq 0 \in \mathbb{Z}$ s.t $N \cdot \alpha$ is an algebraic integer.

Pf/ Given $a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$ $(a_i \in \mathbb{Z}, a_n \neq 0)$, see that $a_n \alpha$ is an algebraic integer. //

We want to show that O_K is a Dedekind domain. For it, we need still to see that it is Noetherian and that all primes are maximals.

__Remark__: R integrally closed integral domain, $K = Q(R)$, L/K a __finite__ extension of K and $b \in L$, then $\exists!$ ~~monic~~ polynomial $f(x) \in K[X]$, monic of least degree such that b is a root.

__Prop 2.5__: b integral over $R \iff f(x) \in R[X]$.

(try ~~to~~ use this to do exercise 4, page 7 [Janusz].

__Recall facts from Localization__:

Can regard $R_S \subseteq$ fraction field (when R is a domain).

__Prop__: There's a 1-1 correspondence between:

$$\left\{ \begin{array}{l} \text{Prime ideals of } R \\ \text{which do not intersect } S \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{prime ideals} \\ \text{of } R_S \end{array} \right\}$$

$$\mathfrak{p} \longmapsto \mathfrak{p} R_S$$

__Note__: if $s \in \mathfrak{p} \cap S$, then $s \cdot \frac{1}{s} \in \mathfrak{p} R_S \Rightarrow 1 \in \mathfrak{p} R_S$, so $\mathfrak{p} R_S = R_S$.

we can localize at a prime $\mathfrak{p}$ ($S = R \setminus \mathfrak{p}$).
Then $R_\mathfrak{p}$ has a unique maximal ideal, namely $\mathfrak{p} R_\mathfrak{p}$.

~~Def~~ A a ring is a <u>Discrete Valuation Ring</u> (DVR) if it is a PID with only one maximal ideal. (in PID, recall maximal $\Leftrightarrow$ prime).

<u>Example</u>: $\mathbb{Z}_{(p)} = \{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \}$, maximal $p\mathbb{Z}_{(p)}$ and is a PID because $\mathbb{Z}$ is.

Suppose R is a DVR, not a field, then $\mathfrak{p} \neq 0$ is the unique maximal.

Then:
- $\mathfrak{p} = \pi R$ for some $\pi \in R$. ($\mathfrak{p}$ is principal!)
- π is the unique prime element (i.e. irreducible elt).
  So $x \in R \Rightarrow x = u \cdot \pi^k$ for a unit u, $k \geq 0$.
- If I is an ideal, then $I = \pi^k R$ for some $k \geq 0$.

~~Def~~ R is <u>Noetherian</u> if every ideal is finitely generated.

~~Def~~ R is a <u>Dedekind domain</u> if:

i) R Noetherian.
ii) R Integral Domain
iii) $R_\mathfrak{p}$ is a DVR $\forall$ primes $\mathfrak{p} \neq 0$.

equivalently, R is a Dedekind domain if:

i) R Noetherian
ii) R Integral Domain
iii) R is Integrally closed.
iv) Every prime $I \subset R$ is maximal.

(3.16 [Janusz]).

<u>Goal</u>: prove that in a Dedekind Domain, ideals factor uniquely into primes (ideals).

Fact: All $\mathcal{O}_K$ (K number field) are Dedekind domains.

Exercise: (HW): $R = \mathbb{Z}[\sqrt{-6}]$ is the ring of integers of $\mathbb{Q}(\sqrt{-6})$ (by ex 4)

Assume $\mathfrak{p} = (2, \sqrt{-6})$ is a prime ideal.

So we know that $R_\mathfrak{p}$ is a DVR, so $\mathfrak{p} R_\mathfrak{p} = \pi R_\mathfrak{p}$ for some $\pi \in R$.

Find π.

Chinese Remainder Theorem:

B a ring, $Q_1, \dots, Q_n$ ideals such that $Q_i + Q_j = B$ $\forall i \neq j$ (pairwise coprime).

Then the natural map $B \longrightarrow B/Q_1 \oplus B/Q_2 \oplus \cdots \oplus B/Q_n$

is surjective, and the kernel is $I = \bigcap_{i=1}^{n} Q_i$ $\left(\text{so } B/I \cong \bigoplus_{i=1}^{n} B/Q_i\right)$.

Note: under these hypothesis, $\bigcap Q_i = \prod Q_i$ ([Janusz] 3.5).

A motivating example for what comes next:

Ex: $R = \mathbb{Z}$, $\mathfrak{U} = (45)$ $(= (3)^2 (5))$. We will factor it in another way:

Look at $\mathbb{Z}/45\mathbb{Z}$, and look at (0) (and factor it).

In $\mathbb{Z}/45\mathbb{Z}$, the only primes are (3) and (5).

$(0 = (3)^2 (5)$ in $\mathbb{Z}/45\mathbb{Z})$. Also, $45\mathbb{Z}_{(3)} = \boxed{3^2}\mathbb{Z}_{(3)}$ V.

$45\mathbb{Z}_{(5)} = \boxed{5}\mathbb{Z}_{(5)}$

$\longleftrightarrow$

Prop: Let B a Noetherian ring, and suppose that every prime in B is maximal.
Then: ↑ even the (0), if it is a prime.

1) Every ideal contains a product of prime ideals.
2) $\exists$ distinct prime ideals $\mathfrak{P}_i$ s.t. $0 = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_n^{a_n}$.
3) For these $\mathfrak{P}_i$, a_i, $B \simeq B/\mathfrak{P}_1^{a_1} \oplus \cdots \oplus B/\mathfrak{P}_n^{a_n}$
4) These $\mathfrak{P}_i$ are the only primes in B.

Note: (0) is prime $\Leftrightarrow$ (0) is maximal $\Leftrightarrow$ B is a field and then it is trivial.

Pf

1) Let $S = \{$ideals which don't contain a product of primes$\}$.

If $S \neq \emptyset$, $\exists$ a maximal element in S, call it $\mathfrak{m}$, which is not prime (otherwise it contains a product of primes).

$\Rightarrow \exists x, y \notin \mathfrak{m}$, s.t. $xy \in \mathfrak{m}$. Let $U = xB + \mathfrak{m}$, $V = yB + \mathfrak{m}$

So each U, V contains of primes, and $U \cdot V \subseteq \overset{\overset{\mathfrak{m}}{\in}}{xy}B + \mathfrak{m} \subseteq \mathfrak{m} \Rightarrow !!$

2) ✓ because it contains $\mathfrak{P}_1^{a_1} \cdot\cdot \mathfrak{P}_n^{a_n}$, but then it equals it.

3) Note that $\mathfrak{P}_i + \mathfrak{P}_j = B \xRightarrow{\text{book}} \mathfrak{P}_i^{a_i} + \mathfrak{P}_j^{a_j} = B$ $\forall a_i, a_j \in \mathbb{N}$. So C.R.T. $\Rightarrow$

$\Rightarrow B \left(= B/(0)\right) = B/\mathfrak{P}_1^{a_1} \oplus B/\mathfrak{P}_2^{a_2} \oplus \cdots \oplus B/\mathfrak{P}_n^{a_n}$.

4) $B \simeq B/\mathfrak{P}_1^{a_1} \oplus \cdots \oplus B/\mathfrak{P}_n^{a_n} = B_1 \oplus \cdots \oplus B_n$.

Then the ideals have the form $I = I_1 \oplus \cdots \oplus I_n$, I_j ideal in B_j

I prime $\Leftrightarrow B_1/I_1 \oplus \cdots \oplus B_n/I_n$ is an integral domain $\Leftrightarrow I = B_1 \oplus \cdot \oplus \underset{\overset{\shortparallel}{I_j}}{\overset{\text{prime}}{\mathfrak{P}}} \oplus \cdot \oplus B_n$.

So $I_j \overset{}{=} \mathfrak{P}$ needs to be a prime of $B/\mathfrak{P}_j^{a_j}$, i.e. a prime of B containing $\mathfrak{P}_j^{a_j} \Rightarrow \mathfrak{P}_j \subseteq \mathfrak{P}$. By $\left(\begin{matrix}\text{maximality}\\ \shortparallel \\ \text{primality}\end{matrix}\right)$, $\mathfrak{P}_j = \mathfrak{P}$. $\Rightarrow I_j = \mathfrak{P}_j/\mathfrak{P}_j^{a_j}$

which corresponds to $\mathfrak{P}_j \subseteq B$.

So the $\mathfrak{P}_j$ are the only primes in B.

Lemma 1: R a Dedekind domain, $\mathfrak{p} \neq 0$ a prime. Then.
Then the only ideals in $R/\mathfrak{p}^a$ are the powers of the ideal $\mathfrak{p}/\mathfrak{p}^a$, which is principal.
(i.e. $\mathfrak{p}/\mathfrak{p}^a, \mathfrak{p}^2/\mathfrak{p}^a, \ldots, \mathfrak{p}^{a-1}/\mathfrak{p}^a$).

Pf Follows from lemma 2, because $R_\mathfrak{p}$ is a DVR $\Rightarrow$ all ideals of $R_\mathfrak{p}$ are powers of $\mathfrak{p}R_\mathfrak{p}$.

Lemma 2: Under the same hypothesis, $R/\mathfrak{p}^a \cong R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$

Pf Look at

$$R \longrightarrow R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$$
$$r \longmapsto r + \mathfrak{p}^a R_\mathfrak{p}$$

The kernel is $(\mathfrak{p}^a R_\mathfrak{p}) \cap R = \mathfrak{p}^a$. So only need to prove that it is a surjection. (see book).

//

Main Theorem: R be a Dedekind domain. Every nonzero ideal can be written
up to order $\rightarrow$ uniquely as a product of primes, $U = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$

Proof: R/U is Noetherian & every prime is maximal. So R/U has only finitely many primes $\bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_n$. These are in 1-1 corresp to the (only finitely many) primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ which contain U.

Let $(0) = \bar{\mathfrak{p}}_1^{b_1} \cdots \bar{\mathfrak{p}}_n^{b_n}$ in R/U. So $\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n} \subseteq U$

By CRT, $R/\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n} \cong R/\mathfrak{p}_1^{b_1} \oplus \cdots \oplus R/\mathfrak{p}_n^{b_n}$

The ideals on RHS have the form $\left(\mathfrak{p}_1^{c_1}/\mathfrak{p}_1^{b_1}\right) \oplus \cdots \oplus \left(\mathfrak{p}_n^{c_n}/\mathfrak{p}_n^{b_n}\right)$ for some $c_i \leq b_i$

which are in 1-1 correspondence with ideals containing $\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n}$ (like U!)

So $U = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_n^{c_n}$.

For uniqueness: The set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are uniquely determined.

$U \cdot R_{\mathfrak{p}_i} = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_n^{c_n} \cdot R_{\mathfrak{p}_i} = \mathfrak{p}_i^{c_i} R_{\mathfrak{p}_i}$. So $\mathfrak{p}_i^{c_i} = \mathfrak{p}_i^{c_i'} \Rightarrow \checkmark$.

//

We want a theorem on Dedekind domain definitions:

<u>Thm</u> (3.16). The following are equivalent defs of Dedekind domains:

1) R is Noeth, integral domain, $R_{\mathfrak{p}}$ is a DVR for all prime ideals $\mathfrak{p} \neq 0$.

2) R is Noetherian, integrally-closed, integral domain and every nonzero prime is maximal.

Pf (Deferred).

(typical approach:

$$(2) \underset{\substack{\text{of} \\ \text{fractional} \\ \text{ideals}}}{\Longrightarrow} \text{unique factorization} \overset{\text{we will see}}{\Longrightarrow} (1).$$

Fractional ideals & the Ideal class group.

Let R be a Dedekind domain, K the fraction field of R.

<u>Def</u>: M is a fractional ideal of R if it's a nonzero finitely-generated R-module $\subseteq K$.

<u>Examples</u>: • Every nonzero ideal $I \subseteq R$ is a fractional ideal. (these are called integral ideals).

• Given $c \in K^\times$, $M := cR$ is a fractional ideal, called "principal fractional ideal".

<u>Lemma</u>: Every fractional ideal M has the form $M = c \cdot I$, $\begin{cases} c \in K^\times \\ I \subseteq R \text{ integral ideal.} \end{cases}$

Pf If I is integral ideal, $I = Rx_1 + \cdots + Rx_n$ (R Noetherian).

So $c \cdot I = Rcx_1 + \cdots + Rcx_n$, a f.g. R-submodule of K. $\Rightarrow$ a fractional ideal.

Conversely, suppose that M is a fractional ideal.

Then $M = R\frac{x_1}{y_1} + \cdots + R\frac{x_n}{y_n} = \underbrace{\frac{1}{y_1 \cdots y_n}}_{c}\big(\overbrace{Rx_1y_2\cdots y_n + Ry_1x_2y_3\cdots y_n + \cdots}^{I}\big) = c \cdot I$

Alternate view: M fractional ideal $\Leftrightarrow \exists\, d \in R, d \neq 0$ s.t dM is an (integral) ideal.

($d = \text{denom}(c)$).

Example: Suppose R is a PID.

Then the fractional ideals are $c \cdot I = c \cdot (r)$, so $M = (cr)R$,

So all the fractional ideals are principal.

Let $I(R)$ be the set of all fractional ideals.

Goal: Show that $I(R)$ is a group.

Def: If M, N are two fractional ideals, then define $M \cdot N = \{\sum m_i n_i \text{ finite}, \, m_i \in M, n_i \in N\}$.

Claim: MN is a fractional ideal.

Pf by the lemma, $M = cI$, $N = dJ$ for $c, d \in K^\times$, $I, J \subseteq R$ integral ideals.

So $MN = cd(IJ)$ //

Def If M is a fractional ideal, define $\underline{M^{-1}} := \{x \in K : xM \subseteq R\}$.

Note: M^{-1} is closed under $+$, scalar mult. by R.

Claim: M^{-1} is a fractional ideal.

Pf Take $m \in M$, $m \neq 0$. Then $mM^{-1} \subseteq R$. So M^{-1} is a fractional ideal, by the "another approach" noted before. //

Def M is said to be invertible if $M \cdot M^{-1} = R$.

(note: MM^{-1} is always an integral ideal $\subseteq I$).

Example: $M = c \cdot R$ (ppal fract. ideal). $M^{-1} = c^{-1} R$, and $MM^{-1} = R$. So they are invertible.

Lemma: if $MN=R$, then $N=M^{-1}$.

Pf/ Recall that $M^{-1} = \{x \in K : xM \subseteq R\}$. So $N \subseteq M^{-1}$, always.

Now $M \cdot M^{-1} \subseteq R \Rightarrow (NM)M^{-1} \subseteq NR \Rightarrow M^{-1} \subseteq N$. //

Prop: Every integral ideal $U \neq 0$ is invertible (R a Dedekind domain).

Pf/

1. Prove that if $\mathfrak{p} \neq 0$ is prime, then $\mathfrak{p}$ is invertible.
2. Factor $U = P_1 \cdots P_n$ (allowing repetitions), then $U \cdot P_1^{-1} \cdots P_n^{-1} = R \cdot R \cdots R = R$. So by the Lemma just proven, $U^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$.

So need to prove that $\mathfrak{p}\mathfrak{p}^{-1} = R$.

We know that $\mathfrak{p}\mathfrak{p}^{-1} \subseteq R$ is an ideal, and $1 \in \mathfrak{p}^{-1}$ $(1 \cdot \mathfrak{p} \subseteq R)$

So $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$. As $\mathfrak{p}$ is maximal, either $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, or $\mathfrak{p}\mathfrak{p}^{-1} = R$.

But if $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1}\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}} = \pi R_{\mathfrak{p}}$.

So $\mathfrak{p}^{-1}\pi R_{\mathfrak{p}} = \pi R_{\mathfrak{p}} \Rightarrow \mathfrak{p}^{-1}R_{\mathfrak{p}} = R_{\mathfrak{p}} \Rightarrow \mathfrak{p}^{-1} \subseteq R_{\mathfrak{p}}$

Suppose $\mathfrak{p} = (x_1, \dots, x_n)$. Then $x_i \in \mathfrak{p}R_{\mathfrak{p}} = \pi R_{\mathfrak{p}} \Rightarrow$

$\Rightarrow x_i = \pi \frac{r_i}{s_i}$ where $s_i \notin \mathfrak{p}$, $r_i \in R$.

Set $\pi' := \frac{\pi}{s_1 \cdots s_n}$. Then $x_i = \pi' r_i'$, $r_i' \in R$.

So $\forall i$, $\frac{1}{\pi'} x_i \in R \Rightarrow \frac{1}{\pi'} \in \mathfrak{p}^{-1}$.

(Note that $\pi R_{\mathfrak{p}} = \pi' R_{\mathfrak{p}}$ because they differ by a unit).

The elements in $R_{\mathfrak{p}}$ are $u(\pi')^k$, $k \geq 0$, u unit.

So $\frac{1}{\pi'} \notin R_{\mathfrak{p}} \Rightarrow$!! //

Prop: Every fractional ideal M can be uniquely written as:

$$M = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_t^{a_t} \quad , \quad \underline{\underline{a_i \in \mathbb{Z}}} \quad , \quad \mathfrak{P}_i \text{ prime.}$$

(in particular, M is invertible).

Pf Given M, $\exists\, d \in R$ s.t. $dM = U$ integral.

Write $(d) = P_1 \cdots P_s$, $U = Q_1 \cdots Q_r$ the respective prime factorizations (allow repeat.)

So $M = Q_1 \cdots Q_r \cdot P_1^{-1} \cdots P_s^{-1}$

Uniqueness: Suppose $M = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_k^{b_k} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_t^{a_t}$, assume $\mathfrak{P}_i \neq \mathfrak{q}_j$ (otherwise cancel)

So can move the ideals so all the powers are nonnegative, and then the pf follows by uniqueness of factorizations on integral ideals. //

What we have seen so far is that $I(R)$ is the free abelian group generated by prime ideals of R.

Also, $P(R)$ is the subgroup of principal fractional ideals $((cR),\ c \in K^*)$.

Def The Class Group is the group $C(R) := I(R)/P(R)$.

Note: $C(R) = \{id\} \iff R$ is a PID.

And $C(R)$ "measures" how far is R from being a PID.

Note: If $\mathcal{O}_K$ is the ring of integers of K, ~~then~~ $C(\mathcal{O}_K)$ is finite.
(but this is not true for general Dedekind domains!)

• The trace and the norm in Separable extensions.

Suppose K is a field, and $\overline{K}$ its alg. closure.

Def: A polynomial $f(X) \in K[X]$ is separable if f has no repeated roots in $\overline{K}$.

- $\alpha \in \overline{K}$ is said to be separable over K if its minimal polynomial $(/K)$ is separable.
- L/K is a separable extension if every algebraic $\alpha \in L$ is separable over K.
- K is perfect if every irreducible polynomial in $K[X]$ is separable ($\Leftrightarrow$ every $\alpha \in \overline{K}$ is separable).

Thm: if $\mathrm{char}(K) = 0$ or K is finite, then K is perfect.

Example: $f(X) = X^p - T$ in $\mathbb{F}_p(T)$ is irreducible and factors (over $\overline{\mathbb{F}_p(T)}$) as $(X-t)^p \Rightarrow$ not separable!

Theorem (of the primitive element).
If L/K is a finite separable extension, then $\exists \alpha \in L$ s.t. $L = K(\alpha)$.

Embeddings:

Let L/K separable of degree n. By the thm, $L = K(\alpha)$, for some α.
Let $m(T) := \prod_{i=1}^{n} (T - \alpha_i)$, $\alpha_i \in \overline{K}$ be the minimal polynomial of α over K.
(the α_i are called the conjugates of α).

Fact: there are exactly n embeddings $\sigma_1, \dots, \sigma_n : L \hookrightarrow \overline{K}$ which extend the inclusion $K \hookrightarrow \overline{K}$ (we suppose a fixed inclusion $K \hookrightarrow \overline{K}$) defined by $\sigma_i(\alpha) := \alpha_i$

Def L/k, $[L:K]=n$, separable. The trace and norm of $x \in L$ is

- $T_{L/K}(x) := \sigma_1(x) + \dots + \sigma_n(x)$
- $N_{L/K}(x) := \sigma_1(x) \cdot \sigma_2(x) \cdots \sigma_n(x)$.

Example: $K = \mathbb{Q}(\sqrt[3]{2})$, $\alpha := \sqrt[3]{2}$. $m_\alpha(x) = x^3 - 2 = (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha)$ where ω is a primitive cube root of 1.

$$T_{K/\mathbb{Q}}(\alpha) = \alpha + \omega\alpha + \omega^2\alpha = (1+\omega+\omega^2)\alpha = 0.$$

$$N_{K/\mathbb{Q}}(\alpha) = \alpha \cdot \omega\alpha \cdot \omega^2\alpha = \alpha^3 = 2.$$

Basic facts:

1) $T_{L/K}(x)$, $N_{L/K}(y) \in K$

2) $T_{L/K}$ is additive and $N_{L/K}$ is multiplicative.

3) For any $c \in K$, $T_{L/K}(cx) = c\, T_{L/K}(x)$, and $N_{L/K}(cx) = c^n N_{L/K}(x)$.

4) If $L \supseteq E \supseteq K$ is a tower of finite sep. extensions, then:

$$T_{E/K}(T_{L/E}(x)) = T_{L/K}(x) \quad \text{and} \quad N_{E/K}(N_{L/E}(x)) = N_{L/K}(x).$$

Pf (1) Let H be a Galois extension of K containing L. $(H = K(\alpha_1, \dots, \alpha_n))$.

Suppose $\sigma \in Gal(H/K)$.

Claim: the collection $\sigma\sigma_1|_L, \dots, \sigma\sigma_n|_L$ is the same as $\sigma_1, \dots, \sigma_n$. (up to reordering).

Then $\sigma(T_{L/K}(x)) = \sigma\sigma_1(x) + \dots + \sigma\sigma_n(x) = \sigma_1(x) + \dots + \sigma_n(x) \Rightarrow$ ✓

(and similar for the norm).

(2) clear

(3) clear

(4)
$$\begin{tikzcd}[row sep=small] L \arrow[d, dash, "m"] \\ E \arrow[d, dash, "d"] \\ K \end{tikzcd} \Bigg\} n = md$$

$\tau_1,..,\tau_m$ embeddings of L fixing E.

$\sigma_1,..,\sigma_d$ embeddings of E fixing K

For each i, let σ_i' be an extension of σ_i to L.

Then $\{\sigma_i'\tau_j\}$ are n embeddings of L which fix K.

<u>Claim</u>: they are distinct (exercise).

So $\{\sigma_i'\tau_j\}$ are the n different embeddings corresponding to L/K.

$$T_{L/K}(x) = \sum_{i,j} \sigma_i'\tau_j(x).$$

$\sum \tau_j(x) \in E$, so σ_i can be exchanged by σ_i'

$$T_{E/K}(T_{L/E}(x)) = T_{E/K}\Big(\sum_j \tau_j(x)\Big) = \sum_i \sigma_i\Big(\sum \tau_j(x)\Big) \overset{\downarrow}{=} \sum_{i,j} \sigma_i'\tau_j(x) \quad ✓$$

(Similarly for the norm).

<u>Connection with the minimal polynomial.</u>

Let α be algebraic over K. Define a linear transformation

$$r_\alpha : K(\alpha) \longrightarrow K(\alpha) \qquad \text{of } K(\alpha) \text{ as a } K\text{-vectorspace.}$$
$$y \longmapsto \alpha y$$

<u>Claim</u>: the min. poly of r_α = the min. poly. of $\alpha = m(T) = \prod_{i=1}^{n}(T-\alpha_i)$

Also, as it has degree n, it equals the characteristic polynomial, i.e.

$$\det(T I_n - [\underset{\uparrow}{r_\alpha}])$$

matrix of r_α in any basis.

Note that $m(T) = T^n - T_{K(\alpha)/K}(\alpha)\,T^{n-1} + \cdots + (-1)^n N_{K(\alpha)/K}(\alpha)$

<u>Fact from linear algebra</u>: $T_{K(\alpha)/K}(\alpha) = tr([r_\alpha])$

$N_{K(\alpha)/K}(\alpha) = det([r_\alpha])$

In the general case, have:

$$\begin{tikzcd} L \arrow[d, dash, "d"'] \\ K(\alpha) \arrow[d, dash, "n"'] \\ K \end{tikzcd}$$

$r_\alpha : L \to L$, $y \mapsto \alpha y$, the min. poly of r_α is $m(T)$

But the char. poly. of r_α is $m(T)^d$

And so it is $T^{nd} - d\,T_{K(\alpha)/K}(\alpha)\,T^{nd-1} + \dots + (-1)^{nd}\left(N_{K(\alpha)/K}(\alpha)\right)^d$

Note: $T_{L/K}(\alpha) = T_{K(\alpha)/K}\left(T_{L/K(\alpha)}(\alpha)\right) = d\,T_{K(\alpha)/K}(\alpha)$.

$N_{L/K}(\alpha) = \cdots\cdots = \left(N_{K(\alpha)/K}(\alpha)\right)^d$

Example: $K = \mathbb{Q}(\alpha)$, $\alpha = \sqrt[3]{2}$

Basis $\{1, \alpha, \alpha^2\}$.

A matrix for r_α in this basis is $\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \rightsquigarrow$ trace $= 0$, det $= 2$

Discriminant of a Number Field.

Let L/K be a sep field extension, $\{u_1, \dots, u_n\}$ a basis for L/K.

~~Def~~ The discriminant of the basis $\{u_1, \dots, u_n\}$ is

$$\Delta(u_1, \dots, u_n) := \det\left(T_{L/K}(u_i u_j)\right)_{ij} \in K$$

Proposition: $\Delta(u_1, \dots, u_n) \neq 0$.

Pf (delayed).

Application: (the trace form and the dual basis)

Define a map $L \times L \to K$, $(x, y) \longmapsto T_{L/K}(x \cdot y)$, which is a symmetric bilinear form (cont application).

Claim: The form $\langle x,y\rangle := T_{L/K}(x\cdot y)$ is non-degenerate, i.e.

$(\text{if } \langle x,y\rangle = 0 \ \forall y\in L, \text{ then } x=0)$

pf (Suppose $x\neq 0$. (and $\langle x,y\rangle=0 \ \forall y\in L$) Set $x=u_1$ and complete it with a basis of L/K, $\overset{x}{\overset{\shortparallel}{u_1}},\dots,u_n$.

Then $\Delta(u_1,\dots,u_n)=0 \Rightarrow \{u_1,\dots,u_n\}$ not a basis $\Rightarrow\Leftarrow$!!

Def Let $L^* := \{K\text{-linear maps } L\to K\}$.

Define $\varphi: L\longrightarrow L^*$, $x\longmapsto \langle x,\cdot\rangle$. By non-degeneracy, $\ker\varphi = 0$

As $\dim L^* = \dim L$, φ is an isomorphism.

Now define f_i on L as $f_i(u_j) := \delta_{ij}$ (Kronecker-δ).

By the above, $\exists\ v_i\in L$ s.t. $f_i(u_j) = \langle v_i,u_j\rangle = T_{L/K}(v_iu_j) = \delta_{ij}$.

The set $\{v_1,\dots,v_n\}$ is called the dual basis for $\{u_1,\dots,u_n\}$.

which is uniquely defined by $v_i(u_j) := \delta_{ij}$.

Rk: $\{v_1,\dots,v_n\}$ is a basis:

if $\sum d_iv_i = 0$ then $(\sum d_iv_i)(u_j) = d_j = 0 \Rightarrow \checkmark$.

Pending pf of $\Delta(u_1,\dots,u_n)\neq 0$:

Let $\sigma_1,\dots,\sigma_n$ be embeddings of L fixing K (in some alg. closure).

$$T_{L/K}(u_iu_j) = \sigma_1(u_i)\sigma_1(u_j) \cdots \sigma_n(u_i)\cdot\sigma_n(u_j) = (\sigma_1(u_1),\dots,\sigma_n(u_1))\begin{pmatrix}\sigma_1(u_j)\\ \vdots\\ \sigma_n(u_j)\end{pmatrix}$$

Set $V^*(u_1,\dots,u_n) := \det(\sigma_i(u_j))_{1\le i,j\le n}$

So $\Delta(u_1,\dots,u_n) = (V^*(u_1,\dots,u_n))^2$

Note: if $\{\omega_1,\dots,\omega_n\}$ is another basis, $\omega_k = \sum_{j=1}^{n} c_{kj}u_j$, $c_{kj}\in K$, $(c_{kj})_{k,j}$ invertible.

$\Rightarrow \sigma_i(\omega_k) = \sum_{j=1}^{n} c_{kj}\sigma_i(u_j)$, and $V^*(\underline{\omega}) = \underset{*_0}{\det}(c_{kj})\cdot V^*(\underline{u})$.

↓

(cont deferred pf).

So only need to show that $\Delta(u_1,\dots,u_n)$ (or $V^*(u_1,\dots,u_n)$) is nonzero for one particular basis:

Let α be a primitive element $(L=K(\alpha))$. The basis is $\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$.

Let $\alpha_1,\alpha_2,\dots,\alpha_n$ be the conjugates of α $(\alpha_i=\sigma_i(\alpha))$.

$$V^*(1,\alpha,\dots,\alpha^{n-1})=\det\begin{pmatrix}1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & & \alpha_n\\ \alpha_1^2 & \alpha_2^2 & & \vdots\\ \vdots & & & \vdots\\ \alpha_1^{n-1} & \alpha_2^{n-1} & & \alpha_n^{n-1}\end{pmatrix}=\prod_{i>j}(\alpha_i-\alpha_j)\neq 0$$ because

as the extension is separable, all conjugates are different. //

<u>Corollary</u>: If $L=K(\alpha)$ of degree n, and separable. Then $\Delta(1,\alpha,\dots,\alpha^{n-1})=\prod_{i>j}(\alpha_i-\alpha_j)^2$

<u>Rk</u>: The number of pairs (i,j) in the product is $n(n-1)/2$.

So $\Delta(1,\dots,\alpha^{n-1})=(-1)^{n(n-1)/2}\prod_{i\neq j}(\alpha_i-\alpha_j)$.

Also, if $f(X)=\prod_{j=1}^{n}(X-\alpha_j)$ is the minimal poly of α,

$f'(X)=\sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)$, so $\Delta(1,\alpha,\dots,\alpha^{n-1})=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}f'(\alpha_i)$

Also, note that $\prod_{i=1}^{n}f'(\alpha_i)=N_{L/K}(f'(\alpha))$.

So $\Delta(1,\alpha,\dots,\alpha^{n-1})=(-1)^{\frac{n(n-1)}{2}}N_{L/K}(f'(\alpha))$.

Thm (6.1): Let R a Dedekind Domain, $K = K(R)$, L/K a finite sep. extension and $R' :=$ integral closure of R in L. Then:

1) R' is a finitely-generated R-module, and R' spans L over K.
2) R' is a Dedekind domain. (Noeth, int. closed, all nonzero primes are maximal).

Corollary: For $K = \mathbb{Q}$, $R = \mathbb{Z}$, then the ring of integers of a number field is a Dedekind Domain

Pf of theorem:

(fact: R Noeth & M a f.gen R-module, then M is Noetherian).

Claim 1: If $y \in L$, then $\exists\, d \in R \setminus \{0\}$ s.t. $dy \in R'$.

~~Note this~~ (is the same as we did for $K = \mathbb{Q}$).

So from a basis of L/K, can obtain a basis $\subseteq R'$, by scaling the elements of it. Call it $\{a_1, \dots, a_n\}$, $a_i \in R'$ $\forall i$.

Let $\{b_1, \dots, b_n\}$ be the dual basis ~~[illegible]~~.

Claim 2: $R' \subseteq \sum_{j=1}^{n} R b_j$

If we prove claim 2, then R' is f.gen/R. (because $\sum R b_j$ is a Noeth. R-module)

This is part (1) of theorem.

Also, every ideal of R' is a R-submodule of $\sum R b_j$, so it is f-gen as R-module, $\Downarrow$ f.gen as R'-module

i.e. R' is Noetherian.

Also, R' is the integral closure of R. So it is integrally closed.

Pf of claim 2: If $y \in R'$, then $T_{L/K}(y)$ is a coeff. of the char. poly for y over K (which is a power of the minimal poly). Prop 2.5 $\Rightarrow$ these coeffs lie in R

$\Rightarrow T_{L/K}(y) \in R$. So (in general): $T_{L/K}(R') \subseteq R$.

Write $y = \sum_{i=1}^{n} c_j b_j$, $c_j \in K$. Then $c_j = (y, a_k) = T_{L/K}(y a_k) \in R$ //

(cont pf)

We only need to show that every non-zero prime ideal $\mathfrak{P}$ of R is maximal.

Need two lemmas:

Lemma: Spz B, A integral domains, $B \supseteq A$, A integrally closed, B integral over A. Spz $\mathfrak{P}$ is a nonzero prime of B. Then $\mathfrak{P} \cap A$ is a nonzero prime of A.

Pf $A \to B/\mathfrak{P}$ has kernel $\mathfrak{P} \cap A$. So $A/\mathfrak{P} \cap A \hookrightarrow B/\mathfrak{P}$.

So $A/\mathfrak{P} \cap A$ is an integral domain, so $\mathfrak{P} \cap A$ is a prime.

To see that $\mathfrak{P} \cap A \neq 0$, exactly as one of the HW problem, or book.

Lemma: (with the same setup), if A is a field, B an integral domain, B integral over A, then B is a field.

Pf Spz $\mathfrak{P} \neq 0$ a maximal of B. By previous lemma, $\mathfrak{P} \cap A$ is a nonzero ideal of $A \Rightarrow 1 \in \mathfrak{P} \cap A \Rightarrow 1 \in \mathfrak{P} \Rightarrow \mathfrak{P} = B \Rightarrow !!$

$$\begin{tikzcd} L \arrow[d, dash] & R' \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\ K & R & \mathfrak{p} \end{tikzcd}$$

$\mathfrak{P} \neq 0 \Rightarrow \mathfrak{p} \neq 0$ Get $\overset{\swarrow\text{field}}{R/\mathfrak{p}} \hookrightarrow R'/\mathfrak{P}$ $\Rightarrow$ need to check that $R'/\mathfrak{P}$ is integral over $R/\mathfrak{p}$ (and then lemma applies and ✓).

But if $\overset{\neq 0}{x} \in R'$, $\exists\, f(X) \in R[X]$ monic s.t. $f(x) = 0$, then $\bar{f}(x + \mathfrak{P}) = 0 + \mathfrak{P} \Rightarrow$ ✓.

Discriminants of number fields & integral basis.

$$\begin{tikzcd} K \arrow[d, dash] & \supseteq & \mathcal{O}_K \arrow[d, dash] \\ \mathbb{Q} & \supseteq & \mathbb{Z} \end{tikzcd}$$

$\exists$ basis $\{\alpha_1, \dots, \alpha_n\}$ of K over $\mathbb{Q}$ with $\alpha_i \in \mathcal{O}_K$ $\forall i$.

So $\mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \dots \oplus \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K$.

By the theorem, (a claim of it) $\exists$ $\beta_1, \dots, \beta_n \in K$ s.t. $\mathcal{O}_K \subset \mathbb{Z}\beta_1 \oplus \dots \oplus \mathbb{Z}\beta_n$.

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

i.e. $\exists$ $\{\omega_1, \dots, \omega_n\} \subseteq \mathcal{O}_K$ s.t. $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n$.

Note: $\{\omega_1, \dots, \omega_n\}$ is a basis for K, also (over $\mathbb{Q}$).

Def A basis $\omega_1, \dots, \omega_n$ for K over $\mathbb{Q}$ is an integral basis if $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n$.

Rk: it is different from just asking that all the $\omega_i \in \mathcal{O}_K$!

Def If K is a number field of degree n, the discriminant of K is $\Delta_K := \Delta(\omega_1, \dots, \omega_n)$ where $\{\omega_1, \dots, \omega_n\}$ is any integral basis.

Pf of well definedness:

Spz $\mu_1, \dots, \mu_n$ another integral basis. Get $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$, $M \in \mathbb{Z}^{n \times n}$

Apply $\sigma_1, \dots, \sigma_n$ of K (embeddings) so:

$$\begin{pmatrix} \sigma_i(\mu_1) \\ \vdots \\ \sigma_i(\mu_n) \end{pmatrix} = M \begin{pmatrix} \sigma_i(\omega_1) \\ \vdots \\ \sigma_i(\omega_n) \end{pmatrix}$$

So $\left(\sigma_i(\mu_j)\right)_{j,i} = M \left(\sigma_i(\omega_j)\right)_{j,i}$.

Thus $\Delta(\underline{\mu}) = \underbrace{(\det M)^2}_{\overset{\|}{1}} \Delta(\underline{\omega})$.

because $\det M = \pm 1$ (M invertible)

Proposition: Let $\{\alpha_1, .., \alpha_n\}$ be a basis for $K/\mathbb{Q}$, with all $\alpha_i \in \mathcal{O}_K$. Let $d = \Delta(\alpha_1, .., \alpha_n)$. Then, each $\alpha \in \mathcal{O}_K$ can be written

$$\alpha = \frac{m_1}{d}\alpha_1 + \cdots + \frac{m_n}{d}\alpha_n \quad \text{where } m_i \in \mathbb{Z},\ d \mid m_i^2\ \forall i.$$

(note that $d \in \mathbb{Z}$, $d \neq 0$).

Note: $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \leq \mathcal{O}_K \subseteq \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}$.

Pf Spse $\alpha \in \mathcal{O}_K$. Write $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$, $x_i \in \mathbb{Q}$.

Let $\sigma_1, .., \sigma_n$ be the embeddings of K in $\mathbb{C}$.

Then,

$$\begin{aligned} \sigma_1(\alpha) &= x_1\sigma_1(\alpha_1) + \cdots + x_n\sigma_1(x_n) \\ &\vdots \\ \sigma_n(\alpha) &= x_1\sigma_n(\alpha_1) + \cdots + x_n\sigma_n(x_n) \end{aligned} \qquad \text{i.e. } \left(\sigma_i(\alpha_j)\right)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}.$$

Let $\delta := \det(\sigma_i(\alpha_j))$ (so $\delta^2 = d$).

Let γ_j be the determinant obtained by replacing j^{th} column in $(\sigma_i(\alpha_j))$ with $\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}$. Then, by Cramer's rule says $x_j = \frac{\gamma_j}{\delta}$.

Both $\gamma_j, \delta \in \mathcal{O}_K$, and $\delta^2 = d \in \mathbb{Z}$.

Then $\underset{\overset{\uparrow}{\mathbb{Q}}}{dx_j} = \delta\gamma_j \in \mathcal{O}_K \Rightarrow$ it is a integer. Call it $m_j = dx_j$.

$\frac{m_j^2}{d} = \frac{\delta^2\gamma_j^2}{d} = \gamma_j^2 \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

• Decomposition of Primes.

Let R be a Dedekind domain, $K=K(R)$ its fraction field, L/K a finite sep. ext, and R' the integral closure of R in L.

(we know that R' is a Dedekind domain, and R' a fin. gen. R-mod).

$$\begin{tikzcd} L \arrow[r, dash] \arrow[d, dash] & R' \arrow[d, dash] \\ K \arrow[r, dash] & R \end{tikzcd}$$

Let $P\neq 0$ a prime ideal of R.

Because R' is a Dedekind Domain, $PR' = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$, $\mathfrak{P}_i$ prime ideals of R'.

(Fact: $PR' \neq R'$) $\Rightarrow$ can take $g \geq 1$, and $e_i > 0$.

Note 1: if $\mathfrak{P}$ is a prime of R' s.t. $\mathfrak{P}\cap R = P$, then $\mathfrak{P} = \mathfrak{P}_i$ for some $1\leq i\leq g$.
We say that $\mathfrak{P}$ lies above p.

Note 2: R' is a fin. gen. R-module. So $R'/\mathfrak{P}$ is a fin. generated $\overset{\text{field}}{R/p}$-module, so $R'/\mathfrak{P}$ is a R/p-vectorspace, for all $\mathfrak{P}$ lying above p.

Def: $f(\mathfrak{P}|p) := \dim_{R/p}(R'/\mathfrak{P}) = [R'/\mathfrak{P} : R/p]$ the relative degree.

$e(\mathfrak{P}|p) :=$ exponent of $\mathfrak{P}$ in the factorization of PR' $(= v_{\mathfrak{P}}(PR'))$ is called the ramification index.

Theorem (Fundamental equality): if $PR' = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$, and $f_i := f(\mathfrak{P}_i/P)$.
Then:
$$\sum_{i=1}^{g} e_i f_i = [L:K]$$

Example: $K=\mathbb{Q}(i)$. $\mathcal{O}_K = \mathbb{Z}[i]$. $(-1\equiv 3\ (4))$.

$2\mathcal{O}_K = (1+i)^2 \Rightarrow g=1,\ f=1,\ e=2.$

$5\mathcal{O}_K = (2+i)(2-i) \Rightarrow g=2,\ e_1=e_2=f_1=f_2=1.$

$7\mathcal{O}_K = (7) \Rightarrow g=1,\ e=1,\ f=2.$

Recall the structure theorem for modules over PID:

If A is a PID and M is a finitely-generated torsion-free A-module. Then M is free.

($\exists\, x_1, \dots, x_n \in M$ s.t $M = Ax_1 \oplus \cdots \oplus Ax_n$).

Def: The rank n of M (is uniquely determined).

Thm (elementary divisor thm): if M is free of rank m over a PID A. Suppose that $N \subseteq M$ is a submodule of M. Then,

1) N is free of rank $n \leq m$.
2) $\exists$ a basis $y_1, \dots, y_m \in M$ s.t $a_1 y_1, \dots, a_m y_m$ are a basis for N where $a_i \in A \setminus \{0\}$ and $a_1 | a_2 | \cdots | a_n$.

We now prove the fundamental equality: $\sum_{i=1}^{g} e_i f_i = [L:K]$

Pf The Chinese-Remainder Thm is $\frac{R'}{pR'} \simeq \frac{R'}{\mathfrak{P}_1^{e_1}} \oplus \cdots \oplus \frac{R'}{\mathfrak{P}_g^{e_g}}$

We'll show that:

1) $\dim_{R/p}(R'/pR') = [L:K]$
2) $\dim_{R/p}\left(R'/\mathfrak{P}_i^{e_i}\right) = e_i f_i$

$\Rightarrow$ thm ✓.

(1) Recall R' is a f.gen. R-module, say $R' = \sum_{i=1}^{m} R x_i$.

Localizing at p, we get R_p is a PID. Let $S = R \setminus P$

$R'_S = R'_p = \{ \frac{r}{s} : r \in R', s \in R \setminus P \}$ ($R'_p = R'_S$ where $S = R \setminus p$).

We get $R'_p = \sum_{i=1}^{m} R_p x_i$. So R'_p is a f.gen. $\overset{\text{PID}}{R_p}$-module.

By the structure thm, R'_p is free over R_p. i.e.

$\exists\, y_1, \dots, y_n \in R'_p$ s.t $R'_p = R_p y_1 \oplus \cdots \oplus R_p y_n$ (note; $n = [L:K]$ since R'_p contains a basis for L/K)

Now $R'_p/pR'_p \simeq \bigoplus_{i=1}^{n} R_p/pR_p \simeq \bigoplus_{i=1}^{n} R/p \Rightarrow \dim_{R/p}\left(R'_p/pR'_p\right) = n = [L:K]$.

And can see (exercise) that $R'_p/pR'_p \simeq R'/pR'$ as a R/p-vectorspace.

To prove (2). Let $\mathfrak{p}^e$ be one of the prime powers (to avoid subscripts).

Note that:

$$R'/\mathfrak{p}^e \supseteq \mathfrak{p}^1/\mathfrak{p}^e \supseteq \mathfrak{p}^2/\mathfrak{p}^e \supseteq \cdots \supseteq \mathfrak{p}^{e-1}/\mathfrak{p}^e \supseteq \{0\}.$$

Each of the things in the chain is an R/p-vectorspace:

(define $(r+p)(b+\mathfrak{p}^e) := rb+\mathfrak{p}^e$, which is well-defined because $p \subseteq \mathfrak{p}^e$)

The successive quotients look like (3rd iso. thm) $\mathfrak{p}^a/\mathfrak{p}^{a+1}$, $0 \leq a \leq e-1$, each of which is a $R'/\mathfrak{p}$-vectorspace $\left(b \in \mathfrak{p}^a, \text{ then } (r+\mathfrak{p})(b+\mathfrak{p}^{a+1}) := rb+\mathfrak{p}^{a+1}\right)$

Claim: $\dim_{R'/\mathfrak{p}}(\mathfrak{p}^a/\mathfrak{p}^{a+1}) = 1$

Recall that $R'/\mathfrak{p}^{a+1}$ is a PID (Cor 3.12). So $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ has a single generator as $R'/\mathfrak{p}^{a+1}$-module. Hence $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ has a single generator as a $R'/\mathfrak{p}$-module (vectorspace).

If $b+\mathfrak{p}^{a+1}$, $b \in \mathfrak{p}^a$ be a generator (over $R'/\mathfrak{p}^{a+1}$).

Now, if $r \in R'$, $(r+\mathfrak{p})(b+\mathfrak{p}^{a+1}) = rb+\mathfrak{p}^{a+1} = (r+\mathfrak{p}^{a+1})(b+\mathfrak{p}^{a+1})$.

(eoc)

This means that $\dim_{R/p}(\mathfrak{p}^a/\mathfrak{p}^{a+1}) = f$

So by the chain, the total dimension $\dim_{R/p}(R'/\mathfrak{p}^e) = e \cdot f$

Decomposition in Galois Extensions.

Suppose L/K is Galois, $\left(K = \mathrm{Frac}(R),\ R' = \text{int. closure of } R \text{ in } L \right)$.

and $\sigma \in \mathrm{Gal}(L/K)$. Then $\sigma(R') = R'$.

(since $x \in L$ integral over $R \Leftrightarrow \sigma x$ is).

Suppose that $\mathfrak{P}$ is a prime over $\mathfrak{p}$. Then $$\overset{\text{integral domain} \Rightarrow \frac{R'}{\sigma(\mathfrak{P})} \text{ also}}{R'/\mathfrak{P}} \simeq \sigma(R')/\sigma(\mathfrak{P}) = R'/\sigma(\mathfrak{P})$$

So $\sigma(\mathfrak{P})$ is a prime ideal in R'.

Also, $\mathfrak{p} = R \cap \mathfrak{P}$ and thus by applying σ to it, $\mathfrak{p} = R \cap \sigma(\mathfrak{P})$.

So $\sigma(\mathfrak{P})$ lies above $\mathfrak{p}$.

Prop: $\mathrm{Gal}(L/K)$ acts transitively on the primes over $\mathfrak{p}$.

(i.e. if $\mathfrak{P}, \mathfrak{P}'$ lie over $\mathfrak{p}$, then $\exists \sigma \in \mathrm{Gal}(L/K)$ s.t. $\sigma \mathfrak{P}' = \mathfrak{P}$).

Pf Suppose $\mathfrak{P} \neq \sigma \mathfrak{P}'$ for any $\sigma \in \mathrm{Gal}(L/K)$.

Use CRT to find $x \in R'$ s.t. $x \equiv 0 \pmod{\mathfrak{P}}$, $x \equiv 1 \pmod{\sigma \mathfrak{P}'}$ $(\forall \sigma \in \mathrm{Gal}(L/K))$.

$$N_{L/K}(x) = \prod_\sigma \sigma x \in \overset{\text{take norm to } K}{K} \cap \overset{\text{because } x \in \mathfrak{P}}{\mathfrak{P}} \cap \overset{\text{because } \sigma x \in R' \forall \sigma}{R'} = \mathfrak{P} \cap \overset{R}{(K \cap R')} = \mathfrak{p} = R \cap \mathfrak{P}'$$

So $\prod_\sigma \sigma x \in \mathfrak{P}' \Rightarrow \sigma x \in \mathfrak{P}'$ for some $\sigma \Rightarrow x \in \sigma^{-1} \mathfrak{P}' \Rightarrow !!$

//

Suppose now that $\mathfrak{p} R' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. We will see that $e_i = e$ $\forall i$, and all ~~rel~~ deg f_i are the same $(= f)$. And so $efg = n$. Stated:

Corollary: If L/K is Galois, then $\mathfrak{p} R' = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ and all the relative degrees are equal to f.

Pf If $\mathfrak{P}_1, \mathfrak{P}_2$ lie over $\mathfrak{p}$, then $\exists \sigma \in \mathrm{Gal}(L/K)$ s.t. $\mathfrak{P}_2 = \sigma \mathfrak{P}_1$.

So $R'/\mathfrak{P}_1 \simeq R'/\mathfrak{P}_2$, and hence $f_1 = f_2$.

Also $\mathfrak{p} \subseteq \mathfrak{P}_1^e \overset{\text{applying } \sigma \text{ to it}}{\Leftrightarrow} \mathfrak{p} \subseteq \mathfrak{P}_2^e \Rightarrow$ ok.

//

~~Def~~ Ramification and Discriminant.

$$\begin{tikzcd} L \arrow[d, dash] & R' \arrow[d, dash] \\ K & R \end{tikzcd}$$

Assume (for simplicity) that $\forall$ prime ideals $\mathfrak{p} \neq 0$ in R, then $R/\mathfrak{p}$ is a perfect field (every finite extension is separable)

(in number fields, $R/\mathfrak{p}$ is finite, so ok).

Def A prime $\mathfrak{p}$ in R is <u>ramified</u> in R' if $e(\mathfrak{P}/\mathfrak{p}) \geq 2$ for some $\mathfrak{P}$ over $\mathfrak{p}$.

Def The <u>discriminant (ideal)</u> $\Delta(R'/R)$ is the ideal of R generated by all the discriminants $\Delta(x_1, \dots, x_n)$, where $\{x_1, \dots, x_n\}$ are basis for L/K contained in R'.

<u>Lemma</u>: If $R' = Rx_1 \oplus \dots \oplus Rx_n$, then $\Delta(R'/R)$ is a principal ideal, and $\Delta(R'/R) = (\Delta(x_1, \dots, x_n))$.

(in particular, if $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$ ← integral basis, then $\Delta(\mathcal{O}_K/\mathbb{Z}) = \Delta(\alpha_1, \dots, \alpha_n)\mathbb{Z}$ which is what we defined as $\Delta_K \mathbb{Z}$)

Pf Suppose $\{y_1, \dots, y_n\}$ is a basis for L/K inside R'.

Then $y_i = \sum_j r_{ij} x_j$, $r_{ij} \in R$.

Then $(\sigma_i(y_j)) = (r_{ij})(\sigma_i(x_j))$ (matrix eqn).

So $\Delta(y_1, \dots, y_n) = \det(r_{ij})^2 \cdot \Delta(x_1, \dots, x_n) \in \Delta(x_1, \dots, x_n)R$. //

<u>Lemma</u>: If S is a multiplicative set in R, then

$$\Delta(R'_S/R_S) = \Delta(R'/R)_S$$

<u>Why is it useful?</u> Suppose $\Delta(R'/R) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t}$. Then $\Delta(R'/R)_{\mathfrak{p}_i} = \mathfrak{p}_i^{n_i} R_{\mathfrak{p}_i}$ $\forall i$

And $\Delta(R'/R)_{\mathfrak{p}} = R_{\mathfrak{p}}$ for all other $\mathfrak{p}$.

(So the discriminant is like the product of the local discriminants).

Pf (of the lemma)

Suppose $x_1,\dots,x_n$ is a basis of L/K contained in R'. So as $R' \subseteq R'_S$, this is a basis in R'_S. So $\Delta(x_1,\dots,x_n) \in \Delta(R'_S/R_S)$.

Thus $\Delta(R'/R) \subseteq \Delta(R'_S/R_S)$. Thus $\Delta(R'/R)_S \subseteq \Delta(R'_S/R_S)$ (because RHS is a R_S-ideal)

Conversely, suppose $y_1,\dots,y_n$ is a basis of L/K contained in R'_S.

Then $\exists s \in S^{\subseteq R}$ s.t $\{sy_1,\dots,sy_n\}$ is a basis of L/K contained in R'.

So $\underbrace{\Delta(sy_1,\dots,sy_n)}_{\overset{\|}{s^{2n}\Delta(y_1,\dots,y_n)}} \in \Delta(R'/R)$. So $\Delta(y_1,\dots,y_n) \in \Delta(R'/R)_S$ //

Theorem: $\mathfrak{p}$ a prime in R. Then $\mathfrak{p}$ ramifies in $R' \Leftrightarrow \mathfrak{p} \mid \Delta(R'/R)$.

Corollary: If K is an alg. number field, $p \in \mathbb{Z}$ a prime, then p ramifies in $\mathcal{O}_K \Leftrightarrow p \mid \Delta_K$.

Example: $\mathbb{Q}(\sqrt{m}) = K$, m □-free, $m \equiv 2, 3 \pmod 4$.

Know $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$, integral basis $\{1, \sqrt{m}\}$.

$\Delta_K = \begin{vmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{vmatrix}^2 = 4m$. So p ramifies iff $p \mid 4m$

Pf (of thm): $S = R \setminus \mathfrak{p}$. Suppose that $\mathfrak{p}R' = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$. Then $\mathfrak{P}_i R'_S$ are the only prime ideals in R'_S. In R'_S, $\mathfrak{p}R'_S = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}R'_S$.

Conclusion: $\mathfrak{p}$ ramifies in $R' \Leftrightarrow \mathfrak{p}R_S$ ramifies in R'_S.

Also, $\mathfrak{p} \supseteq \Delta(R'/R) \Leftrightarrow \mathfrak{p}R_S \supseteq \Delta(R'/R)_S = \Delta(R'_S/R_S)$

So can assume $R = R_S \,(= R_{\mathfrak{p}})$ which is a DVR ($\Rightarrow$ PID).

So $R' = Rx_1 \oplus \cdots \oplus Rx_n$.

$y \in R'$. $r_y : x \mapsto xy$ a linear operator on L. Has a matrix $(r_{ij}) \in M_{n\times n}(R)$.

Then $T_{L/K}(y) = \text{trace}\,(r_{ij})$.

↓

Reducing mod $\mathfrak{p}$, we get:

$$R'/\mathfrak{p}R' = R/\mathfrak{p}\,\bar{x}_1 \oplus \cdots + R/\mathfrak{p}\,\bar{x}_n \quad \text{where } \bar{x}_i = x_i \text{ mod } \mathfrak{p}R'.$$

If $\bar{y} \in R'/\mathfrak{p}R'$, $r_{\bar{y}} : \bar{x} \mapsto \bar{y}\bar{x}$. Its matrix is $(\bar{r}_{ij})$.

Define $tr(\bar{y}) = tr(\bar{r}_{ij})$. So $\boxed{\overline{T_{L/K}(y)} = t_{E/}(\bar{y})}$ $(*)$

Then $\mathfrak{p} \mid \Delta(R'/R) \iff \overline{\Delta(x_1, \dots, x_n)} = \bar{0}$. By $(*)$, this happens iff $\Delta(\bar{x}_1, \dots, \bar{x}_n) = \bar{0}$.

Suppose now that $\mathfrak{p}R' = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. By CRT,

$$R'/\mathfrak{p}R' \simeq R'/\mathfrak{p}_1^{e_1} \oplus \cdots \oplus R'/\mathfrak{p}_g^{e_g} = V_1 \oplus \cdots \oplus V_g$$ (as rings & as $R/\mathfrak{p}$ - vectorspaces).

Let B_K be a basis for V_K. Then $(y_1, \dots, y_n) = (B_1, \dots, B_g)$ is a basis for $R'/\mathfrak{p}R'$. Let C be the change of basis matrix from $\{\bar{x}_i\} \mapsto \{y_j\}$.

Then $\Delta(\bar{x}_1, \dots, \bar{x}_n) = \overbrace{(\det C)^2}^{\neq 0} \cdot \Delta(y_1, \dots, y_n)$. (So $\Delta(\bar{x}_1, \dots, \bar{x}_n) = \bar{0} \iff \Delta(y_1, \dots, y_n) = \bar{0}$).

Note that $y_i y_j = 0$ except when y_i, y_j belong to the same V_K.

So $\Delta(y_1, \dots, y_n) = \begin{vmatrix} \Delta_1 & 0 \\ 0 & \Delta_g \end{vmatrix}$, where $\Delta_K = tr(\omega_i \omega_j)$, $\{\omega_1, \dots, \omega_t\}$ basis for V_K

Note that the operator "mult by $\omega_i \omega_j$" is zero except on V_K.

So $tr(\omega_i \omega_j) = tr_K(\omega_i \omega_j)$. $\xleftarrow{}$ trace of "mult by $\omega_i \omega_j$ on the K^{th} piece".

Suppose that $\mathfrak{p}$ is unramified. Then $V_K = R'/\mathfrak{p}_K$ is a sep. ext of $R/\mathfrak{p}$.

So $\det(\Delta_K) = \det(tr_K(\omega_i \omega_j)) \neq \bar{0}$. So $\Delta(y_1, \dots, y_n) = \det \Delta_1 \cdots \det \Delta_n \neq \bar{0}$.

Suppose now that $\mathfrak{p}$ is ramified. So $V_K = R'/\mathfrak{p}_K^{e_K}$, $e_K \geq 2$.

Can choose a basis $\{\omega_1, \dots, \omega_t\}$, where $\omega_1 \in \mathfrak{p}_K$. Then $(\omega_1 \cdot \omega_j)^{e_K} = 0$, so $\omega_1 \omega_j$ is nilpotent. Then "multip. by $\omega_1 \omega_j$" is nilpotent, so char poly is T^N, and so $tr(\omega_1 \omega_j) = 0$ $\forall j$. So $\det\big(tr(\omega_i \omega_j)\big) = 0$.

• Explicit factorization.

Theorem: Suppose that K is a number field, and $\mathcal{O}_K = \mathbb{Z}[\theta]$, $\theta \in \mathcal{O}_K$.
(17.4) Suppose $p \in \mathbb{Z}$ a prime, $f(x) \in \mathbb{Z}[x]$ is the min poly. for θ.
Suppose $\bar{f}(x) \equiv \bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r} \pmod{p}$, where $\bar{g}_i(x) \in \mathbb{Z}/p\mathbb{Z}[X]$. irred
Then $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i = (p, g_i(\theta))$, and
$f(\mathfrak{p}_i/p) = \deg g_i(x)$. , $e_i = e(\mathfrak{p}_i|p)$

or, more generally:

Theorem: Assume that $R'_S = R_S[\theta]$ for some θ. Let $f(x) \in R_S[x]$ be the minimal polynomial of θ over K. Spse that $\bar{f}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r}$ is the factorization in $\bar{R}[X]$ $(\bar{R} = R/p = R_S/pR_S)$ of $f(x)$. Then,

$$\begin{tikzcd} L \arrow[d, dash] & R' \arrow[d, dash] & R'_S = R_S[\theta] \\ K & R & R_S = R_p \end{tikzcd}$$

$$pR'_S = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \quad \text{where} \quad \mathfrak{p}_i = (pR'_S, \bar{g}_i(\theta)R'_S) \quad \text{and} \quad f(\mathfrak{p}_i/p) = \deg(\bar{g}_i(x))$$

$(g_i(\theta)$ is any lift of $\bar{g}_i(\theta))$.

Rk: this gives as well the factorization of pR'.

Note: if $R' = R[\theta]$, then $R'_S = R_S[\theta]$ $\forall p$, which implies the statement of the first theorem stated above. However, the second assumption is always true except for a finite set of primes.

Pf Have a natural map $R_S[X] \longrightarrow R_S[\theta] = R'_S$. Its kernel is
$G(X) \longmapsto G(\theta)$

$$(f(x)\cdot K[X]) \cap R_S[X] \overset{\text{check}}{=} f(X)R_S[X]. \quad \text{So} \quad R'_S = R_S[\theta] \simeq R_S[X]/(f(x))$$

The isomorphism thus imply

$$R'_S/pR'_S \overset{\text{exercise}}{\simeq} \bar{R}[X]/(\bar{f}(x)) \overset{\text{CRT}}{\simeq} \bar{R}[X]/(\bar{g}_1(x))^{e_1} \oplus \cdots \oplus \bar{R}[X]/(\bar{g}_r(x))^{e_r}$$

Suppose that $pR'_S = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}$.

Then $$R'_S/pR'_S \simeq R'_S/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus R'_S/\mathfrak{p}_t^{a_t}$$

↓

we've got $\frac{\bar{R}[x]}{(\bar{g}_1(x))^{e_1}} \oplus \cdots \oplus \frac{\bar{R}[x]}{(\bar{g}_r(x))^{e_r}} \simeq \frac{R'_S}{\mathfrak{p}_1^{a_1}} \oplus \cdots \oplus \frac{R'_S}{\mathfrak{p}_t^{a_t}}$.

The maximal ideals are $\text{all} \oplus \text{all} \oplus \cdots \oplus \frac{(\bar{g}_i(x))}{(\bar{g}_i(x))^{e_i}} \oplus \text{all} \cdots$ and the quotients are $\bar{R}[x]/\bar{g}_i(x)$.

On the RHS, the maximal ideals are $\text{all} \oplus \cdots \oplus \frac{\mathfrak{p}_i}{\mathfrak{p}_i^{a_i}} \oplus \text{all} \cdots$

the quotients are $R'_S/\mathfrak{p}_i$.

So $r = t$, and after some reordering, $\bar{R}[x]/\bar{g}_i(x) \simeq R'_S/\mathfrak{p}_i$, and the $e_i = a_i$, also.

Also, $\dim_{\bar{R}}\left(\bar{R}[x]/(\bar{g}_i(x))\right) = \deg(\bar{g}_i(x))$, which implies the claim for f_i's.

To prove $\mathfrak{p}_i = PR'_S + g_i(\theta)R'_S$, it is an easy exercise.

We want to see now that the assumption that $R'_S = R_S[\theta]$ is not too restrictive:

Theorem (7.5): Suppose $\theta \in R'$ has $L = K(\theta)$ (primitive el't thm + clearing denominator).
Set $\Delta(\theta) = \Delta(1, \theta, \ldots, \theta^{n-1})$, $n = [L:K]$.
Then $\Delta(\theta)R' \subseteq R[\theta] \subseteq R'$, i.e.
(every element of R' has the form $\frac{r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}}{\Delta(\theta)}$)
(look pf in book) (did $R = \mathbb{Z}$ case earlier).

Corollary: Suppose $P \neq 0$ is a prime ideal in R, and $\Delta(\theta) \notin P$. Then $R'_S = R_S[\theta]$.

Pf We have $\Delta(\theta)R' \subseteq R[\theta] \Rightarrow \Delta(\theta)R'_S \subseteq R_S[\theta] \overset{\Delta(\theta) \notin P \Rightarrow \text{unit}}{\Rightarrow} R'_S \subseteq R_S[\theta]$

The opposite containment is ~~[illegible]~~ easy.

Example: $K = \mathbb{Q}(\sqrt{d})$, d squarefree. $\theta = \sqrt{d}$, min poly is $X^2 - d$.

$\Delta(\sqrt{d}) = 4d$ (recall that $\Delta(\sqrt{d}) = \begin{cases} 4d & \text{if } d \equiv 2,3 \ (4) \\ d & \text{if } d \equiv 1 \ (4) \end{cases}$).

The theorem works if $p \nmid 4d$.

1) if $\left(\frac{d}{p}\right) = 1$, then $X^2 - d \equiv (X-a)(X+a) \ (p)$ (where $a^2 \equiv d \bmod p$).

~~Writing~~ $p\mathcal{O}_K = P_1 P_2$, where $P_1 = (p, \sqrt{d} - a)$, $P_2 = (p, \sqrt{d} + a)$

2) if $\left(\frac{d}{p}\right) = -1$, then $X^2 - d$ is irreducible ~~mod~~ (p), so $p\mathcal{O}_K = P$, $P = (p)\mathcal{O}_K$.

For the primes $p \mid 4d$, have to do it case by case:

(sub) Example: $d \equiv 3 \pmod 4$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

if $p \mid d$, $X^2 - d \equiv X^2 \bmod p$, so $p\mathcal{O}_K = (p, \sqrt{d})^2$

if $p = 2$, $X^2 - d \equiv (X+1)^2 \pmod 2$, so $2\mathcal{O}_K = (2, \sqrt{d}+1)^2$

If $\left(\frac{a}{2}\right) := \begin{cases} 0 & a \text{ even} \\ 1 & \text{if } a \equiv \pm 1 \bmod 8 \\ -1 & \text{if } a \equiv \pm 5 \bmod 8 \end{cases}$, then.

Fact: $\forall$ primes p,

$\left(\frac{\Delta_K}{p}\right) = 1 \Leftrightarrow p\mathcal{O}_K = P_1 P_2$, P_i distinct. (p splits)

$\left(\frac{\Delta_K}{p}\right) = -1 \Leftrightarrow p\mathcal{O}_K = P_1$ (p is inert)

$\left(\frac{\Delta_K}{p}\right) = 0 \Leftrightarrow p\mathcal{O}_K = P_1^2$ (p ramifies).

and $\left(\frac{\Delta_K}{p}\right)$ is the "Kronecker character": it is a primitive Dirichlet character, defined modulo $|\Delta_K|$.

Norm of Ideals.

$$\begin{tikzcd} L \arrow[d, dash] & R' \arrow[d, dash] \\ K & R \end{tikzcd}$$

Recall that $N_{L/K}(\alpha) = \prod_{\sigma} \sigma(\alpha)$ where σ runs over embeddings of L that fix K.

Let now U be an ideal of R'.

Def: The norm of U is $N_{L/K}(U) = N(U) = \{$ideal generated by $N(\alpha), \alpha \in U\} \subseteq R$.

$\left(= \sum_{a \in U} N(a) R\right)$.

Properties:

- $N(aR') = N(a) \cdot R \quad \forall a \in R'$.
- $N(U_S) = N(U)_S$ for S a multiplicative set in R.
- $N(U \cdot V) = N(U) N(V) \quad \forall\, U, V$ ideals in R'.

Pf (only the multiplicativity, the others are easy).

or using unique factorization.

Enough to show that $N(UV)_{\mathfrak{p}} = N(U)_{\mathfrak{p}} N(V)_{\mathfrak{p}}$ for all $\mathfrak{p}$ (non 0) primes in R (Lemma 3.18)

Let $S = R \setminus \mathfrak{p}$. So want to show $N(U_S V_S) = N(U_S) N(V_S)$.

As R'_S is a Dedekind domain. It has finitely many prime ideals (those lying over $\mathfrak{p}$), $\mathfrak{P}_1, \dots, \mathfrak{P}_g$. So it is a PID;

[$\forall i$, can choose $a \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$, $a \notin \mathfrak{P}_j$, $j \neq i$ (by CRT).

Then $v_{\mathfrak{P}}((a)) = v_{\mathfrak{P}}(\mathfrak{P}_i) \quad \forall \mathfrak{P}$ primes of R'_S. So $(a) = \mathfrak{P}_i$.

By factorization into primes, all ideals are principal.]

So $U_S = aR'_S$, $V_S = bR'_S$; and $N(U_S V_S) = N(abR'_S) = N(ab) R_S =$

$= N(a) N(b) R_S = N(aR'_S) \cdot N(bR'_S) = N(U_S) N(V_S)$.

So we only care about the norms of prime ideals, for the norm of any other ideal can be computed from the norm of its factorization

<u>Proposition</u>: Suppose $\mathfrak{P} \subseteq R'$ prime, $\mathfrak{P} \cap R = p$, and $f(\mathfrak{P}|p) = f$.
Then $N(\mathfrak{P}) = p^f$. (could take this as a definition).

Pf/ First, we show that $N(\mathfrak{P}) = p^m$ for some m. (We will assume L/K Galois) ~~to simplify the proof~~ ↖ then remove assumption

If $a \in \mathfrak{P}$, $N(a) = \prod_\sigma \sigma(a) \subseteq \mathfrak{P} \cap K = p$. So $N(\mathfrak{P}) \subseteq p$.

Suppose that $Q \neq p$ is another prime in R. Want $N(\mathfrak{P}) \not\subseteq Q$.

Choose $a \in \mathfrak{P}$, $a \notin \mathfrak{p}$ $\forall \mathfrak{p} \subseteq R'$ lying over Q (by CRT).

Then $\sigma a \notin \mathfrak{p}$ $\forall \mathfrak{p}$ over Q. ($Gal(L/K)$ permutes the primes lying over Q).

$\Rightarrow N(a) = \prod \sigma(a) \notin \mathfrak{p} \Rightarrow N(a) \notin Q \Rightarrow N(\mathfrak{P}) \not\subseteq Q$. So $N(\mathfrak{P}) = p^m$.

We can now localize at $S = R \setminus p$.

So can assume $R' = R'_S$, $R = R_S$. (nothing changes, not even m or f).

Write $\mathfrak{P} = \pi R'$. So $N(\pi R') = N(\mathfrak{P}) = p^m$

On the other hand, $N(\pi R') = N(\pi) R$ $\Rightarrow N(\pi) = p^m$.

Write $pR' = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, $\mathfrak{P} = \mathfrak{P}_1$.

Now, $N(\pi)R' = p^m R' = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{em}$

On the other hand, $N(\pi)R' = \prod_{\sigma \in Gal(L/K)} \sigma(\pi) R' = \prod_\sigma \sigma(\pi R') = \prod_\sigma \sigma(\mathfrak{P}_1) =$

$Gal(L/K)$ acts on $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ and its orbits have size g.

Also, $\# Gal(L/K) = e \cdot f \cdot g$.

So each of $\mathfrak{P}_i$ is $\sigma(\mathfrak{P})$ for $\frac{efg}{g} = ef$ ~~[illegible]~~ different $\sigma \in Gal(L/K)$.

So $\prod \sigma(\mathfrak{P}_1) = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{ef}$

This implies that $f = m$.

Proof of the general case (L/K non - Galois):

Let E be the normal closure of L/K. (i.e. $\begin{matrix} \mathfrak{Q} & E \\ \mathfrak{P} & L \\ p & K \end{matrix}$ Gal.).

Let $\mathfrak{Q}$ a prime over $\mathfrak{P}$. ($\mathfrak{Q} \subseteq R''$).

if $f(\mathfrak{Q}|\mathfrak{P}) = f_1$, $f(\mathfrak{P}|p) = f_2$, then $f(\mathfrak{Q}|p) = f_1 f_2$.

Now $N_{E/K}(\mathfrak{Q}) = p^{f_1 f_2}$ by the Galois case.

Also, $N_{E/K}(\mathfrak{Q}) = N_{L/K}(N_{E/L}(\mathfrak{Q})) = N_{L/K}(\mathfrak{P}^{f_1}) = N_{L/K}(\mathfrak{P})^{f_1}$.

Then $N_{L/K}(\mathfrak{P}) = p^{f_2}$ //

Absolute Norm.

Let K be a number field, $\mathcal{O}_K$ its ring of integers. If $U \subseteq \mathcal{O}_K$ is an ideal, then $N_{K/\mathbb{Q}}(U)$ is an ideal in $\mathbb{Z}$ $\Rightarrow$ it is principal, $N_{K/\mathbb{Q}}(U) = (m)$.

Assuming $m \geq 0$, this is the absolute norm of U.

~~Def~~ we write $m = \mathcal{N}(U)$. (and write, for instance, $N_{K/\mathbb{Q}}(U) = (\mathcal{N}(U))$.)

Example: $K = \mathbb{Q}(i)$, $U = (1+2i)$. $N_{K/\mathbb{Q}}(U) = (1+2i)(1-2i)\mathbb{Z} = +5\mathbb{Z}$.

So $\mathcal{N}((1+2i)) = 5$.

$\Rightarrow U$ is prime (by multiplicativity of $\mathcal{N}$). Also, $f(U|5) = 1$.

So $\mathbb{Z}[i]/_{(1+2i)} \cong \mathbb{Z}/_{5\mathbb{Z}}$

Prop. If $U \neq 0$, an ideal of $\mathcal{O}_K$, then $\mathcal{N}(U) = |\mathcal{O}_K/U|$.

Pf. LHS is multiplicative, and RHS is multiplicative if we factor U as a product of primes (by CRT). So it is enough to show that $\mathcal{N}(\mathfrak{P}^a) = |\mathcal{O}_K/\mathfrak{P}^a|$

Call $(p) = \mathfrak{P} \cap \mathbb{Z}$, p prime. Note also $\mathcal{N}(\mathfrak{P}^a) = p^{fa} \in \mathbb{Z}$, $f = f(\mathfrak{P}/p)$.

Also, have a chain $\mathcal{O}_K/_{\mathfrak{P}^a} \supsetneq \mathfrak{P}/_{\mathfrak{P}^a} \supsetneq \cdots \supsetneq \mathfrak{P}^{a-1}/_{\mathfrak{P}^a} \supsetneq 0$.

And the successive quotients are $\mathfrak{P}^v/_{\mathfrak{P}^{v+1}} \cong \mathcal{O}_K/_{\mathfrak{P}} \Rightarrow |\mathfrak{P}^v/_{\mathfrak{P}^{v+1}}| = |\mathcal{O}_K/_{\mathfrak{P}}| = p^f$ //

Example: Suppose $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$, $[K:\mathbb{Q}]=n$.
Then $\mathcal{N}(p\mathcal{O}_K) = p^n$, and $\mathcal{N}(\mathfrak{p}_i^{e_i}) = p^{e_i f_i}$.
So $n = \sum_{i=1}^{g} e_i f_i$!

Two notes:

1) $\alpha \in \mathcal{O}_K \Rightarrow T_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$! The converse is true only in quadratic extension.

2) $U \subseteq \mathcal{O}_K$, then $N_{K/\mathbb{Q}}(U) = (\mathcal{N}(U))$, $\mathcal{N}(U) \geq 0$.
We saw that $\mathcal{N}(U) = |\mathcal{O}_K/U|$, and so $\mathcal{N}(U)=1 \Leftrightarrow U = \mathcal{O}_K$.
So if $\mathcal{N}(U) = p$ prime then U is a prime ideal of res. deg $=1$. $(\mathcal{O}_K/U \simeq \mathbb{Z}/p\mathbb{Z})$

Algebraic Integers.

Recall that we proved that, if $\{\alpha_1,\ldots,\alpha_n\} \subseteq \mathcal{O}_K$ is a basis for K over $\mathbb{Q}$, then every $\alpha \in \mathcal{O}_K$ can be written as $\alpha = \sum_{i=1}^{n} \frac{m_i}{d}\alpha_i$, where $d = \Delta(\alpha_1,\ldots,\alpha_n)$, $m_i \in \mathbb{Z}$ and $d \mid m_i^2$.

Note that, from $d \mid m_i^2$, then if $p^a \mid d$, hence $\begin{cases} p^{a/2} \mid m_i & \text{if } a \text{ is even} \\ p^{\frac{a+1}{2}} \mid m_i & \text{if } a \text{ is odd.} \end{cases}$

Write $d = \pm d_0 d_1^2$, where d_0 is squarefree.

Then $d_0 d_1 \mid m_i$.

So can write $\alpha = \sum \frac{m_i' \alpha_i}{d_1}$. We get:

Prop (~9.1): With this setup, $\mathcal{O}_K$ is generated as a $\mathbb{Z}$-module by $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, together with the algebraic integers in the finite set $\left\{ \frac{a_1\alpha_1 + \cdots + a_n\alpha_n}{d_1} : 0 \leq a_i < d_1 \right\}$.

Note: it is not true in general that all the elements in this set are algebraic integers!

Example: $\alpha = \sqrt[3]{2}$, $K = \mathbb{Q}(\alpha)$.

$\Delta(1, \alpha, \alpha^2) = -3^3 \cdot 2^2$. $d_1 = 6$

Exercise: Define $S_p := \left\{ \frac{a_1\alpha_1 + \cdots + a_n\alpha_n}{p} \; ; \; 0 \leq a_i < p \right\}$.

If there are no non-zero algebraic integers in S_p ~~for~~ $p \mid d_1$, then

$O_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.

So we would only consider S_2 and S_3, with respectively 8 and 27 elements, and so it is easier.

(**Example**) to rule out $\frac{1+\alpha}{2}$, as $T(\alpha) = 0$. Then $T\left(\frac{1+\alpha}{2}\right) = T\left(\frac{1}{2}\right) + T\left(\frac{\alpha}{2}\right) = \frac{3}{2} \notin \mathbb{Z}$.

Sometimes, however, we cannot use the trace or norm to rule them out.

Example: $\beta = \frac{1+\alpha^2}{3} \in S_3$. $T(\beta) = 3 \cdot \frac{1}{3} = 1$ (as $T(\alpha^2) = 0$, α^2 satisfies $X^3 - 4$).

$1 + \alpha^2$ is a root of $(X-1)^3 - 4$. So $N(1+\alpha^2) = 5$.

Hence $N\left(\frac{1+\alpha^2}{3}\right) = \frac{5}{3^3} \notin \mathbb{Z}$

Remark: For any θ, can compute the minimal polynomial of θ and see whether it has coefficients in $\mathbb{Z}$.

Recall also that $f(x) := \det(X \cdot I - [r_\theta]) = m(x)^{[K:\mathbb{Q}(\theta)]}$

As both m and f are monic in $\mathbb{Q}[X]$, then $m(x) \in \mathbb{Z}[X] \Leftrightarrow f(x) \in \mathbb{Z}[X]$ (by Gauss' lemma).

Composite fields

Let E, L be algebraic number fields. The composite field EL is the intersection of all fields containing both.

$$\begin{tikzcd}[column sep=small] & EL \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & L \arrow[dl, dash] \\ & \cancel{K=}\, E\cap L \arrow[d, dash] & \\ & K & \end{tikzcd}$$

Def Call L and E linearly disjoint over K if $E\cap L = K$

We have a corresponding picture for their rings of integers:

$$\begin{tikzcd}[column sep=small] & \mathcal{O}_{EL} \arrow[dl, dash] \arrow[dr, dash] & \\ \mathcal{O}_E \arrow[dr, dash] & & \mathcal{O}_L \arrow[dl, dash] \\ & \mathcal{O}_{E\cap L} \arrow[d, dash] & \\ & \mathcal{O}_K & \end{tikzcd}$$

Def $\mathcal{O}_E\mathcal{O}_L :=$ largest subring of $\mathcal{O}_{EL}$ that contains both $\mathcal{O}_E$ and $\mathcal{O}_L$. ($\mathcal{O}_E\mathcal{O}_L \subseteq \mathcal{O}_{EL}$ always, by definition!).

Thm (9.3): With this notation, suppose that E, L are linearly disjoint over K.

Then, $\Delta(\mathcal{O}_E/\mathcal{O}_K)\,\mathcal{O}_{EL} \subseteq \mathcal{O}_E\mathcal{O}_L$.

(and, by symmetry, $\Delta(\mathcal{O}_L/\mathcal{O}_K)\,\mathcal{O}_{EL} \subseteq \mathcal{O}_E\mathcal{O}_L$).

Corollary: If $\Delta(\mathcal{O}_E/\mathcal{O}_K)$ and $\Delta(\mathcal{O}_L/\mathcal{O}_K)$ are coprime, then $\mathcal{O}_{EL} = \mathcal{O}_E\mathcal{O}_L$

We will prove another (weaker) version but the proof is "the same".

Theorem: Spse L, K linearly disjoint over $\mathbb{Q}$, and let $d := \gcd(\Delta_K, \Delta_L)$.

Then, $\mathcal{O}_{KL} \subseteq d^{-1}\mathcal{O}_K\mathcal{O}_L$.

Pf Let $\{\alpha_1, .., \alpha_m\}$, $\{\beta_1, .., \beta_n\}$ be integral bases for K and L, resp.

Then $\{\alpha_i\beta_j\}_{i,j}$ is a basis for KL over $\mathbb{Q}$ (not necessarily an integral basis).

If $\gamma \in \mathcal{O}_{KL}$, write $\gamma = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j$, $m_{ij}, r \in \mathbb{Z}$. s.t. $\gcd\{r, \{m_{ij}\}\} = 1$.

want to show that $r \mid \Delta_K$ and $r \mid \Delta_L$ (By symmetry, will do $r \mid \Delta_K$).

Note: $K = \mathbb{Q}(\theta)$, for some $\theta \Rightarrow KL = L(\theta) \Rightarrow$ minimal poly of θ over $\mathbb{Q}$ and L are the same.

By the note, every embedding σ of K extends to a unique embedding of $KL = L(\theta)$ which fixes L (map θ to $\sigma(\theta)$).

Apply such a σ to $\gamma = \sum \frac{m_{ij}}{r} \alpha_i \beta_j$, $\sigma(\gamma) = \sum_{i,j} \frac{m_{ij}}{r} \sigma(\alpha_i)\beta_j$

Set $x_i := \sum_{j=1}^{n} \frac{m_{ij}}{r} \beta_j$, and let $\sigma_1, \ldots, \sigma_m$ be the embeddings of K.

So $\sigma_k(\gamma) = \sum_{i=1}^{m} x_i \sigma_k(\alpha_i)$. By Cramer's rule,

$$x_i = \frac{\delta_i}{\delta} \quad \text{where} \quad \delta = \det\left(\sigma_k(\alpha_i)\right) \quad (\text{and so } \delta^2 = \Delta_K)$$

and $\delta_i \in \mathcal{O}_{KL}$. So $\Delta_K \cdot x_i \in \mathcal{O}_{KL}$

$\Delta_K x_i = \sum_j \frac{\Delta_K m_{ij}}{r} \beta_j \in \mathcal{O}_{KL} \cap L = \mathcal{O}_L$. As $\{\beta_j\}$ is an integral basis for $\mathcal{O}_L$,

then $\frac{\Delta_K m_{ij}}{r} \in \mathbb{Z}$ $\forall i,j \Rightarrow r \mid \Delta_K$ (since $(r, \{m_{ij}\}) = 1$) $\Rightarrow$ ✓ //

How to compute Δ_{KL}?

$$\left.\begin{array}{l} \{\alpha_1, \ldots, \alpha_m\} \text{ int. basis for } K \\ \{\beta_1, \ldots, \beta_n\} \text{ int. basis for } L \\ \{\alpha_i\beta_j\} \subseteq \mathcal{O}_{KL} \text{ a basis for } KL \end{array}\right\} \Rightarrow \Delta(\{\alpha_i\beta_j\}) = d^2 \Delta_{KL}, \ d = \text{index}$$

(like in HW4)

$$\Delta(\alpha_i\beta_j) = \det\left(T_{KL/\mathbb{Q}}(\alpha_i\beta_j\alpha_r\beta_s)\right) \overset{\text{check!}}{=} \det\left(\left(T_{K/\mathbb{Q}}(\alpha_i\alpha_r)\right)_{ir} \cdot \left(T_{L/\mathbb{Q}}(\beta_j\beta_s)\right)_{js}\right)$$

Let $A = \left(T_{K/\mathbb{Q}}(\alpha_i\alpha_r)\right)$ $(m \times m)$, $B = \left(T_{L/\mathbb{Q}}(\beta_j\beta_s)\right)$ $(n \times n)$.

Define $A \otimes B := \begin{bmatrix} Ab_{11} & \cdots & Ab_{1n} \\ \vdots & & \vdots \\ Ab_{n1} & \cdots & Ab_{nn} \end{bmatrix}$ $(nm \times nm)$.

L

General fact: $\det(A \otimes B) = \det(A)^n \det(B)^m$.

Then, we can get $\Delta(\{\alpha_i \beta_j\}) = \det(A \otimes B) = \Delta_K^n \Delta_L^m$.

Conclusion: If K, L are linearly disjoint $(K \cap L = \mathbb{Q})$, then:

1) $\Delta_{KL} \mid \Delta_K^{[L:\mathbb{Q}]} \Delta_L^{[K:\mathbb{Q}]}$ $(= \Delta(\mathcal{O}_K \mathcal{O}_L))$

2) If, in addition, Δ_K and Δ_L are coprime, then $\Delta_{KL} = \Delta_K^{[L:\mathbb{Q}]} \Delta_L^{[K:\mathbb{Q}]}$.

(because $\Delta(\{\alpha_i \beta_j\})$ is the discriminant of $\mathcal{O}_K \mathcal{O}_L$, and $\Delta(\mathcal{O}_K \mathcal{O}_L) = [\mathcal{O}_{KL} : \mathcal{O}_K \mathcal{O}_L]^2 \cdot \Delta(\mathcal{O}_{KL})$

Then as $\mathcal{O}_{KL} \subseteq \mathcal{O}_K \mathcal{O}_L$, then $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L \Leftrightarrow$ ✓.

Example: $\mathbb{Q}(\sqrt{m}, \sqrt{d})$, $(m, d) = 1$, $m \equiv 1 \ (4)$, $d \equiv 2, 3 \ (4)$, m, d $\square$-free.

$\mathbb{Q}(\sqrt{m}) \cap \mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ (why?).

$$\begin{cases} \Delta(\mathbb{Q}(\sqrt{m})) = m \\ \Delta(\mathbb{Q}(\sqrt{d})) = 4d \end{cases}$$

So $\Delta_K = m^2 (4d)^2$, and $\mathcal{O}_K = \mathbb{Z}\Big[\underbrace{\tfrac{1+\sqrt{m}}{2}}_{\alpha}\Big] \cdot \mathbb{Z}\big[\underbrace{\sqrt{d}}_{\beta}\big]$

with integral basis $\{1, \alpha, \beta, \alpha\beta\}$.

Cyclotomic Fields.

Let $n \in \mathbb{N}$, ζ_n a primitive n^{th} root of 1., $\zeta_n^n = 1$, $\zeta_n^m \neq 0 \quad 0 < m < n$.

Then $\mathbb{Q}(\zeta_n)$ is the splitting field of $X^n - 1$. It is called the n^{th}-cyclotomic field.

Thm (Kronecker - Webber): Every abelian extension $K/\mathbb{Q}$ (i.e Galois with abelian galois gp), is contained in some $\mathbb{Q}(\zeta_n)$ for some n.

Def (Euler ϕ-function): $\phi(m) := \# \{ d \leq m : (m,d) = 1 \}$.

Rk: $\phi(p^a) = p^{a-1}(p-1)$; $\phi(mn) = \phi(m)\phi(n)$ if $(m,n) = 1$.

Def If p^a is a prime power, define the cyclotomic polynomial

$$\Phi_{p^a}(X) := \frac{X^{p^a} - 1}{X^{p^{a-1}} - 1} = \frac{t^p - 1}{t - 1} = \underset{\substack{\shortparallel \\ f(t)}}{t^{p-1} + t^{p-2} + \dots + t + 1} \qquad \left(\text{where } t = X^{p^{a-1}}\right).$$

Basic facts.

1) $\Phi_{p^a}(x) = \prod_{\substack{k=0 \\ p \nmid k}}^{p^a - 1} (X - \zeta_{p^a}^k)$, of degree $\phi(p^a)$.

2) As $f(t+1)$ is Eisenstein at p, $f(t)$ is irreducible $\Rightarrow \Phi_{p^a}(X)$ is irreducible.

So if $K := \mathbb{Q}(\zeta_{p^a})$, then $[K : \mathbb{Q}] = \phi(p^a)$.

Prop 4.1: The prime p is totally ramified in K: $p\mathcal{O}_K = (1 - \zeta_{p^a})^{\phi(p^a)} \mathcal{O}_K$, where $(1 - \zeta_{p^a})$ is a prime ideal of relative degree 1 (i.e. norm p).

Pf Evaluating $\Phi_{p^a}(x)$ at $x = 1$, get $p = \prod_{p \nmid k} (1 - \zeta_{p^a}^k)$.

claim: if $p \nmid k$, then $\dfrac{1 - \zeta_{p^a}^k}{1 - \zeta_{p^a}}$ is a unit in $\mathcal{O}_K$. (easy check).

(cont pf)

The claim implies that $p\mathcal{O}_K = (1-\zeta_{p^a})^{\phi(p^a)}\mathcal{O}_K$.

As $efg = [K:\mathbb{Q}] = \phi(p^a)$, this is the prime factorization of $p\mathcal{O}_K$. //

<u>Prop 42</u>: If $K = \mathbb{Q}(\zeta_{p^a})$, then: $(p^a \neq 2)$

1) $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}]$.

2) $\Delta_K = \Delta(\zeta_{p^a}) = \pm p^{p^{a-1}\cdot(ap-a-1)}$ where $+ \Leftrightarrow ([p\equiv 1 (4)]$ or $[p^a = 2^a, a\geq 3])$.

~~Pf~~ Set $q := p^a$.

$$\Delta(\zeta_q) = (-1)^{\phi(q)(\phi(q)-1)/2}\cdot N_{K/\mathbb{Q}}(\Phi_q'(\zeta_q)).$$

1) Check that $\pm$ holds right.

2) $\Phi_q(x) = \dfrac{x^q-1}{x^{q/p}-1} \Rightarrow \Phi_q'(\zeta_q) = \dfrac{q\,\zeta_q^{q-1}}{\zeta_q^{q/p}-1}$

$$N(\Phi_q'(\zeta_q)) = \pm\frac{q^{\phi(q)}}{N_{K/\mathbb{Q}}(\zeta_p - 1)}$$ (where $\zeta_p = \zeta_q^{q/p}$ is a primitive pth root of 1).

So $N_{K/\mathbb{Q}}(\zeta_p - 1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1)^{[K:\mathbb{Q}(\zeta_p)]} = p^{\frac{\phi(q)}{p-1}}$

Now, just observe that the minimal poly. of $\zeta_q + 1$ is Eisenstein at p.

So by HW problem, $p \nmid [\mathcal{O}_K : \mathbb{Z}[1+\zeta_q]] = [\mathcal{O}_K : \mathbb{Z}[\zeta_q]]$.

And $\Delta(\zeta_q) = [\mathcal{O}_K : \mathbb{Z}[\zeta_q]]^2\cdot\Delta_K = \pm p^N$. as $p\nmid$ index, done. //

Later on we'll prove:

<u>Thm</u> (Minkowski): If K is a number field, $K \neq \mathbb{Q}$, then $|\Delta_K| > 1$.
(4.3)

In particular, some prime p ($\leftarrow$ depending on K.) ramifies in any K.

<u>Corollary</u> (4.4): If Δ_K, Δ_L are coprime, then $K\cap L = \mathbb{Q}$ (converse is false!).

~~Pf~~ Otherwise, $\Delta_{K\cap L} \neq \pm 1$, so some p ramifies in $K\cap L \Rightarrow$ ramifies in K and in $L \Rightarrow$
$\Rightarrow p \mid \Delta_K,\ p\mid\Delta_L \Rightarrow$!! //

• The (general) cyclotomic fields $\mathbb{Q}(\zeta_m)$.

$m = \prod p_i^{a_i}$. Then $\mathbb{Q}(\zeta_m)$ is the composition of all the $\mathbb{Q}(\zeta_{p_i^{a_i}})$.

Prop 4.5:

a) p ramifies in $\mathbb{Q}(\zeta_m) \Leftrightarrow p \mid m$.

b) The ring of integers in $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$.

Pf Induction on the number of distinct prime factors.

Suppose it is true for m, and $p \nmid m$ (note that we proved it for $m = p^a$).

$$\begin{tikzcd}
 & K = \mathbb{Q}(\zeta_m, \zeta_{p^a}) \arrow[dl, dash] \arrow[dr, dash] & \\
E = \mathbb{Q}(\zeta_m) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{p^a}) = L \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$(\Delta_E, \Delta_L) = 1$ (by induction hypothesis).

So $E \cap L = \mathbb{Q}$ (by corollary 4.4).

Hence, $\mathcal{O}_K = \mathcal{O}_E \mathcal{O}_L$, and $\Delta_K = \Delta_E^{[L:\mathbb{Q}]} \Delta_L^{[E:\mathbb{Q}]}$.

Corollary 4.6.

a) $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$.

b) $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, with $a \bmod m$ corresponding to $\zeta_m \mapsto \zeta_m^a$.

Pf (a) true if $m = p^a$. Both sides are multiplicative for coprime (m, n), so done.

(b) If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, then $\sigma(\zeta_m)$ is a primitive m^{th} root of 1, which is ζ_m^a for some (unique) a with $(a, m) = 1$, i.e. $a \in (\mathbb{Z}/m\mathbb{Z})^*$. Get an embedding of groups $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^*$. By order consideration, done!

Def: ~~The~~ mth cyclotomic polynomial is $\Phi_m(X) := \prod_{\substack{a=1 \\ (a,m)=1}}^{m-1} (X - \zeta_m^a) = \prod_{\sigma \in G} (X - \sigma(\zeta_m))$ (it has degree $\phi(m)$).

Also $\Phi_m(X) \in \mathbb{Z}[X]$, and it is the minimal polynomial of ζ_m.

Note: $X^n - 1 = \prod_{d | n} \Phi_d(X)$ (the roots are exactly the same).

which allows the computation of $\Phi_n(x)$, recursively.

- <u>Splitting of primes in $\mathbb{Q}(\zeta_n)$.</u>

We start with an (unmotivated) lemma:

<u>Lemma 4.7</u> Spse $p \nmid n$, and that $\mathfrak{P}$ is a prime of $\mathbb{Q}(\zeta_n)$, lying over p.

Then, the nth roots of 1; $\zeta_n, \zeta_n^2, \dots$, are all distinct modulo $\mathfrak{P}$.

Pf/

$$\prod_{j=1}^{n-1} (X - \zeta_n^j) = \frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \dots + X + 1.$$

Setting $X = 1$, get $n = \prod_{j=1}^{n-1} (1 - \zeta_n^j)$. If $\zeta_n^{j_1} \equiv \zeta_n^{j_2} \pmod{\mathfrak{P}}$, where $j_1 \not\equiv j_2 \ (n)$, get $\underbrace{\zeta_n^{j_1 - j_2}}_{\text{unit}} (1 - \zeta_n^j) \in \mathfrak{P}$ for some j, $1 \leq j \leq n-1$.

$\Rightarrow 1 - \zeta_n^j \in \mathfrak{P}$, because $\mathfrak{P}$ is prime. But then $n \in \mathfrak{P}$. $\Rightarrow$!! //

From now on, spse $p \nmid n$, and let $K = \mathbb{Q}(\zeta_n)$. We know that K is Galois, and p is unramified. So,

$p\mathcal{O}_K = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_g$, $\mathfrak{P}_i$ distinct, and $f(\mathfrak{P}_i | \mathfrak{P}) = f$ (Galois), and $f \cdot g = \phi(n)$

<u>Theorem 4.8</u>: Spse $p \nmid n$. Let f be the least positive integer s.t. $p^f \equiv 1 \ (n)$.

Then, p splits into $g = \phi(n)/f$ distinct primes in $\mathbb{Q}(\zeta_n)$, all of relative degree f.

Remark:

This is called the "cyclotomic reciprocity law":

To compute the splitting of p in $\mathbb{Q}(\zeta_n)$, would in principle involve computing $\Phi_n(x)$ mod p, which changes for each prime in consideration.

Knowing the theorem allows one to restrict it to the order of p mod n, which only depends on p mod n (finite for fixed n).

Pf (of theorem):

As $p \nmid n$, $p \in (\mathbb{Z}/n\mathbb{Z})^*$. So $\exists\, \sigma_p \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ defined by $\sigma_p(\zeta_n) = \zeta_n^p$.

Note that $\sigma_p^f = id \Leftrightarrow \sigma_p^f(\zeta_n) = \zeta_n \Leftrightarrow \zeta_n^{p^f} = \zeta_n \Leftrightarrow p^f \equiv 1\ (n)$.

Hence, σ_p has order the order of p mod n.

Suppose $\mathfrak{P}$ is a prime lying over p.

By definition of relative degree, $\mathcal{O}_K/\mathfrak{P}$ has $p^{f(\mathfrak{P}|p)}$ elements.

The multiplicative group of a finite field is cyclic, so

$f(\mathfrak{P}/p)$ is the least positive integer f s.t. $x^{p^f-1} \equiv 1 \pmod{\mathfrak{P}}$, $\forall x \in \mathcal{O}_K \setminus \mathfrak{P}$.

i.e. $x^{p^f} \equiv x \pmod{\mathfrak{P}}$. (($f = f(\mathfrak{P}/p)$ is the least positive integer s.t. ...) $\forall x \in \mathcal{O}_K$.

Claim: $x^{p^f} \equiv x \pmod{\mathfrak{P}}\ \forall x \in \mathcal{O}_K \Leftrightarrow \zeta_n^{p^f} = \zeta_n$

Note that, if the claim is true, then,

$f(\mathfrak{P}/p) = \text{least } f \text{ s.t. } x^{p^f} \equiv x \text{ mod } \mathfrak{P}\ \forall x = \text{least } f \text{ s.t. } \zeta_n^{p^f} = \zeta_n \Leftrightarrow \overset{\text{least } f \text{ s.t.}}{p^f \equiv 1\ (n)}$.

and the theorem follows.

Pf of claim:

$\Rightarrow]$ $x^{p^f} \equiv x \text{ mod } \mathfrak{P}\ \forall x \in \mathcal{O}_K \Rightarrow \zeta_n^{p^f} = \zeta_n \text{ mod } \mathfrak{P} \overset{\text{previous lemma}}{\Rightarrow} \zeta_n^{p^f} = \zeta_n$

$\Leftarrow]$ If $\zeta_n^{p^f} = \zeta_n$ and $x \in \mathcal{O}_K = \mathbb{Z}[\zeta_n]$, so $x = a_0 + a_1\zeta_n + \cdots + a_t\zeta_n^t$, $a_i \in \mathbb{Z}$.

So $x^{p^f} \equiv (\underset{a_0}{\underset{\shortparallel}{a_0^{p^f}}} + \underset{a_1}{\underset{\shortparallel}{a_1^{p^f}}}\underset{\zeta_n}{\underset{\shortparallel}{\zeta_n^{p^f}}} + \cdots + a_t^{p^f}\zeta_n^{tp^f}) \pmod{p\mathcal{O}_K} \equiv x \text{ mod } p\mathcal{O}_K$ ✓.

• Interpretation in terms of class field theory.

There is a "generalized class group", called $Cl_m(\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$ (defined in terms of m and ideal classes in $\mathbb{Z}$).

In Thm 4.7, we saw that $Cl_m(\mathbb{Q}) \xrightarrow{\sim} Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. (only need to define it on primes, because of Dirichlet arith. progression).

$$p \longmapsto \sigma_p : \zeta_m \mapsto \zeta_m^p .$$

Properties: i) $\mathbb{Q}(\zeta_m)$ is unramified away from m.

ii) The decomposition of p in $\mathbb{Q}(\zeta_m)$ is determined by the order of p in $Cl_m(\mathbb{Q})$.

In the general case, if k is a number field, and $\mathfrak{m}$ is a "divisor", there is the class group $Cl_{\mathfrak{m}}(k)$ (defined by objects belonging to k). It turns out to be that 1) $\exists!$ abelian extension K/k s.t. $Cl_{\mathfrak{m}}(k) \overset{\text{Artin symbol}}{\simeq} Gal(K/k)$

$$\mathfrak{p} \longmapsto \sigma_{\mathfrak{p}}$$

2) K/k unramified away from $\mathfrak{m}$.

3) Decomp. of $\mathfrak{p}$ in K is determined by the order of $\mathfrak{p}$ in the class group.

Suppose now that $p \mid n$. Write $n = p^a \cdot m$, $p \nmid m$.

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_{p^a}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{p^a}) \arrow[dl, dash] \\
& p \in \mathbb{Q} &
\end{tikzcd}$$

$\leftarrow$ invariants E, F, G. $\Rightarrow e \mid E$, $f \mid F$, $g \mid G$.

and $efg = \phi(m)\phi(p^a) = \phi(n)$

f, g s.t. $f \cdot g = \phi(m)$

$\leftarrow e = \phi(p^a)$

So $e = E$, $f = F$, $g = G$.

So, we know the splitting of any prime p in any cyclotomic field $\mathbb{Q}(\zeta_m)$!.

Example: $K = \mathbb{Q}(\zeta_{20})$.

- $2\mathcal{O}_K = \mathfrak{p}^2$, $f = 4$. $(e = 2, g = 1)$. $(\mathfrak{p} = (1+i))$.
- $5\mathcal{O}_K = (1+2i)^4(1-2i)^4$, $f = 1$. $(e = 4, g = 2)$.
- $7\mathcal{O}_K$ is unramified, $f = 4, e = 1, g = 2$. So $7\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. What is $\mathfrak{p}_i$??

How to find $\mathfrak{p}_1 \mathfrak{p}_2 = 7\mathcal{O}_K$. (in $K = \mathbb{Q}(\zeta_{20})$).

Method 1: write the minimal poly. for ζ_{20}, $\Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$.

Then $\Phi_{20}(X) = f_1(X) f_2(X) \bmod 7$, and $\mathfrak{p}_1 = (7, f_1(\zeta_{20}))$...

Method 2: Try to find a quadratic subextension where 7 already splits.

By one of the HW problems, $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$.

As $\left(\frac{5}{7}\right) = -1$, 7 doesn't split in $\mathbb{Q}(\sqrt{5})$.

Also, $\mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}(\zeta_{20})$, because $i \in \mathbb{Q}(\zeta_{20})$.

In this case, $\left(\frac{-5}{7}\right) = 1 \Rightarrow 7$ splits in $\mathbb{Q}(\sqrt{-5})$.

So can factor $X^2 + 5 \equiv (X+3)(X-3) \bmod 7$

Hence, $\mathfrak{p}_1 = (7, \sqrt{5} + 3)\mathcal{O}_K$, $\mathfrak{p}_2 = (7, \sqrt{-5} - 3)\mathcal{O}_K$.

Quadratic Reciprocity.

p an odd prime. The Legendre Symbol is $\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv a \bmod p \text{ has a solution} \\ -1 & \text{o/w} \end{cases}$
(for $p \nmid a$).

$\mathbb{F}_p^*$ is cyclic of order $p-1$. Then $(\mathbb{F}_p^*)^2$ has index 2, and $\left(\frac{a}{p}\right) = 1 \Leftrightarrow \bar{a} \in (\mathbb{F}_p^*)^2$.

So $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ (because $\mathbb{F}_p^* / \mathbb{F}_p^{*2} \simeq \{-1, +1\}$.

Also, $a \in \mathbb{F}_p^{*2} \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$. So $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Thm (quadratic reciprocity law). (Thm 4.9).

a) If p, ℓ are distinct odd primes, then $\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right) \cdot (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}$

b) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Pf only will do pt (a), using Gauss sums.

We work in $\mathbb{Z}[\zeta_\ell]$. Define a Gauss sum $\tau := \sum_{a \in \mathbb{Z}/\ell\mathbb{Z}} \left(\frac{a}{\ell}\right) \zeta_\ell^a \in \mathbb{Z}[\zeta_\ell]$.

Lemma 4.10: $\tau^2 = \left(\frac{-1}{\ell}\right) \ell$ (so $\pm\sqrt{\left(\frac{-1}{\ell}\right)\ell} \in \mathbb{Z}[\zeta_\ell]$).

pf (of the lemma)

Two facts:

1) $\sum_{a=0}^{\ell-1} \zeta_\ell^{at} = \begin{cases} 0 & \text{if } \ell \nmid t \\ \ell & \text{if } \ell \mid t \end{cases}$ $\leftarrow$ at runs through $\mathbb{Z}/\ell\mathbb{Z}$ as a does $\Rightarrow$ ✓. $\leftarrow$ easy

2) $\sum_{a=0}^{\ell-1} \left(\frac{a}{\ell}\right) = 0$ (exercise (Hint: multiply by $\left(\frac{x}{\ell}\right)$, where $\left(\frac{x}{\ell}\right) = -1$)).

Using this, write $\tau^2 = \sum_a \sum_b \left(\frac{ab}{\ell}\right) \zeta_\ell^{a+b} = \sum_{a\neq 0} \sum_{b \neq 0} \left(\frac{ab}{\ell}\right) \zeta_\ell^{a+b}$

In the inner sum, write $b = c \cdot a$. c runs through $(\mathbb{Z}/\ell\mathbb{Z})^\#$ as b does.

$$= \sum_{a \neq 0} \sum_{c \neq 0} \left(\frac{a^2 c}{\ell}\right) \zeta_\ell^{a+ca} = \sum_{c \neq 0} \left(\frac{c}{\ell}\right) \sum_{a \neq 0} \zeta_\ell^{a(1+c)}$$

The inner sum is now $\sum_{a \neq 0} \zeta_\ell^{a(1+c)} = \begin{cases} \ell - 1 & \text{if } c \equiv -1 \bmod \ell \\ -1 & \text{if } c \not\equiv -1 \bmod \ell \end{cases}$

So $\tau^2 = \left(\frac{-1}{\ell}\right)(\ell-1) + (-1) \sum_{c \neq 0,-1} \left(\frac{c}{\ell}\right) = \left(\frac{-1}{\ell}\right)(\ell - 1) + (-1) \cdot -\left(\frac{-1}{\ell}\right) = \left(\frac{-1}{\ell}\right)\ell.$ // (of lemma)

Pf of Theorem:

$$\tau^p = \left(\sum_a \left(\frac{a}{\ell}\right) \zeta_\ell^a\right)^p \overset{p \text{ odd}}{\equiv} \sum_a \left(\frac{a}{\ell}\right) \zeta_\ell^{ap} \pmod{p} \overset{\text{in the ring } \mathbb{Z}[\zeta_\ell]}{\equiv} \left(\frac{p}{\ell}\right) \overbrace{\sum_a \left(\frac{pa}{\ell}\right) \zeta_\ell^{ap}}^{=\tau} \pmod{p}$$

$$\equiv \left(\frac{p}{\ell}\right) \tau \pmod{p}$$

By the lemma, $\tau^p = \tau \cdot (\tau^2)^{\frac{p-1}{2}} = \tau \cdot \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}} \ell^{\frac{p-1}{2}} = \tau \cdot (-1)^{\frac{\ell-1}{2} \cdot \frac{p-1}{2}} \ell^{\frac{p-1}{2}} \overset{\ell^{\frac{p-1}{2}} \equiv \left(\frac{\ell}{p}\right) \bmod p.}{\equiv} \tau (-1)^{\frac{\ell-1}{2} \frac{p-1}{2}} \left(\frac{\ell}{p}\right)$ mod p

Combining it, we get $\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2} \frac{p-1}{2}} \left(\frac{\ell}{p}\right)$.

To cancel τ, multiply both sides by τ, and $\tau^2 \in \mathbb{Z}$. To cancel the (mod p), use just that p is odd (and both sides are ± 1).

• Hilbert's Ramification Theory.

Let L/K be a finite Galois extension (of number fields). Let $G = \mathrm{Gal}(L/K)$.

$$\begin{tikzcd}
L \arrow[d, dash] & \mathfrak{P} \arrow[dr, dash] & & \mathfrak{P}' \arrow[dl, dash] \\
k & & p &
\end{tikzcd}$$

Know that any two primes lying over p are conjugate ($\exists\, \sigma \in G$ s.t. $\mathfrak{P}' = \sigma\mathfrak{P}$).

<u>Def</u>: if $\mathfrak{P}$ is a prime of L, define its <u>decomposition group</u>

$$G_\mathfrak{P} := \{\sigma \in \mathrm{Gal}(L/k) : \sigma\mathfrak{P} = \mathfrak{P}\} \leq \mathrm{Gal}(L/k).$$

The <u>decomposition field</u> is $Z_\mathfrak{P}$ = the fixed field of $G_\mathfrak{P}$, $\{x \in L : \sigma x = x \ \forall \sigma \in G_\mathfrak{P}\}$.

By the fundamental theorem of Galois theory,

$$\begin{tikzcd}
L \arrow[d, dash] & \{1\} \arrow[d, dash] \\
Z_\mathfrak{P} \arrow[d, dash] & G_\mathfrak{P} \arrow[d, dash] \\
k & G
\end{tikzcd}$$

and $\mathrm{Gal}(L/Z_\mathfrak{P}) = G_\mathfrak{P}$.

and $[Z_\mathfrak{P} : k] =$ ~~[illegible]~~ $[G : G_\mathfrak{P}]$.

<u>Note</u>: The decomposition groups of all primes of L which lie over a fixed prime p of k are all conjugate,

$$G_{\sigma\mathfrak{P}} = \sigma \cdot G_\mathfrak{P} \cdot \sigma^{-1} \qquad \text{(check)}.$$

(and so, if the extension L/k is abelian, there's only one decomposition group).

<u>Important Fact</u>: $G_\mathfrak{P}$ encodes how the prime p splits in L:

If $p\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, and $\mathfrak{P} = \mathfrak{P}_1$.

As σ runs through the cosets of $G/G_\mathfrak{P}$, $\sigma\mathfrak{P}$ hits every prime above p exactly once. ($\sigma\mathfrak{P} = \sigma'\mathfrak{P} \Leftrightarrow \sigma, \sigma'$ are in the same coset of $G/G_\mathfrak{P}$).

So $g = [G : G_\mathfrak{P}] = [Z_\mathfrak{P} : k]$, and $ef = \#G_\mathfrak{P} = [L : Z_\mathfrak{P}]$.

Notes:

1) p non-split in $L \Leftrightarrow g=1 \Leftrightarrow Z_{\mathfrak{P}} = K$.

2) p totally split in $L \Leftrightarrow ef=1 \Leftrightarrow Z_{\mathfrak{P}} = L$.

Prop 5.1: Let $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$

1) $\mathfrak{P}_Z$ is non-split in L. (i.e. $\mathfrak{P}$ is the only prime above $\mathfrak{P}_Z$).

2) $e(\mathfrak{P}/\mathfrak{P}_Z) = e$, $f(\mathfrak{P}/\mathfrak{P}_Z) = f$.

3) $e(\mathfrak{P}_Z/p) = 1, f(\mathfrak{P}_Z/p) = 1$.

$$\begin{tikzcd}
\mathfrak{P} \arrow[d, dash] & L \arrow[d, dash] & \{1\} \arrow[d, dash] \\
\mathfrak{P}_Z \arrow[d, dash] & Z_{\mathfrak{P}} \arrow[d, dash] & G_{\mathfrak{P}} \arrow[d, dash] \\
p & K & G
\end{tikzcd}$$

(Rk: p need not split completely in $Z_{\mathfrak{P}}$!)

Pf 1) By FTGT, $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. So all primes over $\mathfrak{P}_Z$ have the form $\sigma\mathfrak{P}$, where $\sigma \in G_{\mathfrak{P}}$. But $\sigma\mathfrak{P} = \mathfrak{P}$ by def. of $G_{\mathfrak{P}}$, so done.

(2)(3),

$$\begin{tikzcd}
\mathfrak{P} \arrow[d, dash, "{e',f'}"'] \arrow[dd, dash, bend left, "{e,f}"] & L \arrow[d, dash, "ef"] \\
\mathfrak{P}_Z \arrow[d, dash, "{e'',f''}"'] & Z_{\mathfrak{P}} \arrow[d, dash, "g"] \\
p & K
\end{tikzcd}$$

We know: $\mathfrak{P}$ is the only prime lying over $\mathfrak{P}_Z$.

So $e'f' = [L : Z_{\mathfrak{P}}] = ef$

Also, $e'e'' = e$, $f'f'' = f$.

Then (2) and (3) follow.

We will now define the inertia group and field, which will stratify the decomposition of a particular prime.

Recall (Finite Fields).

$\mathbb{F}_{p^n}$ is the splitting field for $f(X) = X^{p^n} - X$, and $\mathbb{F}_{p^n}$ is Galois.

The Frobenius automorphism is $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\alpha \mapsto \alpha^p$, which is an automorphism.

Also, $|\sigma| = n$, so it generates the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$.

Subfields of $\mathbb{F}_{p^n}$ are 1:1 with subgroups of $\mathbb{Z}/n\mathbb{Z}$, 1:1 divisors $d \mid n$.

Inertia group.

$$\begin{tikzcd}L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\ K & \mathfrak{p}\end{tikzcd}$$

Define $\kappa(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$

$\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$

By definition, $f(\mathfrak{P}/\mathfrak{p}) = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = \# Gal\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$.

Define a map $(*)$ $G_{\mathfrak{P}} \to Gal\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$ $\quad \sigma \mapsto \bar{\sigma}$

where $\bar{\sigma}(\alpha + \mathfrak{P}) := \sigma(\alpha) + \mathfrak{P}$. (well defined because $\sigma\mathfrak{P} = \mathfrak{P}$).

~~Def~~ The kernel of $(*)$ is the inertia group of $\mathfrak{P}$, $I_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} : \sigma\alpha \equiv \alpha \pmod{\mathfrak{P}} \ \forall \alpha \in \mathcal{O}_L\}$.

The inertia field is the fixed field of $I_{\mathfrak{P}}$, called $T_{\mathfrak{P}}$.

Fact: $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong Gal\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$ (of order $f(\mathfrak{P}/\mathfrak{p})$) by the following:

Prop 5.2: The map $(*)$ is surjective (and so).

Assuming this, then:

Basic facts:

Set $\mathfrak{P}_T := \mathfrak{P} \cap \mathcal{O}_{T_{\mathfrak{P}}}$.

1) $I_{\mathfrak{P}} \triangleleft G_{\mathfrak{P}}$. So $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ is Galois, and $Gal(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong G_{\mathfrak{P}}/I_{\mathfrak{P}}$ of order f

2) $Gal(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$, of order e.

Pf of Prop 5.2.

Let $\bar{\theta}$ be a primitive element for $\kappa(\mathfrak{P})$ over $\kappa(\mathfrak{p})$. Let $\theta \in \mathcal{O}_L$ be any lift of $\bar{\theta}$ in $\mathcal{O}_L$ ($\bar{\theta} \equiv \theta \bmod \mathfrak{P}$).

Let $f(x)$ be the minimal poly. of θ over K. Let $\bar{g}(x)$ the minimal poly of $\bar{\theta}$ over $\kappa(\mathfrak{p})$

As $\bar{f}(\bar{\theta}) = \overline{f(\theta)} = 0$, then $\bar{g}(x) \mid \bar{f}(x)$.

Let $\bar{\sigma} \in Gal\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)$. We know that $\bar{g}(\bar{\sigma}\bar{\theta}) = 0$, so $\bar{f}(\bar{\sigma}\bar{\theta}) = 0$.

$f(x) = \prod(x - \theta_i)$, and so $\bar{\sigma}\bar{\theta} \equiv \theta_i \bmod \mathfrak{P}$ for some i. Let $\sigma : \theta \mapsto \theta_i$, $\sigma \in Gal(L/K)$. This maps to $\bar{\sigma}$, and also fixes $\mathfrak{P}$, so done.

//

$$\begin{tikzcd}[row sep=small]
\mathfrak{P} \arrow[d, dash] & L \arrow[d, dash, "e"] & 1 \arrow[d, dash] \\
\mathfrak{P}_T \arrow[d, dash] & T_{\mathfrak{P}} \arrow[d, dash, "f"] & I_{\mathfrak{P}} \arrow[d, dash] \\
\mathfrak{P}_Z \arrow[d, dash] & Z_{\mathfrak{P}} \arrow[d, dash, "g"] & G_{\mathfrak{P}} \arrow[d, dash] \\
p & K & G
\end{tikzcd}$$

Prop 5.3. with the notation,

a) $e(\mathfrak{P}/\mathfrak{P}_T)=e$

$f(\mathfrak{P}/\mathfrak{P}_T)=1$

b) $e(\mathfrak{P}_T/\mathfrak{P}_Z)=1$

$f(\mathfrak{P}_T/\mathfrak{P}_Z)=f$

Pf/ By comparing degrees, it's enough to prove any of the 4 statements. We'll figure out what is the inertia group of $\mathfrak{P}$ over $\mathfrak{P}_T$.

$$\{\sigma \in Gal(L/T_{\mathfrak{P}}) : \sigma\alpha \equiv \alpha \mod \mathfrak{P} \ \forall \alpha \in \mathcal{O}_L\}$$ //

As $Gal(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$, then $\nearrow \| \ I_{\mathfrak{P}}$. So it is the whole inertia group. This is also $Gal(L/T_{\mathfrak{P}})$. By $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}))$, then the LHS is $\{1\}$, so $\kappa(\mathfrak{P})=\kappa(\mathfrak{P}_T)$.

Hence, $f(\mathfrak{P}/\mathfrak{P}_T)=1$. //

Note: if $\sigma \in G$, then $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$. So $Z_{\sigma\mathfrak{P}} = \sigma(Z_{\mathfrak{P}})$.

Hence, all the decomposition fields are conjugate.

If $G_{\mathfrak{P}} \triangleleft G$, then they are all equal. So they only depend on p. The same argument is true for $I_{\mathfrak{P}}$.

Corollary 5.4 If $G_{\mathfrak{P}} \triangleleft G$, then p splits into g distinct primes in $Z_{\mathfrak{P}}$, each of which stays prime in $I_{\mathfrak{P}}$, and becomes an e^{th}-power in L.

Pf In this case, $Z_{\mathfrak{P}}/K$ is Galois, so as $\mathfrak{P}_Z$ has $e=f=1$, then all the primes of $Z_{\mathfrak{P}}$ over p have ~~equal~~ $e=f=1$. //

Let $L|K$ be a Galois extension, and K' a subextension. Let $\mathfrak{P}$ be a prime of L, and p', p the primes below:

$$\begin{tikzcd}[row sep=small]
L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\
K' \arrow[d, dash] & p' \arrow[d, dash] \\
K & p
\end{tikzcd}$$

Prop 5.5:

1) $Z_\mathfrak{P}$ is the largest K' s.t. $e(p'|p) = f(p'|p) = 1$.

2) $Z_\mathfrak{P}$ is the smallest K' s.t. $\mathfrak{P}$ is the only prime of L above $\mathfrak{p}'$.

3) $T_\mathfrak{P}$ is the largest K' s.t. $e(p'|p) = 1$

4) $T_\mathfrak{P}$ is the smallest K' s.t. $e(\mathfrak{P}|p') = [L:K']$. ($p'$ is totally ramified in L).

Pf/ First note that $Z_\mathfrak{P}$ and $T_\mathfrak{P}$ have the properties claimed.

Let $G' < G$ be the Galois gp of L/K'. Define the groups for G'.

$$\begin{tikzcd}[row sep=small]
L \arrow[d, dash] & 1 \arrow[d, dash] \\
T'_\mathfrak{P} \arrow[d, dash] & I'_\mathfrak{P} \arrow[d, dash] \\
Z'_\mathfrak{P} \arrow[d, dash] & G'_\mathfrak{P} \arrow[d, dash] \\
k'' & G'
\end{tikzcd}$$

It is easy to see that $\begin{cases} G'_\mathfrak{P} = G_\mathfrak{P} \cap G' \\ I'_\mathfrak{P} = I_\mathfrak{P} \cap G' \end{cases}$

By the FTGT, $\begin{cases} Z'_\mathfrak{P} = Z_\mathfrak{P} \cdot K' \\ T'_\mathfrak{P} = T_\mathfrak{P} \cdot K' \end{cases}$

$$\begin{tikzcd}
 & L \arrow[dl, dash, "e"'] \arrow[d, dash, "e'"] \\
T_\mathfrak{P} \arrow[d, dash, "f"'] \arrow[r, dash] & T_\mathfrak{P}K' \arrow[d, dash, "f'"] \\
Z_\mathfrak{P} \arrow[d, dash, "g"'] \arrow[r, dash] & Z_\mathfrak{P}K' \arrow[d, dash, "g'"] \\
K \arrow[r, dash] & K'
\end{tikzcd}$$

1) Spz $e(p'/p) = f(p'/p) = 1$.
Then $e' = e$ and $f' = f$, by looking at the diagram.
This implies that $Z_\mathfrak{P} = Z_\mathfrak{P}K'$, and so $K' \subseteq Z_\mathfrak{P}$.

2) Spz $\mathfrak{P}$ is the only prime of L over $\mathfrak{p}'$.
Then G' acts transitively on the primes over p'. Then $\sigma\mathfrak{P} = \mathfrak{P}$ $\forall \sigma \in G'$. $\Rightarrow G' < G_\mathfrak{P}$. So $Z_\mathfrak{P} \subseteq K'$.

The rest are done similarly.

//

We prove two useful propositions.

<u>Prop 5.6</u>: Suppose L, M are extensions of K. $\longrightarrow$

$$\begin{tikzcd} & LM \arrow[dl, dash] \arrow[dr, dash] & \\ L \arrow[dr, dash] & & M \arrow[dl, dash] \\ & K & \end{tikzcd}$$

a) P is unramified in $LM \Leftrightarrow$ is unramified in L and in M.

b) P splits completely in $LM \Leftrightarrow$ it splits completely in L and in M.

Pf/ (a) Let P' be a prime of LM over P. Let F be the normal closure of LM over K, and let $\mathfrak{P}$ be a prime of F over P'.

If P is unramified ~~over~~ L and M, then $L \cap \mathfrak{P}$ is unramified over P.

So

$$\begin{tikzcd} F \arrow[d, dash] \\ T_{\mathfrak{P}} \arrow[d, dash] \\ Z_{\mathfrak{P}} \arrow[d, dash] \\ K \end{tikzcd}$$

$\Rightarrow$ $L \subseteq T_{\mathfrak{P}}$. Similarly, $M \subseteq T_{\mathfrak{P}}$. So $LM \subseteq T_{\mathfrak{P}}$. $\Downarrow$ ✓.

Hence $LM \cap \mathfrak{P} = P'$ is unramified over P.

(other direction is obvious).

Part (b) is done in the same way.

//

<u>Prop 5.7</u>: L/K a number field extension, M the normal closure of L/K. Let P be a prime of K.

a) P unramified in $L \Leftrightarrow P$ unramified in M.

b) P splits completely in $L \Leftrightarrow P$ splits completely in M.

Pf M is the composite of σL, where σ runs through the embeddings of L. If P is unramified in L, it is unramified in all the σL, so get the result by applying <u>prop 5.6.</u> several times.

//

We'll prove again quadratic reciprocity, in a more conceptual way.

Let p, q be distinct odd primes. When is q a d^{th} power mod p?

We may WLOG assume that $d \mid p-1$.

Consider $\mathbb{Q}(\zeta_p)$. The Gal. group is $G = (\mathbb{Z}/p\mathbb{Z})^*$, cyclic of order $p-1$.

$\forall d \mid p-1$, $\exists!$ subgroup of order $\frac{p-1}{d}$. Call it $G_{\frac{p-1}{d}}$.

The corresponding fixed field is F_d, of degree d over $\mathbb{Q}$.

(the unique subfield of degree d over $\mathbb{Q}$).

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[d, dash] \\
F_d \arrow[d, dash, "d"] \\
\mathbb{Q}
\end{tikzcd}$$

$F_{d_1} \subseteq F_{d_2} \iff d_1 \mid d_2$. (easy!).

Also, $G_{\frac{p-1}{d}} = \{\text{all } d^{th} \text{ powers in } G\}$.

Suppose now that f is the order of q mod p, and $g := \frac{p-1}{f}$.

Then, the decomposition field of q is F_g, fixed by G_f.

Note also that $G_f = \langle \bar{q} \rangle \subseteq (\mathbb{Z}/p\mathbb{Z})^*$.

So q is a d^{th} power mod $p \iff \bar{q} \in G_{\frac{p-1}{d}} \iff G_f \subseteq G_{\frac{p-1}{d}} \iff$

$\iff f \mid \frac{p-1}{d} \iff \frac{p-1}{g} \mid \frac{p-1}{d} \iff d \mid g \iff F_d \subseteq F_g \iff$

$\iff q$ splits completely in F_d (because F_g is the decomp. field).

We've got then:

Prop 5.7: with the previous notation, q is a d^{th} power mod $p \iff q$ splits completely in F_d.

For quadratic reciprocity, we ~~take~~ $d=2$.

<u>QRL</u>: $\left(\frac{q}{p}\right)=1 \iff q$ is a square mod $p \iff q$ splits (completely) in $\overset{\text{quadratic}}{\overset{\downarrow}{F_2}}$

$$\begin{tikzcd} \mathbb{Q}(\zeta_p) \arrow[d, dash] \\ F_2 \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

we've proved in some HW that $F_2 = \mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)$.

So $\left(\frac{q}{p}\right)=1 \iff q$ splits in $\mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)$.

Recall now that, if K is a quadratic field, and Δ_K is its discriminant, then $\left(\frac{\Delta_K}{q}\right)=1 \iff q$ splits in K.

In this case, ~~$\Delta_K =$~~ note that q being odd $\Rightarrow$ only need to consider $\left(\frac{-1}{p}\right)p$ (the 4 factor doesn't matter).

So $\left(\frac{q}{p}\right)=1 \iff \left(\frac{\left(\frac{-1}{p}\right)p}{q}\right)=1 \iff \left(\frac{\left(\frac{-1}{p}\right)}{q}\right)\left(\frac{p}{q}\right)=1$

and just need to note that $\left(\frac{\left(\frac{-1}{p}\right)}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

//

• Class Group and Unit theorem.

The tool we will use to prove the two fundamental theorems is Minkowski's Theory, also called "geometry of numbers": view # in K as points in $\mathbb{R}^n$.

<u>Idea</u>: $\mathbb{Q}(i)=:K \longrightarrow$  $\mathbb{R}^2 \text{ "=" } \mathbb{C}$, and $\mathbb{Z}[i]$ corresponds to the lattice  $\begin{matrix}\mathbb{Z}^2\\ \cap \\ \mathbb{C}\end{matrix}$.

Let V be an n-dimensional inner-product space, with a fixed orthonormal basis, called $\{u_1,\dots,u_n\}$. (think of $V=\mathbb{R}^n$, $\{u_i\}$ the standard basis).

<u>Def</u> A <u>lattice</u> is an additive subgroup of V of the form

$$\Lambda = \mathbb{Z}v_1+\dots+\mathbb{Z}v_r \quad \text{, with } \{v_1,\dots,v_r\} \text{ linearly independent over } \mathbb{R}.$$

We call $\{v_1,\dots,v_r\}$ a <u>basis</u> for Λ.

The lattice Λ is <u>full</u> if $r=n$.

Suppose that Λ is a full lattice. The basis is <u>not</u> unique, but iff then $\{v_1,\dots,v_n\}$, $\{v_1',\dots,v_n'\}$ are bases for Λ. $\Longleftrightarrow$ $\underline{v}=A\underline{v}'$, $A\in GL_n(\mathbb{Z})$.

<u>Def</u>: A fundamental paralelopiped for Λ is a set $T=\{\sum_{i=1}^{n} r_i v_i \, ; \, 0\le r_i<1\}$

Note that T depends on the basis, but by linear algebra,

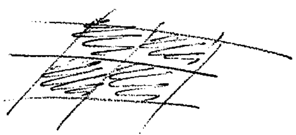
$Vol(T)=|\det(\alpha_{ij})|$, where (α_{ij}) is the matrix of $\underline{v}$ in terms of the given $\underline{u}$.

So $Vol(T)$ does <u>not</u> depend on the chosen basis for the lattice.

Hence, we get the definition of $Vol(\Lambda):=Vol(T)$ for any T.

<u>Lemma 6.1 (12.1 in book)</u>: If Λ is a full lattice in V, and T is a fundamental ppd, then the translates $\lambda+T$, $\lambda\in\Lambda$ are disjoint and cover the whole V.

Pf Look at the book or think.



//

Def A subgroup Λ of V is discrete if ~~Every has no isolated p~~ every $\lambda \in \Lambda$ is isolated. (in the topology induced by the inner product).

Example:

i) $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ is not discrete (see ex. 1 in book).

ii) Any lattice Λ is discrete:

Take a basis for Λ, and extend $v_1, \dots, v_r$ to a basis for V, $\{v_1, \dots, v_r, v_{r+1}, \dots, v_n\}$

If $\gamma = a_1 v_1 + \dots + a_r v_r \in \Lambda$, let $U := \{x_1 v_1 + \dots + x_n v_n \; ; \; |x_i - a_i| < 1 \quad i = 1..r\}$.

Then $U \cap \Lambda = \{\gamma\}$ $\rightsquigarrow$ done.

Theorem 6.2 (12.2 in book): An additive subgroup of V is a lattice iff it's discrete.

Note: Λ is discrete iff any bounded subset of V contains finitely many points of Λ. (easy!)

Minkowski's theorem:

Idea: a set big enough and with enough symmetry has a lattice point.
(in particular, contains a nonzero lattice point).

Def A set $X \subseteq V$ is
- centrally symmetric if $x \in X \Rightarrow -x \in X$.
- convex if whenever $x, y \in X \Rightarrow L(x,y) \subseteq X$ ← line segment ~~x~~

$L(x,y) = \{tx + (1-t)y : 0 \leq t \leq 1\}$.

Thm 6.3 (Minkowski's convex body thm):
If $X \subseteq V$ is convex and centrally symmetric, and $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Lambda)$, then X contains a nonzero lattice point.

↑ should define that... need either countably additive measure, or assume X bounded.

Note: The theorem is sharp: $\Lambda = \mathbb{Z}^n$, $X = (-1,1)^n$. $\mathrm{vol}(X) = 2^n$ and doesn't satisfy conclusion!

↓

Pf (of Minkowski):

Claim: enough to show $\exists \lambda_1 \neq \lambda_2 \in \Lambda$ s.t. $\left(\frac{1}{2}X + \lambda_1\right) \cap \left(\frac{1}{2}X + \lambda_2\right) \neq \emptyset$

Because: if it is nonempty, then $\frac{1}{2}x_1 + \lambda_1 = \frac{1}{2}x_2 + \lambda_2$, $x_i \in X$.
So $\frac{1}{2}(x_1 - x_2) = \lambda_2 - \lambda_1$. $\lambda_2 - \lambda_1 \in \Lambda$, $\lambda_2 - \lambda_1 \neq 0$ and $\frac{1}{2}(x_1 - x_2) \in X$ by symmetry.

If the sets $\{\frac{1}{2}X + \lambda\}$ are pairwise disjoint, let T be the fundamental p-piped. Then the sets $T \cap (\frac{1}{2}X + \lambda)$ are still pairwise disjoint.

$$\text{So } \operatorname{vol} T \geq \sum_{\lambda \in \Lambda} \operatorname{vol}\left(T \cap \tfrac{1}{2}X + \lambda\right) \underset{\substack{\uparrow \\ \text{vol is translation} \\ \text{invariant}}}{=} \sum_{\lambda \in \Lambda} \operatorname{vol}\left((T - \lambda) \cap \tfrac{1}{2}X\right) = \underset{\substack{\| \\ \frac{1}{2^n}\operatorname{vol}(X)}}{\operatorname{vol}\left(\tfrac{1}{2}X\right)}$$

(Since $T - \lambda$ cover V and are pairwise disjoint)

//

Rk: if X is compact, then can weaken "$>$" to "$\geq$".

Pf For $m = 1, 2, 3, \ldots$ look at $(1 + \frac{1}{m})X$. By the theorem, each of them contains a non-zero lattice point, x_m. $\{x_m\}$ is bounded and discrete (because they are lattice points). So there's only finitely many x_m's. So one of them lies in infinitely many of $(1 + \frac{1}{m})X$. $\Rightarrow$ it's in $\overline{X} = X$. //

The next section will relate ideals and lattices.

- Ideals as lattices.

K a number field, $U \subseteq \mathcal{O}_K$ an ideal. Recall that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. In fact, U is also a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n (because it contains a basis for $K/\mathbb{Q}$).

Write $U = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_n$, and $\Delta(U) := \Delta(a_1, \ldots, a_n) = (\det \sigma_i(a_j))^2$.

Also, $\Delta(U) = (\mathcal{O}_K : U)^2 \Delta_K$, and $N(U) := |\mathcal{O}_K/U|$, so $\underline{\underline{\Delta(U) = N(U)^2 \Delta_K}}$. (*)

Fix an embedding $K \hookrightarrow \mathbb{C}$. Let σ be this embedding. It is called real if $\sigma(K) \subseteq \mathbb{R}$, and complex if $\sigma(K) \not\subseteq \mathbb{R}$.

The complex embeddings come in pairs $\sigma, \bar{\sigma}$. So $n = r + 2s$, where $r = \#$ real embeddings, $s = \#$ pairs of complex embeddings; $\sigma_1, \dots, \sigma_r, \tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s$.

Consider a map $V : K \to \mathbb{R}^n$, as $V(x) := (\sigma_1(x), \dots, \sigma_r(x), \mathrm{Re}(\tau_1(x)), \mathrm{Im}(\bar{\tau}_1(x)), \dots \mathrm{Re}(\tau_s(x)), \mathrm{Im}(\tau_s(x)))$

<u>Thm (6.4, bx 13.5)</u>: If $U \subseteq \mathcal{O}_K$ is a nonzero ideal, then $V(U)$ is a full lattice in $\mathbb{R}^n$, with Volume $2^{-s} N(U) \sqrt{|\Delta_K|}$.

Pf Write $U = \mathbb{Z}a_1 \oplus \dots \oplus \mathbb{Z}a_n$. Then $\{V(a_1), \dots, V(a_n)\}$ spans $V(U)$ as a $\mathbb{Z}$-module. Need only to show that they are l.i. over $\mathbb{R}$.

Let $M = \begin{pmatrix} V(a_1) - \\ \text{---} \\ \text{---} \\ - V(a_n) - \end{pmatrix}$, $D = \begin{pmatrix} | & & | & | & | & & | & | \\ \sigma_1(a_i) & \cdots & \sigma_r(a_i), & \tau_1(a_i) & \bar{\tau}_1(a_i) & \cdots & \tau_s(a_i) & \bar{\tau}_s(a_i) \\ | & & | & | & | & & | & | \end{pmatrix}$

It is easy to check that (by column operations) $\det(M) = (-2i)^{-s} \cdot \det(D)$.

$\Delta(U) = \det(D)^2 \, (\neq 0) \Rightarrow \det(M) \neq 0 \Rightarrow \{V(a_i)\}$ are l.i.

Moreover, $\mathrm{vol}(V(U)) = |\det M| = 2^{-s} \cdot \sqrt{|\Delta(U)|} = 2^{-s} N(U) \sqrt{|\Delta_K|}$ //

<u>Thm (6.5, bx 13.6)</u>: If $U \subseteq \mathcal{O}_K$ is a nonzero ideal, then $\exists a \in U, a \neq 0$, s.t. $|N_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s N(U) \sqrt{|\Delta_K|}$.

Pf For $x \in \mathbb{R}^n$, define $N(x) := x_1 \cdots x_r \cdot (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2)$.

Note now that, if $a \in K$, $N_{K/\mathbb{Q}}(a) = N(V(a))$. So the theorem follows from

<u>Claim</u>: if Λ is a full lattice in $\mathbb{R}^n$, then $\exists \lambda \neq 0, \lambda \in \Lambda$ s.t. $|N(\lambda)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \mathrm{vol}(\Lambda)$

This claim will be proven by next theorem.

//

Thm 6.5'': Suppose that Y is a convex, centrally-symmetric, compact set in $\mathbb{R}^n$, with $\mathrm{vol}(Y) > 0$, and with the property $y \in Y \Rightarrow |N(y)| \leq 1$. Then, any full lattice Λ has a non-zero point λ such that $|N(\lambda)| \leq \frac{2^n \mathrm{vol}(\Lambda)}{\mathrm{vol}(Y)}$.

Pf Define t by $t^n := 2^n \mathrm{vol}(\Lambda) / \mathrm{vol}(Y)$. Set $X := t \cdot Y$.

Then $\mathrm{vol}(X) = t^n \mathrm{vol}(Y) = 2^n \mathrm{vol}(\Lambda)$. ($X$ is cpt. centrally-symmetric, convex).

So $\exists \lambda \neq 0, \lambda \in X \cap \Lambda$. Then $\lambda = t \cdot y$, $y \in Y$. And $N(\lambda) = t^n N(y) \leq t^n$.

So by Minkowski, it's done. //

We will find sets Y with the property of 6.5'', and with big volume.

1st try: Y defined by $|x_1| \leq 1, \dots, |x_r| \leq 1$, $y_1^2 + z_1^2 \leq 1, \dots, y_s^2 + z_s^2 \leq 1$.

$\mathrm{Vol}(Y) = 2^r \pi^s$.

Then 6.5' says: $|N(\lambda)| \leq \left(\frac{4}{\pi}\right)^s \mathrm{vol}(\Lambda) \overset{6.5}{\underset{\Downarrow}{=}} |N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \mathcal{N}(\mathfrak{a}) \sqrt{|\Delta_K|}$.

2nd try: define Y_t by $|x_1| + \dots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \dots + 2\sqrt{y_s^2 + z_s^2} \leq t$, and $Y := Y_n$.

Y is compact, centrally symmetric and convex.

Why convex? just check that it is closed under taking midpoints.

Use $|a+b| \leq |a| + |b|$ and $\sqrt{(a+b)^2 + (c+d)^2} \leq \sqrt{a^2+c^2} + \sqrt{b^2+d^2}$.

Claim 1: $y \in Y \Rightarrow |N(y)| \leq 1$.

Pf Consider the arithmetic mean of $|x_1|, \dots, |x_r|, \overbrace{\sqrt{y_1^2+z_1^2}, \sqrt{y_1^2+z_1^2}}^{\text{repeated twice!}}, \dots, \overbrace{\sqrt{y_s^2+z_s^2}, \sqrt{y_s^2+z_s^2}}$.

Its arithmetic mean is ≤ 1, clearly.

Its geometric mean is then ≤ 1. But its geom. mean is $|N(y)|^{1/n} \leq 1$ //.

Claim 2: $\mathrm{vol}(Y) = \frac{n^n}{n!} 2^{r-s} \pi^s$. ($\Longrightarrow$ Theorem 6.5!)

Pf Define $\mathrm{Vol}_{r,s}(t) := \mathrm{Vol}(Y_t)$. Note that $\mathrm{Vol}_{r,s}(t) = t^{r+2s} \mathrm{Vol}_{r,s}(1)$.

$\mathrm{Vol}_{r,s}(1) = 2 \cdot \int_0^1 \mathrm{Vol}_{r-1,s}(1-x)\,dx = 2 \cdot \int_0^1 (1-x)^{r-1+2s} \cdot \mathrm{Vol}_{r-1,s}(1)\,dx = \frac{2}{r+2s} \mathrm{Vol}_{r-1,s}(1)$

So $\mathrm{Vol}_{r,s}(1) = \left(2^r / (r+2s)(r+2s-1)\dots(2s+1)\right) \cdot \mathrm{Vol}_{0,s}(1)$. Do then $V_{0,s}(1) = \iint_{x^2+y^2 = 1/4} \mathrm{Vol}_{0,s-1}(1 - 2\sqrt{x^2+y^2})\,dx\,dy$ //

We are now going to prove some important consequences of the theory of the geometry of numbers.

Recall that $C(K)$ is the class group $= \text{fractional ideals} / \text{principal fractional ideals}$.

Recall that a frac. ideal $\mathfrak{m}$ is $\mathfrak{m} = \alpha I$, $\alpha \in K^*$, I an integral ideal.

Also, $\mathfrak{m} \sim \mathfrak{m}' \Leftrightarrow \mathfrak{m}' = \alpha \mathfrak{m}$, $x \in K^*$.

Note that every class $\mathfrak{C} \in C(K)$ contains an integral ideal.

Fact: Let M be any constant. Then:

"Every integral ideal U contains $a \neq 0$ with $|N_{K/\mathbb{Q}}(a)| \leq M\,\mathcal{N}(U)$" $\Rightarrow$ "Every ideal class contains an integral ideal J with $\mathcal{N}(J) \leq M$"

Corollary 6.6: (Minkowski bound): Every ideal class contains an integral ideal J with

$$\mathcal{N}(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}$$

Pf Thm.

Pf of the fact: Let $\mathfrak{C}$ be an ideal class. Let U be an integral ideal in $\mathfrak{C}^{-1}$. Then $\exists\, a \neq 0$ in U s.t. $|N_{K/\mathbb{Q}}(a)| \leq M \cdot N(U)$.

Note: $(a) \subseteq U \Rightarrow (a) = U \cdot J$ for some integral ideal $J \overset{U\cdot J \text{ is principal!}}{\Rightarrow} J \in \mathfrak{C}$.

Note: $|N_{K/\mathbb{Q}}(a)| = N((a)) = N(U) \cdot N(J) \Rightarrow N(J) \leq M$. //

Corollary 6.7. The class group $C(K)$ is finite.

Pf Show that there are only finitely many integral ideals J with $N(J) \leq M$.

Let $J = \prod P_i^{a_i}$, $a_i \geq 0$. Then $N(J) = \prod N(P_i)^{a_i} \leq M$

we know that $N(\mathbf{P}_i) = p_i^{k_i}$ (power of a prime number). For any $p_i \in \mathbb{Z}$, there are only finitely many $\mathbf{P}_i$. So P_i and a_i are restricted to finite sets $\Rightarrow$ ✓ //

Note: $N(\mathfrak{U})$ is defined for integral ideals, and is multiplicative.

(recall $N(\mathfrak{U}) = |\mathcal{O}_K/\mathfrak{U}|$).

This can be extended multiplicatively to fractional ideals:

$N(\prod \mathfrak{p}_i^{a_i}) := \prod N(\mathfrak{p}_i)^{a_i}$ $(a_i \in \mathbb{Z})$.

(the book Janusz gets the def. wrong in 13.4).

Corollary 6.8. If K is a number field, then $|\Delta_K| \geq 4^{r-1}\pi^{2s}$.

In particular, if $K \neq \mathbb{Q}$, then $|\Delta_K| > 1$. So some primes will ramify.

Pf/ By Minkowski's bound, taking any of the J, as $N(J) \geq 1$, then:

$\sqrt{|\Delta_K|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$. An easy induction argument gives the formula. //

Example 1: $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. $K_1 := \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{-3})$ $\to$ $\Delta_{K_1} = 8$, $\Delta_{K_2} = -3$ $\Rightarrow K_1 \cap K_2 = \mathbb{Q}$.

So $\Delta_K = 8^2 \cdot (-3)^2 = 9 \cdot 64$.

$n = 4$, $r = 0$, $s = 2$. The bound by Minkowski says that every class contains an integer ideal J with norm $\leq \frac{4!}{4^4}\left(\frac{4}{\pi}\right)^2 \sqrt{|\Delta_K|} = \frac{4!}{4^4}\frac{4}{\pi} \cdot 3 \cdot 8 = \frac{36}{\pi^2}$

So every class contains J with norm ≤ 3.

So only $N(J) = 1$ ($\Leftrightarrow J = \mathcal{O}_K$) or $N(J) = 2, 3$, which implies J is a prime ideal over 2 or over 3.

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, no head] \arrow[dr, no head] & \\
\overset{e=2}{\underset{f=g=1}{}}\ \mathbb{Q}(\sqrt{2}) \arrow[dr, no head] & & \mathbb{Q}(\sqrt{-3})\ \overset{e=1}{\underset{g=1,\ f=2}{}} \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Note that 2 is inert in $\mathbb{Q}(\sqrt{-3})$.

So in $\mathcal{O}_K$, $(2)\mathcal{O}_K = J_2^2$, $N(J_2) = 4 \Rightarrow$ nobody.

Similarly with 3.

So we end up getting $C(K) \cong \{1\}$.

Remark: $\mathbb{Q}(\sqrt{-6})$ has class group $\mathbb{Z}/2\mathbb{Z}$, so the class group of a subfield need not be a subgroup of the class group of the big field.

Example 2: $K = \mathbb{Q}(\sqrt{26})$. $n=2$, $r=2$, $s=0$.

$\Delta_K = 4 \cdot 26$, } Minkowski bound gives $\frac{2!}{2^2} \cdot 2\sqrt{26} < 6$

Look then at J with $N(J) \leq 5$.

Primes above 2: 2 ramifies, $2\mathcal{O}_K = J_2^2$, $N(J_2) = 2$.

Primes above 3: $\left(\frac{4 \cdot 26}{3}\right) = \left(\frac{26}{3}\right) = \left(\frac{2}{3}\right) = -1 \Rightarrow 3$ is inert, $N(3\mathcal{O}_K) = 9 > 5$.

Primes above 5: $\left(\frac{26}{5}\right) = \left(\frac{1}{5}\right) = 1 \Rightarrow 5$ splits, $5\mathcal{O}_K = J_5 J_5'$, $N(J_5) = N(J_5') = 5$

Hence $[\mathcal{O}_K], [J_2], [J_2^2], [J_5], [J_5']$ generate $C(K)$.

Note that $[J_2^2] = [\mathcal{O}_K]$ because J_2^2 is principal.

Moreover, $[J_5'] = [J_5]^{-1}$

Is $[J_2] = [\mathcal{O}_K]$? i.e. is J_2 principal ?

If $J_2 = (x + \sqrt{26}\,y)$, $x, y \in \mathbb{Z}$. Then $N(J_2) = 2 = |N_{K/\mathbb{Q}}(x + \sqrt{26}\,y)|$

$\Rightarrow x^2 - 26y^2 = \pm 2 \Rightarrow x^2 \equiv \pm 2 \pmod{13} \Rightarrow \left(\frac{\pm 2}{13}\right) = 1 \Rightarrow !!$

So J_2 is *not* principal.

The same argument $\Rightarrow$ J_5 is not principal.

What is the relation between $[J_2]$ and $[J_5]$?

Look at $\alpha := 6 + \sqrt{26}$ Note that $N_{K/\mathbb{Q}}(\alpha) = 10$. So (α) is not prime

$\Rightarrow (\alpha)\mathcal{O}_K = (\text{ideal of norm } 2) \cdot (\text{ideal of norm } 5)$ (the norm is not a prime power)

Suppose WLOG $(\alpha) = J_2 \cdot J_5$. So $[J_5] = [J_2]^{-1} = [J_2]$.

Also, $[J_5'] = [J_5]^{-1} = [J_2]$. So $C(K) = \mathbb{Z}/2\mathbb{Z}$ //

- Remarks on class numbers.

Let K be a #field, $C(K)$ its class group, and $h_K := \# C(K) < \infty$ be its class number.

Then h_K and $C(K)$ are very unpredictable, and there are lots of open problems.

Open problem: Are there ∞ many K with $h_K = 1$?

Def The Dedekind zeta function $\zeta_K(s) := \sum_{A \subseteq \mathcal{O}_K} N(A)^{-s}$ $(s \in \mathbb{C})$

(note that $\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} n^{-s} = \zeta(s)$, the Riemann-zeta function).

$\zeta_K(s)$ has a meromorphic continuation to $\mathbb{C}$, and has a simple pole at $s=1$.

Analytic class number formula:

$$\operatorname*{Res}_{s=1} \zeta_K(\underset{\substack{\uparrow \\ \text{complex variable}}}{s}) = \frac{2^r (2\pi)^{\overset{\text{\# complex embeddings}}{\overset{\downarrow}{s}}} h_K R_K}{\omega \sqrt{|\Delta_K|}}$$

R_K is the regulator of K (depends on the units in $\mathcal{O}_K$).
ω is the # of roots of 1 in K.

General "phenomenon": "Special values of L-series" (as the zeta function) are related to ~~arithmetic~~ some invariants of arithmetic objects.

Gauss' class number problem

Let $D < 0$ be the discriminant of an imaginary quadratic number field, and write $h(D)$ for the class number of this field.

Gauss observed that $h(D) \longrightarrow \infty$ as $D \to -\infty$.

The GRH (Generalised Riemann Hypothesis) says that all non-trivial zeros of $\zeta_K(s)$ (for K imaginary quadratic) lie on $\mathrm{Re}(s) = 1/2$.

- Hecke (1918): GRH $\Rightarrow \exists\, c > 0$ s.t. $h(D) > c\sqrt{|D|} \log|D|$.
- Mordell (1934): If RH is false, then $h(D) \to \infty$ as $D \to -\infty$.
- Heilbrunn (1934): If GRH is false, then $h(D) \to \infty$ as $D \to -\infty$

$\Rightarrow h(D) \to \infty$ as $D \to -\infty$ (unconditional!)

- Siegel (1935): $\forall\, \varepsilon > 0$, $\exists\, C(\varepsilon) > 0$ s.t. $h(D) > C(\varepsilon)|D|^{1/2 - \varepsilon}$ (also completely ineffective).

Continuing with the history,

- Gross-Zagier-Oesterle-Goldfeld (1976): $h(D) > \frac{1}{55}\log|D| \cdot \prod_{p|D}\left(1-\frac{[2\sqrt{p}]}{p+1}\right)$

  $\forall D$ such that $(D, 5077)=1$.

- Heegner (1952): The only $D<0$ for $h(D)=1$ are $-3,-4,-7,-8,-11,-19,-43-67$

  and -163. (Gauss suspected this). (nobody believed this proof at first)

  In 1967, Baker and Stark proved it independently.

  After this, they noticed that Heegner was right.

- Baker-Stark proved that the last D with $h(D)=2$ is $D=-427$.
- Oesterle, using the G-Z-O-G bound, proved that the last D with $h(D)$ is -907.

  Gauss suspected both of these results.

When $D>0$, nothing is known, but it's conjectured that there exists infinitely many D with $h(D)=1$.

Computations suggest that $\simeq 80\%$ of $D>0$ have $h(D)=1$.

Cohen-Lenstra heuristics give conjectures for divisibility of $h(D)$.

•Dirichlet's Unit Theorem.

Let K be a number field, I_K = fractional ideals (free abelian gen. by prime ideals).
Can define $i : K^* \to I_K$, $i(\alpha) = (\alpha) = \alpha\mathcal{O}_K$. $\ker(i) = U_K$ = set of units in $\mathcal{O}_K$.

Also, $C(K) = I_K / i(K^*)$, hence:

finite group

$$1 \to \underset{\text{what's this?}}{U_K} \xrightarrow{\text{inclusion}} K^* \xrightarrow{i} I_K \longrightarrow C(K) \longrightarrow 1.$$

Basic Fact: $\alpha \in \mathcal{O}_K$. Then $\alpha \in U_K \iff N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Example: K an imaginary quadratic field. Can use the previous fact to prove:

$K = \mathbb{Q}(i) \Rightarrow U_K = \{\pm 1, \pm i\}$ (4^{th} roots of 1).

$K = \mathbb{Q}(\sqrt{-3}) \Rightarrow U_K = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$ (6^{th} roots of 1).

All other K (imag quadratic) $\to U_K = \{\pm 1\}$ (2^{nd} roots of 1)

(proof it as an exercise).

K a real quadratic field:

$K = \mathbb{Q}(\sqrt{2})$ and $u := 1 + \sqrt{2}$, then $(1+\sqrt{2})(1-\sqrt{2}) = -1 \Rightarrow 1+\sqrt{2}$ is a unit.

It turns out that $U_K = \{\pm(1+\sqrt{2})^n\}_{n \in \mathbb{Z}}$.

Thm 6.9 (Dirichlet's Unit Thm).

K a number field, $[K:\mathbb{Q}] = n = r + 2s$ (r the number of real embeddings).
Then, $U_K \cong V \times W$, where
- V = set of roots of 1 in K (finite cyclic group).
- W = free abelian group of rank $r+s-1$.

i.e. $\exists$ units $u_1, \dots, u_{r+s-1}$ s.t. every $u \in U_K$ can be uniquely written as

$$u = w \cdot u_1^{b_1} \cdots u_{r+s-1}^{b_{r+s-1}}, \quad b_i \in \mathbb{Z}, \quad w \text{ a root of } 1.$$

Def: $u_1, \dots, u_{r+s-1}$ is called a fundamental system of units.

Pf (D.U.T.):

Idea of the proof: want to view U_K as a lattice (the free part, at least).

For this, we need to change multiplication to addition.

Use the "log" map. (defined, in fact, over all of K)

Recall the map we had $K^* \longrightarrow \mathbb{R}^{r+2s}$

$$a \longmapsto v(a) = (\sigma_1(a), .., \sigma_r(a), \mathrm{Re}(\tau_1(a)), \mathrm{Im}(\tau_1(a)), .., \mathrm{Re}(\tau_s(a)), \mathrm{I}( ))$$

We follow it with the log map:

$$\log : \mathbb{R}^{r+2s} \longrightarrow \mathbb{R}^{r+s} \text{ as } \log(x_1, .., x_r, y_1, z_1, .., y_s, z_s) = \cancel{\log(|x_1|, .., |x_r|,}$$
$$= (\log|x_1|, \log|x_r|, \log|y_1^2+z_1^2|, .., \log|y_s^2+z_s^2|)$$

This map is not defined on the whole $\mathbb{R}^{r+2s}$, but is indeed defined on the image of v, $v(K^*)$.

Let $\ell := (\log \circ v) : K^* \longrightarrow \mathbb{R}^{r+s}$. Notice that $U \subseteq K^*$.

want that $\ell(U)$ is a lattice..

Facts: 1) $\ell(ab) = \ell(a) + \ell(b)$ (easy)

2) $\ell(U)$ is contained in the hyperplane $H \subseteq \mathbb{R}^{r+s}$, defined by $z_1 + .. + z_{r+s} = 0$

(because $u \in U \Rightarrow N_{K|\mathbb{Q}}(u) = \pm 1$).

3) Any bounded set in $\mathbb{R}^{r+s}$ has a finite inverse image in U.

(because $v(O_K) = \Lambda$, a lattice in $\mathbb{R}^{r+2s}$. $U \hookrightarrow O_K \setminus \{0\} \xrightarrow[\sim]{v} \overset{\overset{\mathbb{R}^{r+2s}}{\cup\!|}}{\Lambda \setminus \{0\}} \xrightarrow{\log} \mathbb{R}^{r+s}$

As the inverse image of log is bounded, can only have finitely many preimages in $\Lambda \setminus \{0\}$, so only some of them in U.)

4) $\mathrm{Ker}(\ell)$ is finite by (3). If $\zeta \in \mathrm{Ker}(\ell)$, then ζ is a root of unity.

Conversely, ζ a root of 1 $\Rightarrow$ all of its conjugates have abs. value 1 $\Rightarrow$ goes to 0.

So $\mathrm{Ker}(\ell) = \{$roots of 1 lying in $K\}$. It's a cyclic group

(recall that any finite subgroup of the multiplicative group of a field K is cyclic!).

$\downarrow$

(cont'd)

<u>More facts:</u>

5) $\ell(U)$ is a lattice in $\mathbb{R}^{r+s}$.

by Thm 6.2

→ abelian sgp of $\mathbb{R}^{r+s}$ ✓.

→ it is discrete, because (3) $\Rightarrow$ bounded set in $\mathbb{R}^{r+s}$ $\Rightarrow$ finitely many elts of $\ell(U)$ in it $\overset{\downarrow}{\Rightarrow}$ ✓.

<u>Note</u>: $\ell(U) \subseteq H$ (hyperplane of dim $r+s-1$). $\Rightarrow$ $\operatorname{rk} \ell(U) \leq r+s-1$.
* want to see equality.

We use the following lemma:

<u>Lemma 6.10</u>: Let $A = (a_{ij}) \in \mathbb{R}^{m \times m}$. Suppose that

1) all row-sums are zero.
2) all $a_{ii} > 0$ $\forall i$
3) all $a_{ij} < 0$ $\forall i$

Then $\operatorname{rk} A = m-1$.

$v_1, \dots, v_m$ the columns of A

Pf/ want to show that the first $m-1$ columns are l.i. (as $\sum \overset{\downarrow}{v_i} = 0 \Rightarrow \operatorname{rk} A \leq m-1$).

Suppose $t_1 v_1 + \dots + t_{m-1} v_{m-1} = 0$ (not all t_i's $= 0$).

Let k be s.t. $|t_k| \geq |t_i|$ $i = 1..m$, and divide through t_k. So can assume $t_k = 1$, and so $|t_j| \leq 1$ $\forall j \neq k$.

Consider the k^{th} row:

$$0 = t_k a_{kk} + \sum_{j \neq k} t_j a_{kj} \geq a_{kk} + \sum_{\substack{j \neq k \\ j \leq m-1}} a_{kj} > a_{kk} + \sum_{\substack{j \neq k \\ j \leq m}} a_{kj} = \sum_{j=1}^{m} a_{kj} = 0 \Rightarrow !!$$

//

Now it's enough to show:

<u>Prop 6.11</u>: Suppose $1 \leq k \leq r+s$. Then, $\exists u \in U_K$ s.t. if $\ell(u) = (z_1, \dots, z_{r+s})$, then $z_i < 0$ $\forall i \neq k$.

<u>Lemma 6.12</u>: Suppose $1 \leq k \leq r+s$. Then, $\forall \alpha \in \mathcal{O}_K$, $\alpha \neq 0$, $\Rightarrow \exists \beta \in \mathcal{O}_K$, $\beta \neq 0$ such that:

- $|N_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}$
- If $\ell(\alpha) = (a_1, \dots, a_{r+s})$ and $\ell(\beta) = (b_1, \dots, b_{r+s})$, then $b_i < a_i$ $\forall i \neq k$.

$\downarrow$

(cont pf of DUT).

Note that the lemma 6.12 implies the prop. 6.11:

Fix K, $1 \le K \le r+s$. Choose $\alpha_1 \in \mathcal{O}_K$, $\alpha_1 \neq 0$.

Apply the lemma repeatedly, and get a sequence

$\alpha_1, \alpha_2, \alpha_3, \ldots$ of nonzero elements in $\mathcal{O}_K$, s.t.

1) $|N_{K/\mathbb{Q}}(\alpha_j)| \le M \quad \forall j$ (some M).

2) the i^{th} coordinate of $\ell(\alpha_{j+1})$ is <u>less than</u> the i^{th} coordinate of $\ell(\alpha_j)$ for $i \neq K$

As $N((\alpha_j)) \le M \ \forall j \Rightarrow \exists h > j$ s.t $(\cancel{\alpha}_h) = (\alpha_j) \Rightarrow \alpha_h = u\alpha_j$ for some unit $u \in U_K$. Then, $\ell(\alpha_h) = \ell(u) + \ell(\alpha_j) \Rightarrow$ proposition. //

So to prove <u>DUT</u> we only need to prove <u>lemma 6.12</u>:

Pf (lemma 6.12)

We'll use Minkowski. Define a set $X \subseteq \mathbb{R}^{r+2s}$ s.t $v(\beta) \in X \Rightarrow |N_{K/\mathbb{Q}}(\beta)| \le \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}$ and guarantee that X contains $v(\beta)$ for some $\beta \neq 0$.

We'll need that X is symmetric, and that $\text{vol}(X) \geq 2^n \text{vol}(\Lambda_K) = 2^n\, 2^{-s}\sqrt{|\Delta_K|} = 2^{r+s}\sqrt{|\Delta_K|}$

Define X by:

$|x_1| \le c_1, \ldots, |x_r| \le c_r, \ (y_1^2+c_1^2) \le c_{r+1}, \ldots, y_s^2 + z_s^2 \le c_{r+s}$ for some c's.

where $c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}$. If such c's exist, then:

$\text{vol}(X) = 2^r \cdot \pi^s \cdot c_1 \cdots c_{r+s} = 2^{r+s}\sqrt{|\Delta_K|}$.

Also, $v(\beta) \in X \Rightarrow |N_{K/\mathbb{Q}}(\beta)| \le c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}$.

We need to choose the c_i's s.t. if $v(\beta) \in X$, then $b_i < a_i \ \forall i \neq K$.

Just need to take $0 < c_i < e^{a_i} \quad \forall i \neq K \quad (\Rightarrow \overset{b_i}{\log c_i} < a_i)$

Choose c_K so that $c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}$, and done. //

Real Quadratic Fields

$K = \mathbb{Q}(\sqrt{d})$, $d>0$, squarefree <u>real</u> quadratic.

By Dirichlet Thm, $U_K = \langle \pm 1 \rangle \times \langle u \rangle$.

<u>Note</u>: u a unit $\Rightarrow$ $u, -u, u^{-1}, -u^{-1}$ are all units. (assume $u \neq \pm 1$). $\Rightarrow$ exactly one of them is > 1.

<u>Def</u> u is a fundamental unit if $U_K = \langle \pm 1 \rangle \times \langle u \rangle$ and $u > 1$.

<u>Want to find u</u>: $N_{K/\mathbb{Q}}(u) = \varepsilon = \pm 1$.

The min. poly for u is $f(X) = X^2 - aX + \varepsilon \Rightarrow u = \dfrac{a \pm \sqrt{a^2-4\varepsilon}}{2}$

To take the ~~positive one~~ greater-than-one, we pick the $\oplus$ sign: $u = \dfrac{a+\sqrt{a^2-4\varepsilon}}{2}$.

Note that $\sqrt{a^2-4\varepsilon} \in \mathbb{Q}(\sqrt{d}) \Rightarrow \sqrt{a^2-4\varepsilon} = m\sqrt{d}$ for some $m \in \mathbb{N}$.

So get that a unit u has the form $u = \dfrac{a+m\sqrt{d}}{2}$ $a, m \in \mathbb{N}$.

We get that $N_{K/\mathbb{Q}}(u) = \dfrac{a^2-m^2d}{4} = \varepsilon (= \pm 1)$. $\Rightarrow (a^2 - m^2 d = \pm 4)(*)$

Let $a>0$ be the <u>least</u> s.t. $(*)$ has a solution. Then $u := \dfrac{a+m\sqrt{d}}{2}$ is the fundamental unit.

<u>Pf of claim</u>:
certainly $u>1$. If it's not fundamental, then $u = u_0^k$ where $u_0 = \dfrac{a_0+m_0\sqrt{d}}{2}$ is a fundamental unit. But then $a > a_0 \Rightarrow !!$.

<u>Example</u>: $\mathbb{Q}(\sqrt{10})$

Solve $a^2 - 10m^2 = \pm 4$ ----> see that the first nontrivial solution is $(a=6, m=2)$

Hence the fundamental unit is $u = \dfrac{6+2\sqrt{10}}{2} = 3+\sqrt{10}$.

<u>Example</u>: $\mathbb{Q}(\sqrt{46})$. The fundamental unit is $24335 + 3588\sqrt{46}$.

$\mathbb{Q}(\sqrt{48})$ ——— — — $7+\sqrt{48}$.

Example (canonical comp. question)

$K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Describe a subgroup of finite index in U_K.

$r = 4, s = 0 \Rightarrow U_K = \langle \pm 1 \rangle \times \mathbb{Z}^3$.

So need to find three multiplicatively independent units u_1, u_2, u_3

(i.e. $u_1^a u_2^b u_3^c = \pm 1 \Rightarrow a = b = c = 0$).

$u_1 = 2 + \sqrt{3}$, $u_2 = 2 + \sqrt{5}$.

For the third one, look at $\mathbb{Q}(\sqrt{15}) \subseteq K$. $\rightarrow u_3 = 4 + \sqrt{15}$.

Are they multiplicatively independent?

If not, get $u_1^a u_2^b = \pm u_3^c \Rightarrow (A + B\sqrt{3})(C + D\sqrt{5}) = \pm(E + F\sqrt{15}) \Rightarrow B = D = 0 \Rightarrow !!$ //

Completions and Valuations

$\mathbb{Q}$. Have usual absolute value, $|\cdot|_\infty$ (∞ thought of a prime)

For p a prime, have the p-adic abs. value, $\frac{a}{b} = p^n \frac{a'}{b'}$ with $p \nmid a'b'$. Then $\left|\frac{a}{b}\right|_p := p^{-n}$.

Def K a field. An absolute value on K, $|\cdot|$, is a map $K \to \mathbb{R}$ s.t.

(a) • $|x| \geq 0$ and $|x| = 0 \Leftrightarrow x = 0$.

(b) • $|xy| = |x||y|$

(c) • $\exists C \geq 1$ s.t. $|x+y| \leq C \cdot \max(|x|, |y|)$. $(\forall x, y \in K)$

Two special cases

→ Triangle Inequality: $|x+y| \leq |x| + |y| \Longrightarrow$ prop.(c) with $C := 2$.

→ Strong Triangle Inequality: $|x+y| \leq \max\{|x|, |y|\}$ $(C = 1)$.

Note: if $|\cdot|$ is an absolute value, then $|\cdot|^a$ is another absolute value. $a \in \mathbb{R}$.

we usually don't consider the trivial absolute value, $|x| = 1$ $\forall x \neq 0$, $|0| = 0$.

Note that, if $a > 0$, then $|x| < 1 \Leftrightarrow |x|^a < 1$.

Def $|*|$ and $|\cdot|_1$ are equivalent if $\left[\, |x| < 1 \Leftrightarrow |x|_1 < 1 \,\right]$.
(define the same topology), and note as $|\cdot| \sim |\cdot|_1$

Prop 7.1: Suppose that $|\cdot| \sim |\cdot|_1$. Then $|\cdot|_1 = |\cdot|^a$ for some $a \in \mathbb{R}_{>0}$.

Pf Assume $|\cdot|$ is not trivial.

Choose $y \in K$ s.t. $|y| > 1$. (take any y with $|y| \neq 1$, and either y or y^{-1} works).

Set $a := \dfrac{\log|y|_1}{\log|y|} > 0$ $\left(|y| > 1 \Leftrightarrow |y|_1 > 1 \right)$.

Choose any $x \in K^*$. Will show that $\dfrac{\log|x|_1}{\log|x|} = a$ (so that $|x|_1 = |x|^a$).

Know that $\exists\, b \in \mathbb{R}$ s.t. $|x| = |y|^b$. Choose a sequence $\left\{ \frac{m_i}{n_i} \right\} \subseteq \mathbb{Q}$ which decrease monotonically to b.

$$|x| = |y|^b < |y|^{\frac{m_i}{n_i}} \overset{\text{properties of } |\cdot|}{\Longleftrightarrow} \left| \frac{x^{n_i}}{y^{m_i}} \right| < 1 \Leftrightarrow \left| \frac{x^{n_i}}{y^{m_i}} \right|_1 < 1 \Leftrightarrow |x|_1 < |y|_1^{\frac{m_i}{n_i}}$$

Hence, $|x|_1 \leq |y_1|^b$ $\left(\frac{m_i}{n_i} \searrow b \right)$.

Do the same with an increasing sequence and get the other inequality. //

Def: Call $|\cdot|$ a valuation if the triangle inequality holds (the usual one).
Call $|\cdot|$ a non-arquimedian valuation if the strong triangle inequality holds.

Remark: If $|\cdot|_1 \sim |\cdot|$ with $|\cdot|$ non-arquimedian, then $|\cdot|_1$ is non-arquimedian.

Def Call $|\cdot|$ arquimedian if it is not non-arquimedian.

Lemma 7.2: If $|\cdot|$ is non-Arquimedian, and $|a| \neq |b|$, then $|a+b| = \max(|a|, |b|)$.

Pf Suppose $|b| < |a|$. $|a| = |a+b-b| \leq \max\{|a+b|, |b|\} = |a+b|$. //

Example: K a number field, and $\varphi : K \hookrightarrow \mathbb{R}$ a real embedding.

Define $|y| := |\varphi(y)|_{\mathbb{R}}$ (check that this satisfies the axioms).

We have $\mathbb{Z} \subseteq K$, and $|n| = |n|_{\mathbb{R}} \Rightarrow |\cdot|$ is arquimedian.

So for any embedding (even $\varphi : K \hookrightarrow \mathbb{C}$) also get an arquimedian absolute value (actually, if $\bar{\varphi}$ is ~~the~~ conjugate of φ, then get the same absolute value).

So get $r+s$ arquimedian absolute values.

It turns out that these are the only ones.

$\mathfrak{P}$-adic valuations

R a Dedekind domain, $K = Q(R)$, $y \in K^*$. Then $yR \overset{\text{unique factorization}}{=} \prod_{\mathfrak{P} \text{ prime}} \mathfrak{P}^{v_{\mathfrak{P}}(y)}$, $v_{\mathfrak{P}}(y) \in \mathbb{Z}$ uniquely determined

Note: $R_{\mathfrak{P}}$ is a DVR, so $yR_{\mathfrak{P}} = \mathfrak{P}^{v_{\mathfrak{P}}(y)}$, i.e. if $\mathfrak{P}R_{\mathfrak{P}} = \pi R_{\mathfrak{P}}$, then $y = u \cdot \pi^{v_{\mathfrak{P}}(y)}$, u a unit of $R_{\mathfrak{P}}$.

Properties:

1) $v_{\mathfrak{P}}(y) \in \mathbb{Z}$
2) $v_{\mathfrak{P}}(xy) = v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(y)$
3) $v_{\mathfrak{P}}(x+y) \geq \min\{v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y)\}$.

Def: If v is a map on K satisfying the previous three properties, v is called an exponential valuation.

Pick c, $0 < c < 1$ and define $|y| := \begin{cases} c^{v(y)} \\ 0 \text{ if } y = 0 \end{cases}$. Then $|\cdot|$ is a non-Arquemedean valuation.

Note that different choices of c give equivalent valuations.

We'll prove that all equivalence classes for the non-Arquimedean valuations in K a number field come from one of these $\mathfrak{P}$-adic valuations.

Valuation Ring

K a field, $|\cdot|$ a non-Arquimedean valuation. Then

Def The valuation ring is $R := \{x \in K : |x| \leq 1\}$. (it is a ring, easy to check).

Define $\mathfrak{P} \subseteq R$ as $\mathfrak{P} := \{x \in K : |x| < 1\}$ ($\mathfrak{P}$ is an ideal of R).

Note: As $|x||x^{-1}| = 1$, for $x \in K^*$ either $x \in R$ or $x^{-1} \in R$.

The units of R are those elements with $|x| = 1$.

Also, $R^\times = R \setminus P$, so P is the unique maximal ideal of R (R is local).

Example: $K = \mathbb{Q}$, p a prime, define for $x \in \mathbb{Q}^*$, $|x|_p := p^{-v_p(x)}$ (i.e. $c := \frac{1}{p}$).

Then $R = \{\frac{a}{b} : p \nmid b\} (= \mathbb{Z}_{(p)})$, $P = pR = \{\frac{a}{b} : p \mid a, p \nmid b\} (= p\mathbb{Z}_{(p)})$

Call $\{|x| : x \in K^*\}$ the value group. It's a multiplicative subgroup of $\mathbb{R}_{>0}$

Def $|\cdot|$ is discrete if the value group is infinite cyclic. (i.e. $\exists\, c < 1$ s.t. $|a|, a \in K^*$ are $\{c^k, k \in \mathbb{Z}\}$)

Lemma 73: $|\cdot|$ is discrete $\Longleftrightarrow$ P is principal (iff R is a DVR).

Pf If P is principal, $P = \pi R$, then R is a UFD, with π the only prime element, so $a \in K^* \Rightarrow a = u \cdot \pi^n$, u a unit of R, $n \in \mathbb{Z}$ So $|a| = |\pi|^n \Rightarrow c = |\pi| \Rightarrow$ ✓.

Conversely, if $|\cdot|$ is discrete, then let $\pi \in R$ s.t $|\pi| < 1$ and maximal with this property.

Then, if $a \in P$, $|a| < 1$ and $|\frac{a}{\pi}| = \frac{|a|}{|\pi|} \leq 1 \Rightarrow \frac{a}{\pi} \in R \Rightarrow a \in \pi R \Rightarrow$ ✓ //

Characterization of Non-Archimedian Valuations

Let K be a field, with identity 1_K.

If $|\cdot|$ is non-Arquimedian, then $|n 1_K| = |1_K + \dots + 1_K| \leq \max\{|1_K|, \dots, |1_K|\} = 1$

Prop: The valuation $|\cdot|$ is non-Arquimedian $\Leftrightarrow$ the values of $|n 1_K|$ are bounded.

Pf in the book //

Valuations on $\mathbb{Q}$

$|\cdot|_\infty$ is a valuation inherited from $\mathbb{R}$. Also, have $|\cdot|_p$ the p-adic valuation for each p, with $|p|_p = \frac{1}{p}$.

Thm (Ostrowski): The non-trivial valuations on $\mathbb{Q}$ are $|\cdot|_\infty^a$, $|\cdot|_p^a$ for some $a > 0$.

· Completions.

Def If $K \hookrightarrow K_0$ is an embedding, an extension of $|\cdot|$ on K is a valuation $|\cdot|_0$ on K_0, which restricts to $|\cdot|$ on K.

Def $\hat{K}$ of K ~~is~~ a ~~completion~~ for K if it's a pair $(\hat{K}, |\cdot|)$ which extends $(K, |\cdot|)$ s.t.

1) $\hat{K}$ is complete.
2) K is dense in $\hat{K}$ (every element of $\hat{K}$ is a limit of elements of K)

Thm 7.6: Let K be a field, with a valuation $|\cdot|$. Then there exists a completion $(\hat{K}, |\cdot|)$, which is unique up to an isomorphism which preserves the absolute value $|\cdot|$.

(For example. $K = \mathbb{Q}(i)$, $\hat{K} = \mathbb{C}$, $\hat{K}_1 = \mathbb{C}$ $\psi : \hat{K} \to \hat{K}_1$ as $\psi(z) = \bar{z}$, corresponding to the two embeddings of K in $\mathbb{C}$).

Pf we construct $\hat{K}$: Let $\mathcal{C} = \{$all Cauchy sequences of elements of $K\}$.

Have an embedding $K \hookrightarrow \mathcal{C}$ by $x \mapsto \{x\}$ ($x_n = x \ \forall n$).

Define $+, \cdot$ componentwise on $\mathcal{C}$. So $\mathcal{C}$ is a commutative ring with identity.

Define $N := \{$Cauchy sequences $\{x_n\} \in \mathcal{C} : \lim x_n = 0\}$ (~~an~~ ideal of $\mathcal{C}$).

We call $\hat{K} := \mathcal{C}/N$.

Note 1: $\{x_n\} \sim \{y_n\} \Leftrightarrow \lim (x_n - y_n) = 0$.

Changing finitely-many terms doesn't affect the class $\{x_n\} + N$.

Note 2: If $\{x_n\} \in \mathcal{C}$, then $\{|x_n|\}$ is a Cauchy sequence in $\mathbb{R}$.

So ~~$|x_n| \to$~~ $\lim |x_n|$ exists.

So define $|\{x_n\}| := \lim |x_n|$. (well defined, and extends the original $|\cdot|$ on K).

$\hat{K}$ is a field: if $\{x_n\} \in \mathcal{C} \setminus N$, then $\lim |x_n| > 0 \Rightarrow x_n \neq 0 \ \forall n >> 1$.

So can invert it.

We just need to prove that it is complete.

↓

(cont pf)

Let $v^{(1)}, v^{(2)}, \ldots$ be a Cauchy sequence of elements in $\hat{K}$.

$v^{(1)}: \quad y_1^{(1)}, y_2^{(1)}, y_3^{(1)}, - - -$

$\vdots$

$v^{(n)}: \quad y_1^{(n)}, y_2^{(n)}, y_3^{(n)}, \ldots, y_k^{(n)}, \ldots$

$\vdots$

$v^{(m)}: \quad y_1^{(m)}, \ldots \ldots, y_k^{(m)}, \ldots$

① Delete finitely-many terms from each $v^{(n)}$ to assure $|y_j^{(n)} - y_k^{(n)}| < \frac{1}{n} \quad \forall j,k$

② Show that $\{y_1^{(n)}\}$ is a Cauchy sequence:

Let $\varepsilon > 0$. Then $|v^{(n)} - v^{(m)}| < \varepsilon \quad \forall\, n,m$ sufficiently large.

i.e. $\lim_{k\to\infty} |v_k^{(n)} - v_k^{(m)}| < \varepsilon$ for n,m suff large.

$\Rightarrow |v_k^{(n)} - v_k^{(m)}| < \varepsilon$ for suff large n,m,k

So $|y_1^{(n)} - y_1^{(m)}| \leq |y_1^{(n)} - y_k^{(n)}| + |y_k^{(n)} + y_k^{(m)}| + |y_k^{(m)} - y_1^{(m)}| < \frac{1}{n} + \varepsilon + \frac{1}{m}$

//

③ Let $Y := \{y_1^{(n)}\}_n$. Show that $v^{(m)} \to Y$:

$|Y - v^{(m)}| = \lim_{k\to\infty} |y_1^{(k)} - y_k^{(m)}|$.

$|y_1^{(k)} - y_k^{(m)}| \leq |y_1^{(k)} - y_1^{(m)}| + |y_1^{(m)} - y_k^{(m)}| < \varepsilon/2 + \varepsilon/2$ for k,m suff large.

//

//

Uniqueness: Follows from the following general fact:

Suppose $(K, |\cdot|)$, $(L, |\cdot|)$ are two fields with valuation (valued fields), and let $\sigma: K \hookrightarrow L$ be an embedding s.t $|\sigma(x)| = |x| \ \forall x \in K$.

Proposition 7.7: With this setup, there exists a unique embedding $\hat{\sigma}: \hat{K} \to \hat{L}$ s.t this commutes:

$$\begin{tikzcd} \hat{K} \arrow[r, hook, "\hat{\sigma}"] & \hat{L} \\ K \arrow[u] \arrow[r, hook, "\sigma"] \arrow[ur, phantom, "\circlearrowleft"] & L \arrow[u] \end{tikzcd}$$

and $|\hat{\sigma}(x)| = |x| \quad \forall x \in \hat{K}$.

d

Pf of prop:

If $x = \{x_n\} \in \hat{K}$, (have to) define $\hat{\sigma} x = \{(\sigma x_n)\}_n \in \hat{L}$

Note that $\{\sigma x_n\}$ is a Cauchy sequence of elements of L, so $\{\sigma x_n\}_n \in \hat{L}$

Easy to check that $\hat{\sigma}$ is an embedding $\hat{K} \hookrightarrow \hat{L}$, and $|\hat{\sigma} x| = |x|$.

To check uniqueness, because $\hat{\sigma}$ is determined over K which is dense in $\hat{K}$, and $\hat{\sigma}$ is continuous $\Rightarrow$ ✓.

Corollary 7.7: The completion $(\hat{K}, |\cdot|)$ is unique, up to a valuation-preserving isom.

Pf/ Suppose $\hat{K}, \hat{K}_1$ are two completions. Apply the proposition:

$$\begin{tikzcd} \hat{K} \arrow[r, "\hat{\sigma}"] & \hat{K}_1 \\ K \arrow[u] \arrow[r, hook, "id"] & K \arrow[u] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \hat{K}_1 \arrow[r, "\hat{\hat{\sigma}}"] & \hat{K} \\ K \arrow[u] \arrow[r, hook, "id"] & K \arrow[u] \end{tikzcd}$$

$\Rightarrow \hat{\sigma}\hat{\hat{\sigma}} = id$, $\hat{\hat{\sigma}}\hat{\sigma} = id$

$\Rightarrow \hat{K}_1 \cong \hat{K}$.

Remark: If $|\cdot|$ is a discrete non-archimedean valuation on K, then $\exists\ \pi \in K$ s.t. $|K^*| = \{|\pi|^m : m \in \mathbb{Z}\}$ (π is called a "uniformizer")

If $\hat{k}$ is its completion and $a \in \hat{K}^*$, then $a = \lim a_n$, $a_n \in K$, and so $0 \neq |a| = \lim |a_n|$.

As $|K^*|$ is discrete, it is closed in $\mathbb{R}_{>0}$. So $|a| \in |K^*|$.

Conclusion: $|\hat{K}^*| = |K^*|$ (we don't get new possible absolute values)

We have a valuation ring as before:

$\hat{R} := \{x \in \hat{K} : |x| \leq 1\}$. , $\hat{P} := \{x \in \hat{K} : |x| < 1\}$.

Note that $\hat{R}$ is the closure of R in $\hat{K}$, and $\hat{P}$ is the closure of P in $\hat{K}$.

and also, note that $\hat{P} = \pi \hat{R}$ by the same argument used to show $P = \pi R$.

Lemma 7.9: $R/\mathfrak{p}^m \cong \hat{R}/\hat{\mathfrak{p}}^m \quad \forall m \geq 0$.

Pf The map $R \to \hat{R}/\hat{\mathfrak{p}}^m$ has kernel $R \cap \hat{\mathfrak{p}}^m = \{x \in R : |x| \leq |\pi|^m\} = \mathfrak{p}^m$.

to show surjectivity, as $\hat{R}$ is the closure of R, then $\forall x \in \hat{R}$, $\exists a \in R$ s.t $|x-a| \leq |\pi|^m$. So $x - a \in \hat{\mathfrak{p}}^m \Rightarrow x \equiv a \mod \hat{\mathfrak{p}}^m$. //

· Representation of elements as power series.

Prop 7.10: Let $\hat{K}$ be the completion of K wrt $|\cdot|$ (discrete, non-archimedean valuation). Let S be a set of coset representatives for $R/\mathfrak{p}$, and let π be a uniformizer.

Then, every $x \in \hat{K}^*$ has a unique representation $x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$ where $a_i \in S$, $a_0 \neq 0$, $m \in \mathbb{Z}$.

Example: $\mathbb{Q}_p$ = completion of $\mathbb{Q}$ wrt $|\cdot|_p$, $\mathbb{Z}_p = \{a_0 + a_1 p + a_2 p^2 + \cdots\}$, where $a_i \in \mathbb{Z}/p\mathbb{Z}$ (for a set of rep's for $\mathbb{Z}/p\mathbb{Z}$).

(Pf of prop):

1) This series converges:

The partial sum is $S_M = \pi^m(a_0 + a_1\pi + \cdots + a_M\pi^M)$

If $N > M$, then $|S_N - S_M| = |\pi^m(a_{M+1}\pi^{M+1} + \cdots + a_N\pi^N)| \leq |\pi|^{m(M+1)} \xrightarrow[M\to\infty]{} 0$.

2) Let $x \in \hat{K}^*$. Then $x = \pi^m \cdot u$, where $u \in \hat{R}^*$ ($|u| = 1$), and m is uniquely determined.

As $\hat{R}/\hat{\mathfrak{p}} \cong R/\mathfrak{p}$, $u \mod \hat{\mathfrak{p}}$ has a unique $a_0 \in S$ s.t $a_0 \equiv u \mod \hat{\mathfrak{p}}$.

So $u - a_0 \in \hat{\mathfrak{p}} = \pi\hat{R}$. So $u - a_0 = \pi b_1$, $b_1 \in \hat{R}$.

Repeat this, to get $a_1 \in S$ $\quad b_1 - a_1 = \pi b_2$, $b_2 \in \hat{R} \Rightarrow u = a_0 + \pi a_1 + \pi^2 b_2$ [illegible]

Iterating, we get a series $a_0 + \pi a_1 + \pi^2 a_2 + \cdots\cdots$, which converges to u.

Prop 7.11 (Weak Hensel's lemma). Let R be a complete ~~valuation~~ DVR.

(i.e. the valuation ring of a complete field, with $|\cdot|$ a discrete non-archimedean valuation).

Suppose $f(X) \in R[X]$, and $a_0 \in R$ is a simple root mod $(\pi) = \mathfrak{p}$

Then, $\exists!\, a \in R$ s.t. $f(a) = 0$, $a \equiv a_0 \mod \mathfrak{p} = (\pi)$.

Example: $R = \mathbb{Z}_5$, $\pi = 5$

$$f(x) = x^2 + 1 \equiv (x+2)(x+3) \mod 5 \quad \text{(two simple roots)}.$$

So $\exists\, a_2, a_3$ roots in $\mathbb{Z}_5$ s.t. $a_2 \equiv 2\ (5)$ $a_3 \equiv 3\ (5)$.

Exercise: Show that in $\mathbb{Z}_p$ there exist, for $i = 1 \ldots p-1$, a $(p-1)^{th}$ root of 1 $\equiv i \pmod p$. ← called the Teichmuller representative of i

The setup is now:

K complete wrt discrete non-archimedean valuation $|\cdot|$.

$R = \text{val. ring} = \{x \in K : |x| \leq 1\}$ a complete DVR,

$R^\times = \{x \in K : |x| = 1\}$, $P = \{x \in K : |x| < 1\}$, $P = \pi R$, π uniformizer.

The elements of $K^\times$ are written as $x = \pi^m \underbrace{(a_0 + a_1\pi + \cdots)}_{\text{unit}}$, $|x| = |\pi|^m$, $a_0 \notin P$.

Pf of 7.11:

Have a_0 a simple root mod π (i.e. $f(a_0) \equiv 0 \pmod \pi$, $f'(a_0) \not\equiv 0 \pmod \pi$).

Let $n = \deg(f)$ and $x_0 \in R$. Then can expand as Taylor:

$$f(x_0 + c) = f(x_0) + cf'(x_0) + \frac{c^2}{2!} f''(x_0) + \cdots + c^n \frac{f^{(n)}(x_0)}{n!}$$

Note that $\dfrac{f^{(k)}(x_0)}{k!} \in R$ $\forall k$, because the $k!$ appears in $f^{(k)}(x_0)$, as well.

Then,
$$f(x_0 + h\pi^n) \equiv f(x_0) + h\pi^n f'(x_0) \pmod{\pi^{2n}}.$$

Suppose given $a_{n-1} \equiv a_0 \pmod \pi$, and $f(a_{n-1}) \equiv 0 \pmod{\pi^n}$. (true for $n=1$).

Write $a_n = a_{n-1} + h\pi^n$, and want to solve

$$f(a_n) = f(a_{n-1} + h\pi^n) \equiv 0 \mod \pi^{n+1}$$

Note that $f(a_{n-1} + h\pi^n) \equiv \overbrace{f(a_{n-1})}^{= \pi^n \cdot A} + h\pi^n f'(a_{n-1}) \mod \pi^{n+1}$ $\quad f'(a_{n-1}) \overset{f'(a_0)}{\equiv} \pmod \pi$

So need that $A + h f'(a_{n-1}) \equiv 0 \pmod \pi$ ⇝ find $\underset{\uparrow \text{unique!}}{h}$ if $f'(a_{n-1})$ is a unit.

Suppose that $f(x) = a_nX^n + \cdots + a_1x + a_0 \in K[X]$, with K complete. (as before).

Recall that, for $a \in K^*$, $a = \pi^m u$ and $v_\pi(a) = m$. (and $v_\pi(0) = \infty$).

Def: $v_\pi(f) := \min_i \{ v_\pi(a_i) \}$

If $v_\pi(f) = m$, then $f = \pi^m(b_nX^n + \cdots + b_0)$. where i) $v_\pi(b_i) \geq 0$ $\forall i$

ii) $v_\pi(b_j) = 0$ for some j.

(i.e. $v_\pi(b_nX^n + \cdots + b_0) = 0$)

(i.e. $b_nX^n + \cdots + b_0 \in R[X]$ but $\notin P[X]$).

Def f is called primitive if any of these conditions holds. (i.e $v_\pi(g) = 0$).

Fact: The product of two primitive polynomials is primitive.

Fact: $v_\pi(f \cdot g) = v_\pi(f) + v_\pi(g)$ (follows from the previous).

Now suppose that $f(x) \in R[x]$ is primitive, and that $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in \overset{!!}{\overset{\downarrow}{K}}[X]$

Then, $v_\pi(f) = 0 = v_\pi(g) + v_\pi(h)$. So if $n := v_\pi(g)$, this says that

$g = \pi^m g_0$, $h = \pi^{-m} h_0$ with g_0, h_0 primitive.

So then $f = g_0 h_0$, is a factorization with $g_0(x), h_0(x) \in R[X]$. So:

Lemma 7.12: If $f(x) \in R[X]$ is reducible over K, then it's reducible over R.

Suppose $f(x) = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ is reducible, and $\pi \nmid a_n$.

Then $f(x) = \overset{g(x)}{(b_rx^r + \cdots + b_0)} \overset{h(x)}{(c_sx^s + \cdots + c_0)}$ and $\pi \nmid b_r$, $\pi \nmid c_s$.

So $\bar{f} = \bar{g} \cdot \bar{h}$ where $\bar{\ }$ means reduced mod π, where $\deg(\bar{g}) = \deg g$, $\deg(\bar{h}) = \deg h$.

Theorem 7.13 (Hensel's Lemma). Let R be a DVR, and $f(x) \in R[X]$ primitive, and $\bar{f}(x) \equiv \bar{g}(x)\bar{h}(x) \pmod{\pi}$, where $\bar{g}, \bar{h}$ are coprime. Then:

There exist $g, h \in R[X]$ s.t. $\deg g = \deg \bar{g}$, $\deg h = \deg \bar{h}$, $g \equiv \bar{g} \pmod{\pi}$, $h \equiv \bar{h} \pmod{\pi}$

and $f(x) = g(x) \cdot h(x)$

Remarks:

→ This implies Weak Hensel.

→ Can loosen the condition of coprimality.

Theorem $\overset{7.17}{}$ (Ostrowski):

If K is a field, complete wrt an archimedean valuation $|\cdot|$, then $K \cong \mathbb{R}$ or $\mathbb{C}$, and the valuation of K is equivalent to the ordinary absolute value on $\mathbb{R}$ or $\mathbb{C}$.

Note: $|\cdot|_{\mathbb{C}}$ on $\mathbb{C}$ is the unique extension of $|\cdot|_{\mathbb{R}}$ on $\mathbb{R}$.

Pf See Janusz, II, ~~§4~~, Marcus II, 4.2 //

Theorem 7.18:

Let K be complete wrt a discrete non-archimedean valuation $|\cdot|_K$. If L/K is any algebraic extension of K, then there is a unique extension $|\cdot|_L$ of $|\cdot|_K$ to L. Moreover, if L/K is finite, $|\alpha|_L = |N_{L/K}(\alpha)|_K^{1/n}$ where $n=[L:K]$.

Remark: an analogous statement is true for $\mathbb{R}$ and $\mathbb{C}$, as $N_{\mathbb{C}/\mathbb{R}}(a+bi)=a^2+b^2$.

Pf First, we prove it for finite extensions:

If L/K is finite, and $R :=$ val. ring (a complete DVR) for $|\cdot|_K$ on K.

Let $S :=$ integral closure of R in L (note that R is Dedekind domain).

$$\begin{tikzcd} L \arrow[r, dash] \arrow[d, dash] & S \arrow[d, dash] \\ K \arrow[r, dash] & R \supseteq P \end{tikzcd}$$

Claim: $S = \{\alpha \in L : N_{L/K}(\alpha) \in R\}$.

Pf $\subseteq$) clear, as $N_{L/K}(\alpha)$ is essentially one of the coeffs on the min. poly of α.

$\supseteq$) Let $N(\alpha) \in R$, and let $f(x) = x^{d} + \dots + a_d$ be the min. poly of α in L/K.

Then $N_{L/K}(\alpha) = \pm a_d^{m}$ where $m = [L:K(\alpha)]$.

Since f is irreducible & monic, and $a_d \in R$ (R is int. closed in K), then by 7.14 $\Rightarrow$ ✓. //

Define $|\cdot|_L$ on L by $|\alpha| = |\alpha|_L := |N_{L/K}(\alpha)|_K^{1/n}$, $n=[L:K]$.

(note that, if $a \in K$, then $|a|_L = |a^n|_K^{1/n} = |a|_K$, so it really extends the valuation).

Also, $|\alpha|_L \leq 1 \Leftrightarrow |N_{L/K}(\alpha)|_K \leq 1 \Leftrightarrow N(\alpha) \in R \Leftrightarrow \alpha \in S$, so S is the val. ring for $|\cdot|_L$.

Let Q be the (unique maximal) of S. So $Q \cap R = P$.

(cont pf)

Claim: If $\beta \in L \setminus S$, then $S[\beta] = L$.

Note that S is a DVR (discrete because $|L^*| \subseteq |K^*|^{1/n}$ and $|K^*|$ is discrete).

Any $\beta \in L \setminus S$ has the form $\beta = \frac{u}{\pi^n}$ $(\pi S = Q)$, $u \in S^*$.

So $\frac{1}{\pi} = (\underbrace{u^{-1}\pi^{n-1}}_{\substack{\rotatebox{-90}{$\in$} \\ S}})\beta \Rightarrow \frac{1}{\pi} \in S[\beta]$. Every nonzero elt of L is $v\pi^m$, $m \in \mathbb{Z}$, $v \in S^*$

so it is in $S[\beta]$

Uniqueness: Spse $|\cdot|'$ is another extension of $|\ |_K$ to L.

Let S' = val ring of $|\cdot|'$.

Claim: $S \subseteq S'$

Pf S' is integrally closed and it contains R, Hence it contains S, the int. closure of R in L.

But if $S' \supsetneq S$, then $S' = L$, so $|\cdot|'$ is the trivial valuation $(|\alpha| = 1\ \forall \alpha \in L^*)$

But $|\cdot|'$ is trivial on K as well $\Rightarrow$!!

Therefore, $S' = S$. Two discrete valuations with the same valuation ring are equivalent $\Rightarrow |\cdot|' \sim |\cdot|_L$ i.e. $|\alpha|' = |\alpha|^b$ for every $\alpha \in L^*$. But if $a \in K$, $|a|' = |a|_K^b \Rightarrow b = 1 \Rightarrow |\cdot|' = |\cdot|_L$

Finally, if L/K is not finite but it is algebraic, define

$$|\alpha|_L := |\alpha|_{K(\alpha)}$$

If $\alpha, \beta \in L$, then
$$\left\{\begin{array}{l} |\alpha|_L = |\alpha|_{K(\alpha)} = |\alpha|_{K(\alpha,\beta)} \\ |\beta|_L = |\beta|_{K(\beta)} = |\beta|_{K(\alpha,\beta)} \end{array}\right. \Rightarrow \checkmark$$

(Note: Clearly, $|\cdot|_L$ is a valuation, as we defined at the beginning: $|\alpha\beta| = |\alpha||\beta|$, and $|\alpha+\beta| \leq \max\{|\alpha|,|\beta|\}$, for if $|\beta| = \max\{|\alpha|,|\beta|\}$, then $|\alpha+\beta| = |\beta||(\frac{\alpha}{\beta}+1)|$, and $|\frac{\alpha}{\beta}| \leq 1$, so $\frac{\alpha}{\beta} \in S$. $\therefore \frac{\alpha}{\beta} + 1 \in S$, so $|\frac{\alpha}{\beta}+1| \leq 1$. Hence, $|\alpha+\beta| \leq |\beta|$.

end of Thm.

Remark: If L/K is not finite, then $|\cdot|_L$ need not be discrete.

Corollary: If L/K is finite, then L is complete wrt $|\cdot|_L$.

Valuation on an algebraic number field K.

$\mathfrak{P}$ a prime of R = ring of integers of K.

There is a discrete non-archimedean valuation $|\cdot|_{\mathfrak{P}}$, ~~[illegible]~~ whose restriction to $\mathbb{Q}$ is $|\cdot|_p$, if $\mathfrak{P}$ is lying over p. ; $|\alpha|_{\mathfrak{P}} = N(\mathfrak{P})^{-v_{\mathfrak{P}}(\alpha)}$

Fact 1: These are – up to equivalence – the only non-archimedean valuations of K.

If $\rho : K \hookrightarrow \mathbb{C}$ is a $\mathbb{Q}$-embedding, then there is an archimedean valuation of K, $|\cdot|_\rho$ by pullback of the usual abs. value of $\mathbb{C}$. ($|\alpha|_\rho = |\rho(\alpha)|_{\mathbb{C}}$).

If c is complex conjugation (i.e. $Gal(\mathbb{C}/\mathbb{R}) = \langle c \rangle$). Then $|\cdot|_{c\circ\rho} = |\cdot|_\rho$.

Fact 2: The archimedean valuations of K are, – up to equivalence – in one-to-one correspondence with $K \hookrightarrow \mathbb{R}$ and the pairs of conjugates of $K \hookrightarrow \mathbb{C}$. (i.e there are $r+s$ non-equivalent valuations).

Def: The non-archimedean valuations are called finite primes (or places) and the archimedean valuations are called infinite primes (or places).

Example: $K = \mathbb{Q}(\alpha)$, $\alpha^3 = 2$. $n = 3$, one real embedding, two complex (one pair).

So get two archimedean valuations. ~~[illegible]~~

$|1+\alpha|_1 = |1+\sqrt[3]{2}|_{\mathbb{R}}$

$|1+\alpha|_2 = \left\|1 + \frac{-1+\sqrt{3}i}{2}\sqrt[3]{2}\right\|^{\text{usual}}$ $\mathbb{C}$!

Let now K be an algebraic number field, and let v be an additive valuation on K. Let K_v be the completion of K wrt v.

Let $\overline{K_v}$ be the alg. closure of K_v.

Then, the valuation v on K_v extends <u>uniquely</u> to a valuation $\bar{v}$ on $\overline{K_v}$

Also, if $\sigma \in Gal(\overline{K_v}/K_v)$, then $\bar{v} \circ \sigma = \bar{v}$.

Let L/K be an extension, Then to any embedding $\tau : L \hookrightarrow \overline{K_v}$, we can associate a valuation $\bar{v} \circ \tau$ on L, extending v.

$$\begin{tikzcd}
& \overline{K_v} \\
& \tau(L)\cdot K_v \arrow[u, dash] \\
L \arrow[ur, "\tau"] & \\
K \arrow[u, "<\infty"] \arrow[r, hook] & K_v \arrow[uu, dash, "<\infty"']
\end{tikzcd}$$

Also, $\tau(L)\cdot K_v$ is the <u>closure</u> of $\tau(L)$ in $\overline{K_v}$

And $\tau(L)\cdot K_v \cong L_{(\bar{v}\circ\tau)}$

We've observed that the valuation $\bar{v} \circ \tau$ is the same if we change τ to $\sigma \circ \tau$, for $\sigma \in Gal(\overline{K_v}/K_v)$.

(conjugate embeddings over K_v give the same valuation on L).

Let $[L:K]=n$, so there are n distinct embeddings of $L \hookrightarrow \overline{K_v}$ fixing K.

~~extending~~ These split up into conjugacy classes over K_v.

If $L = K(\alpha)$, and $Irr(\alpha, K) = f(x) \in K[X]$, then f need not be irred in $K_v[X]$,

so $f(x) = \prod_{i=1}^{g} f_i(x)$, $f_i(x)$ irred. in $K_v[X]$.

Then, K_v-conjugacy classes of embeddings $L \hookrightarrow \overline{K_v}$ are in 1-1 correspondence with the factors $f_i(x)$

Write $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ in $\overline{K_v}[X]$.

(Then, if $\tau_i : \alpha \mapsto \alpha_i$, then $\tau_i(L) . K_v = K_v(\alpha_i)$).

Proposition: Every valuation of L extending v arises in the described way.

Pf/ Let w be any valuation of L extending v of K, and let L_w be the corresponding completion, $L \xhookrightarrow{i} L_w$, and $K \subseteq L$. The closure of K in L_w is complete w.r.t. v, since w extends v.

$$\begin{tikzcd}
L \arrow[r, hook] \arrow[d, dash] & L_w \arrow[d, dash] \\
K \arrow[r, hook] & K_v
\end{tikzcd}$$

L_w is algebraic over K_v, so have

$$\begin{tikzcd}
L_w \arrow[rr, hook, "\rho_w"] & & \overline{K_v} \\
& K_v \arrow[ul, hook] \arrow[ur] &
\end{tikzcd}$$

The composition $L \xhookrightarrow{i} L_w \xhookrightarrow{\rho_w} \overline{K_v}$ is an embedding $\tau = \rho_w \circ i : L \hookrightarrow \overline{K_v}$ and $|\cdot|_{\bar{v}\circ\tau} = |\ |_w$. (ie $\bar{v} \circ \tau = w$).

Fact: Two extensions of v, $\bar{v}\circ\tau$ and $\bar{v}\circ\tau'$ ~~of~~ v to L are the same iff τ' and τ are conjugate over K_v.

Pf

$$\begin{tikzcd}
& \overline{K_v} \arrow[dl, dash] \arrow[dr, dash] & \\
\tau(L)K_v & & \tau'(L)K_v
\end{tikzcd}$$

$\rightsquigarrow$ get an iso $\tau(L)K_v \xrightarrow{\sim} \tau'(L)K_v$ fixing the ground field K.

Final Remarks

$\mathbb{Q}_p$ is much bigger than $\mathbb{Q}$ (for instance, it is uncountable). It also contains lots of number fields (eg $\mathbb{Q}(\zeta_{p-1})$, $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Q}_p^2$ ...).

- Concrete way of visualizing all the previous results

$L = K(\alpha)$, $f(X) \in K[X]$ the min. poly of α.

Factor $f(X) = f_1(X) \cdots f_r(X)$ in $K_v[X]$.

Then there are exactly r different extensions of v to L, one for each of the poly's $f_i(X)$, because : ~~$\forall$~~

$$\begin{aligned} \tau_i : L &\longrightarrow \overline{K_v} \\ \alpha &\longmapsto \alpha_i \end{aligned} \quad \text{for some root } \alpha_i \text{ of } f_i(X).$$

(Different roots of $f_i(X)$ give conjugate embeddings)

So get $w_1, \dots, w_r$ extensions of v, and $|\beta|_{w_i} = |\tau_i(\beta)|_{\overline{v}}$.

Also, τ_i extends to an isomorphism $\tau_i : L_{w_i} \xrightarrow{\sim} K_v(\alpha_i)$.

Examples:

- $K = \mathbb{Q}$, $K_v = \mathbb{Q}_p$. $L = \mathbb{Q}(\zeta_{p-1})$, with min poly $\Phi_{p-1}(X)$.

  In $\mathbb{Q}_p[X]$, $\Phi_{p-1}(X) = \prod_{j=1}^{m} (X - \alpha_j)$, $m = \phi(p-1)$.

  So we get extensions $w_1, \dots, w_m$ of $|\cdot|_p$ to $\mathbb{Q}(\zeta_{p-1})$.

  If $x \in L = \mathbb{Q}(\zeta_{p-1})$, $x = \sum b_n \zeta_{p-1}^n$ $b_n \in \mathbb{Q}$.

  Then, $|x|_{w_i} = |\sum b_n \alpha_i^n|_p$ $(i = 1 \dots m)$

- $L = \mathbb{Q}(\sqrt{5})$. Want to describe its valuations.

  1) The arquimedian valuations $\longleftrightarrow$ embeddings of $L \hookrightarrow \mathbb{C}$ or $\mathbb{R}$

  $$\left\{ \begin{aligned} |a+b\sqrt{5}|_{\infty_1} &= \|a+b\sqrt{5}\|_\infty \\ |a+b\sqrt{5}|_{\infty_2} &= \|a-b\sqrt{5}\|_\infty \end{aligned} \right.$$

  2) The non-arquimedian valuations: extensions of $|\cdot|_p$.

  a) X^2-5 has a root γ in $\mathbb{Q}_p$ (by Hensel, true iff $\left(\frac{5}{p}\right)=1$).

  Get two embeddings of $\mathbb{Q}(\sqrt{5}) \hookrightarrow \overline{\mathbb{Q}_p}$, $\sqrt{5} \longmapsto \pm\gamma$ giving *different* extensions.

  b) X^5-5 is irreducible in $\mathbb{Q}_p$ ($\left(\frac{5}{p}\right) = -1$, or $p = 2, 5$)

  Get two conjugate embeddings of $\mathbb{Q}(\sqrt{5}) \hookrightarrow \overline{\mathbb{Q}_p}$, so we get only one extension:

  $$|a+b\sqrt{5}|_w = |a+b\gamma|_{p_1} = |N_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(a+b\gamma)|_p^{1/2} = \sqrt{|a^2-5b^2|_p}.$$

More Math 530 notes. 5/5/06. Please let me know if you find typos.

4. CYCLOTOMIC FIELDS

References: Washington, Janusz, Neukirch.

Theorem (Kronecker-Weber). *If $K/\mathbb{Q}$ is an abelian extension then K is contained in a cyclotomic field.*

A proof can be found in the exercises of chapter 4 of Marcus.

Let ζ_n be a primitive nth root of 1 and let $\Phi_n(x)$ be the nth cyclotomic polynomial (i.e. the minimal polynomial of ζ_n over $\mathbb{Q}$).

Proposition 4.1. *Let p^a be a prime power and set $K := \mathbb{Q}(\zeta_{p^a})$. Then the prime p is totally ramified in K and*

$$p\mathcal{O}_K = (1-\zeta_{p^a})^{\phi(p^a)}\mathcal{O}_K$$

(where ϕ is the Euler phi function). Here $(1-\zeta_{p^a})$ is a prime ideal of norm p (i.e. of relative degree 1).

Proposition 4.2. *Let $p^a \neq 2$ be a prime power and set $K := \mathbb{Q}(\zeta_{p^a})$. Then*

1. *$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}]$.*
2. *$\Delta_K = \Delta(\zeta_{p^a}) = \pm p^{p^{a-1}(pa-a-1)}$, where the plus sign holds if and only if $p \equiv 1 \pmod 4$ or $p = 2$ and $p^a \geq 8$.*

In section 6 we will prove the following

Theorem 4.3 (Minkowski's theorem). *If $K \neq \mathbb{Q}$ is an algebraic number field then $|\Delta_K| \neq 1$. In particular, some prime $p \in \mathbb{Z}$ ramifies in K.*

Corollary 4.4. *If Δ_L and Δ_K are coprime then $L \bigcap K = \mathbb{Q}$.*

Now write $m = \prod p_i^{a_i}$. Then $\mathbb{Q}(\zeta_m)$ is the compositum of the fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$.

Proposition 4.5. (1) *p ramifies in $\mathbb{Q}(\zeta_m)$ if and only if $p \mid m$.*
(2) *$\mathbb{Z}[\zeta_m]$ is the ring of integers of $\mathbb{Q}(\zeta_m)$.*

Proposition 4.6. *$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \approx (\mathbb{Z}/m\mathbb{Z})^*$, under the isomorphism*

$$a \pmod m \quad \mapsto \quad (\zeta_m \mapsto \zeta_m^a).$$

Lemma 4.7. *If $p \nmid n$ and $\mathfrak{P}$ is a prime of $\mathbb{Q}(\zeta_n)$ over p then the nth roots of unity are distinct modulo $\mathfrak{P}$.*

Theorem 4.8. *If $p \nmid n$ then let f be the multiplicative order of p modulo n. Then p splits into $g = \phi(n)/f$ distinct primes in $\mathbb{Q}(\zeta_n)$, each of relative degree f.*

Finally, we have

Theorem 4.9 (Quadratic reciprocity). *If p and q are distinct odd primes then $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Further, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.*

5. HILBERT'S RAMIFICATION THEORY

References: Neukirch, Marcus.

Suppose that L/K is a Galois extension of number fields, $\mathfrak{P}$ a prime of L, $\mathfrak{p}$ a prime of K whose splitting in L is determined by the invariants e, f, g. Recall that

$$G_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K)\ :\ \sigma\mathfrak{P} = \mathfrak{P}\}$$

and that $Z_{\mathfrak{P}}$ is the fixed field of $G_{\mathfrak{P}}$. Then

$$[L\ :\ Z_{\mathfrak{P}}] = ef = |G_{\mathfrak{P}}|, \quad [Z_{\mathfrak{P}}\ :\ K] = g.$$

Let $\mathfrak{P}_Z$ be the prime of $Z_{\mathfrak{P}}$ below $\mathfrak{P}$.

Proposition 5.1. *With this setup,*

1. *$\mathfrak{P}_Z$ is non-split in L (i.e. $\mathfrak{P}$ is the only prime of L above it).*
2. *$e(\mathfrak{P}|\mathfrak{P}_Z) = e$, $f(\mathfrak{P}|\mathfrak{P}_Z) = f$.*
3. *$e(\mathfrak{P}_Z|\mathfrak{p}) = 1$, $f(\mathfrak{P}_Z|\mathfrak{p}) = 1$.*

Now let $k(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$, $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. These are finite fields, and by definition,

$$[k(\mathfrak{P})\ :\ k(\mathfrak{p})] = f.$$

So $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ is cyclic of order f. We have a natural map

$$\begin{aligned} G_{\mathfrak{P}} &\to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \\ \sigma &\mapsto \overline{\sigma} \end{aligned}$$

where $\overline{\sigma}(\alpha + \mathfrak{P}) := \sigma(\alpha) + \mathfrak{P}$.

The inertia group is the kernel of this map; i.e.

$$I_{\mathfrak{P}} := \{\sigma \in G_{\mathfrak{P}}\ :\ \sigma\alpha \equiv \alpha \pmod{\mathfrak{P}}\ \ \forall\alpha \in \mathcal{O}_L.\}.$$

and the inertia field $T_{\mathfrak{P}}$ is its fixed field.

Proposition 5.2. *The map above is surjective. In other words,*

$$G_{\mathfrak{P}}/I_{\mathfrak{P}} \approx \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

Let $\mathfrak{P}_T$ be the prime of $T_{\mathfrak{P}}$ below $\mathfrak{P}$.

Proposition 5.3. *With this setup,*

1. *$e(\mathfrak{P}|\mathfrak{P}_T) = e$, $f(\mathfrak{P}|\mathfrak{P}_T) = 1$.*
2. *$e(\mathfrak{P}_T|\mathfrak{P}_Z) = 1$, $f(\mathfrak{P}_T|\mathfrak{P}_Z) = f$.*

Corollary 5.4. *If $G_{\mathfrak{P}}$ is normal in* $\mathrm{Gal}(L/K)$ *then $\mathfrak{p}$ splits into g distinct primes in $G_{\mathfrak{P}}$. Each remains prime in $T_{\mathfrak{P}}$ and becomes an eth power in L.*

If K' is an intermediate field of the Galois extension L/K, define $\mathfrak{p}' := \mathfrak{P} \bigcap K$.

Proposition 5.5.
1. *$Z_{\mathfrak{P}}$ is the largest intermediate field K' such that $e(\mathfrak{p}' \mid \mathfrak{p}) = f(\mathfrak{p}' \mid \mathfrak{p}) = 1$.*
2. *$Z_{\mathfrak{P}}$ is the smallest K' such that $\mathfrak{P}$ is the only prime of L over $\mathfrak{p}'$.*
3. *$T_{\mathfrak{P}}$ is the largest K' such that $e(\mathfrak{p}' \mid \mathfrak{p}) = 1$.*
4. *$T_{\mathfrak{P}}$ is the smallest K' such that $e(\mathfrak{P} \mid \mathfrak{p}') = [L\ :\ K']$ (i.e. $\mathfrak{p}'$ is totally ramified in L).*

Corollary 5.6. *If $G_{\mathfrak{P}}$ is normal in* $\mathrm{Gal}(L/K)$ *then $Z_{\mathfrak{P}}$ is the largest subfield of L in which $\mathfrak{p}$ splits completely.*

Proposition 5.7. *Suppose that L and M are extensions of K and that $\mathfrak{p}$ is a prime ideal of K.*

(1) *$\mathfrak{p}$ is unramified in L and in M if and only if it is unramified in LM.*
(2) *$\mathfrak{p}$ is totally split in L and in M if and only if it is totally split in LM.*

Corollary 5.8. *Suppose that L/K is an extension of number fields, that $\mathfrak{p}$ is a prime ideal of K, and that M is the normal closure of L over K.*

(1) *$\mathfrak{p}$ is unramified in L if and only if it is unramified in M.*
(2) *$\mathfrak{p}$ is totally split in L if and only if it is totally split in M.*

The Galois group of $\mathbb{Q}(\zeta_p)$ is cyclic of order $p-1$. For each $d \mid p-1$ there is a unique subgroup of order $(p-1)/d$. Call it $G_{(p-1)/d}$, and let F_d be the fixed field. Let q be another prime. Then

Proposition 5.9. *q is a dth power mod p if and only if q splits completely in F_d.*

This can be used to prove

Theorem 5.10 (Quadratic reciprocity). *If p and q are distinct odd primes, then $(\frac{p}{q}) = (\frac{q}{p})$ unless both p and q are congruent to 3 modulo 4.*

6. CLASS GROUP AND UNIT THEOREM.

Refs: Janusz, Marcus

An additive subgroup Λ of $\mathbb{R}^n$ is a lattice if it has the form

$$\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r,$$

where the v_i are linearly independent over $\mathbb{R}$. It is a full lattice if $r = n$.

Lemma 6.1 (Book 12.1). *If Λ is a full lattice in $\mathbb{R}^n$ and T is the fundamental parallelepiped, then the translates $\lambda + T$ for $\lambda \in \Lambda$ are disjoint and cover $\mathbb{R}^n$.*

Theorem 6.2 (Book 12.2). *An additive subgroup Λ of $\mathbb{R}^n$ is discrete if and only if it's a lattice.*

Theorem 6.3 (Minkowski's lattice point theorem). *Suppose that Λ is a full lattice in $\mathbb{R}^n$ and that X is a centrally symmetric convex subset of $\mathbb{R}^n$. If*

$$\mathrm{Vol}(X) > 2^n \,\mathrm{Vol}(\Lambda)$$

then X contains a non-zero lattice point $\lambda \in \Lambda$. If X is compact, then the $>$ can be weakened to $\geq$.

Suppose that K is a number field of degree $n = r + 2s$, where r is the number of real embeddings. Let the embeddings of K be

$$\sigma_1, \ldots, \sigma_r, \tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s$$

and define the map $v : K \to \mathbb{R}^n$ by

$$v(x) := (\sigma_1 x, \ldots \sigma_r x, \mathrm{Re}(\tau_1(x)), \mathrm{Im}(\tau_1(x)), \ldots, \mathrm{Re}(\tau_s(x)), \mathrm{Im}(\tau_s(x))\,.$$

Theorem 6.4 (Book 13.5). *Suppose that $U \subseteq \mathcal{O}_K$ is a non-zero ideal. Then $v(U)$ is a full lattice in $\mathbb{R}^n$ and*

$$\operatorname{Vol}(v(U)) = 2^{-s}\mathbb{N}(U)\sqrt{|\Delta_K|}.$$

Theorem 6.5 (Book 13.6). *Suppose that $U \subseteq \mathcal{O}_K$ is a non-zero ideal. Then there exists a non-zero element $a \in U$ such that*

$$|\operatorname{N}_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \mathbb{N}(U)\sqrt{|\Delta_K|}.$$

For $x = (x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s) \in \mathbb{R}^n$, we define

$$N(x) := x_1 \dots x_r(y_1^2 + z_1^2)\dots(y_s^2 + z_s^2).$$

The last theorem follows from

Theorem 6.5'. *If $\Lambda \subseteq \mathbb{R}^n$ is a full lattice, then there exists $\lambda \neq 0$ in Λ with*

$$|\operatorname{N}(\lambda)| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \operatorname{Vol}(\Lambda).$$

This in turn follows from

Theorem 6.5". *If $\Lambda \subseteq \mathbb{R}^n$ is a full lattice and Y is a compact centrally symmetric set such that*

$$y \in Y \implies |\operatorname{N}(y)| \leq 1,$$

then there exists $\lambda \neq 0$ in Λ with

$$|\operatorname{N}(\lambda)| \leq \frac{2^n}{\operatorname{Vol}(Y)} \operatorname{Vol}(\Lambda).$$

Corollary 6.6 (Minkowski bound). *If K is a number field of degree $n = r + 2s$, then each ideal class C in the ideal class group $C(K)$ contains an integral ideal J with*

$$\mathbb{N}(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

Corollary 6.7. *The class group $C(K)$ is finite.*

Corollary 6.8. *If $K \neq \mathbb{Q}$ is an algebraic number field then $|\Delta_K| \neq 1$. In particular, some prime $p \in \mathbb{Z}$ ramifies in K.*

If K is a number field, let U_K be the group of units of $\mathcal{O}_K$.

Theorem 6.9 (Dirichlet's unit theorem). *If K is a number field of degree $n = r + 2s$, then*

$$U_K \approx V \times W,$$

where V is the finite cyclic group consisting of all roots of unity in K and W is a free abelian group of rank $r + s - 1$.

To prove this we define $\log : \mathbb{R}^{r+2s} \longrightarrow \mathbb{R}^{r+s}$ by

$$\log(x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s) := (\log|x_1|, \dots \log|x_r|, \log(y_1^2 + z_1^2), \dots, \log(y_s^2 + z_s^2))$$

and let $\ell : K^* \longrightarrow \mathbb{R}^{r+s}$ be the composite $\ell = v \circ \log$. The theorem follows from properties of ℓ together with the next three lemmas.

Lemma 6.10. *Suppose that* $A = (a_{ij}) \in \mathbb{R}^{m\times m}$ *has all diagonal entries positive, all off-diagonal entries negative, and all row-sums equal to zero. Then* $\operatorname{Rank}(A) = m - 1$.

Lemma 6.11. *Suppose that* K *is a number field and that* $1 \leq k \leq r+s$. *Then there exists* $u \in U_K$ *such that if*

$$\ell(u) = (z_1, \ldots, z_{r+s}),$$

then $z_i < 0$ *for all* $i \neq k$.

Note that this implies $z_k > 0$.

Lemma 6.12. *Suppose that* $1 \leq k \leq r+s$. *For each non-zero* $\alpha \in \mathcal{O}_K$ *there exists a non-zero* $\beta \in \mathcal{O}_K$ *such that*

1. $|\,\mathrm{N}_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}$.
2. *If* $\ell(\alpha) = (a_1, \ldots, a_{r+s})$ *and* $\ell(\beta) = (b_1, \ldots, b_{r+s})$, *then* $b_i < a_i$ *for all* $i \neq k$.

Math 530 notes. 4/26/06. Please let me know if you find typos.

7. Section 7. Valuations and Completions.

Definition. If K is a field, then two absolute values $|\cdot|$, $|\cdot|_1$ are equivalent if

$$|x| < 1 \iff |x|_1 < 1.$$

Proposition 7.1. *$|\cdot|$ and $|\cdot|_1$ are equivalent if and only if $|\cdot| = |\cdot|_1^a$ for some $a > 0$.*

Definition. $|\cdot|$ is a valuation if the triangle inequality holds. If the strict triangle inequality holds, then $|\cdot|$ is non-archimedian. Otherwise it is archimedian.

Lemma 7.2. *If $|\cdot|$ is a non-archimedian valuation and $|a| \neq |b|$ then*

$$|a+b| = \max\{|a|, |b|\}.$$

Let K be a field with non-arch. valuation $|\cdot|$. The valuation ring

$$R := \{x \in K \ : \ |x| \leq 1\}$$

has unique maximal ideal

$$P := \{x \in K \ : \ |x| < 1\}$$

and unit group

$$R^* = \{x \in K \ : \ |x| = 1\}.$$

The value group is

$$|K^*| := \{|x| \ : \ x \in K^*\}.$$

The valuation is discrete if the value group is infinite cyclic (i.e. the value group is a discrete subgroup of the positive real numbers).

Lemma 7.3. *$|\cdot|$ is discrete if and only if P is principal (i.e. R is a DVR).*

In this case there is an element $\pi \in R$ such that $|\pi| < 1$ and such that $|\pi|$ generates the value group. Call π a uniformizer for R. (Note: if π has this property, so does $\pi \cdot u$ for any unit u of R.) We have

$$P = \pi R.$$

If $x \in K^*$ then $x = \pi^m \cdot u$ for some unit u of R, and $|x| = |\pi|^m$.

Let 1_K denote the identity element of K.

Proposition 7.4. *$|\cdot|$ is non-archimedian iff the values $|n \cdot 1_K|$ are bounded for $n \in \mathbb{Z}$.*

Let $|\cdot|_\infty$ be the usual absolute value on $\mathbb{Q}$ and for p prime let $|\cdot|_p$ be the p-adic absolute value, normalized so that

$$|p|_p = \frac{1}{p}.$$

Theorem 7.5. *(Ostrowski's theorem). The non-trivial valuations on $\mathbb{Q}$ are of the form $|\cdot|_\infty^a$ and $|\cdot|_p^a$, where a is a positive real number.*

A field K is complete with respect to $|\cdot|$ if every Cauchy sequence of elements of K converges to an element of K. A completion $\hat{K}$ of K consists of a pair $(\hat{K}, |\cdot|)$ extending $(K, |\cdot|)$ such that $\hat{K}$ is complete and such that K is dense in $\hat{K}$ (i.e. every element of $\hat{K}$ is the limit of a sequence of elements of K.)

Theorem 7.6. *If $(K, |\cdot|)$ is a field with valuation, then a completion $(\hat{K}, |\cdot|)$ exists. The completion is unique up to an isomorphism which preserves the valuation.*

The field $\hat{K}$ is constructed as the set of Cauchy sequences of elements of K modulo the maximal idea of sequences which converge to 0.

If $a \in \hat{K}^*$ then $a = \lim a_n$ with $a_n \in K$, and we define

$$|a| := \lim |a_n|.$$

Suppose that the valuation on K is discrete. Then we must have $|a| \in |K^*|$. I.e. passing to the completion does not enlarge the value group.

In the complete field $\hat{K}$ we have the valuation ring

$$\hat{R} := \{x \in \hat{K} \ : \ |x| \leq 1\},$$

which has unique maximal ideal

$$\hat{P} := \{x \in \hat{K} \ : \ |x| < 1\}$$

and unit group

$$\hat{R}^* = \{x \in \hat{K} \ : \ |x| = 1\}.$$

If π is a uniformizer for R then it is also a uniformizer for $\hat{R}$. In other words,

$$P = \pi R, \quad \hat{P} = \pi \hat{R}.$$

there seem to be two missing lemma numbers here..........

Lemma 7.9. *$R/P^m \approx \hat{R}/\hat{P}^m$ for all $m \geq 0$.*

Proposition 7.10. *Suppose that $\hat{K}$ is the completion of K with respect to the discrete non-archimedian valuation $|\cdot|$. Let $R \subseteq K$ be the valuation ring, let P be the maximal ideal, and let π be a uniformizer. Let S be a complete set of representatives for R/P. Then every $x \in \hat{K}^*$ has a unique representation as a power series*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \dots).$$

where $m \in \mathbb{Z}$, $a_i \in S$ for all i, and $a_0 \notin P$.

Let K be complete with respect to the discrete non-archimedian valuation $|\cdot|$ and let R be the valuation ring. (R is called a complete DVR.)

We look at the question of factorization of polynomials in $R[x]$.

Proposition 7.11. *(Weak Hensel's lemma). Suppose that R is a complete DVR and that π is a uniformizer. Suppose that $f(x) \in R[x]$ has a simple root $a_0 \in R$ modulo π (i.e. $f(a_0) \equiv 0 \pmod{\pi}$ but $f'(a_0) \not\equiv 0 \pmod{\pi}$.) Then $f(x)$ has a unique root $a \in R$ with $a \equiv a_0 \pmod{\pi}$.*

Lemma 7.12. *If R is a complete DVR and K the fraction field, and $f(x) \in R[x]$ is reducible over K, then it is reducible over R.*

If $a \in K^*$ then $a = \pi^m u$ for some unit u of R. We define

$$v_\pi(a) := m \quad \text{(by convention } v_\pi(0) := \infty).$$

If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ then define

$$v_\pi(f) := \min\{v_\pi(a_i)\}.$$

One checks that

$$v_\pi(fg) = v_\pi(f) + v_\pi(g).$$

We call f primitive if $v_\pi(f) = 0$. This is equivalent to saying that $f \in R[x]$ and not all coefficients are divisible by π.

Theorem 7.13. *(Hensel's Lemma). Suppose that R is a complete DVR. Suppose that $f(x) \in R[x]$ is primitive and that*

$$\overline{f}(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{\pi}$$

where $\overline{g}$ and $\overline{h}$ are relatively prime modulo π. Then we have

$$f(x) = g(x)h(x),$$

where g, $h \in R[x]$, $\deg(g) = \deg(\overline{g})$, and

$$g \equiv \overline{g} \pmod{\pi}, \quad h \equiv \overline{h} \pmod{\pi}.$$

Proof. Let $d = \deg(f)$ and $m = \deg(\overline{g})$. Then $\deg(\overline{h}) \leq d - m$. Let g_0, $h_0 \in R[x]$ be polynomials such that

$$g_0 \equiv g \pmod{\pi}, \quad h_0 \equiv h \pmod{\pi}, \quad \deg(g_0) = m, \quad \deg(h_0) \leq d - m.$$

Since $(\overline{g}, \overline{h}) = 1$ there are polynomials $a(x)$, $b(x) \in R[x]$ with $ag_0 + bh_0 \equiv 1 \pmod{\pi}$. Therefore we have

$$f - g_0h_0 \in P[x], \quad ag_0 + bh_0 - 1 \in P[x] \quad (\text{where } P = \pi R.) \tag{7.1}$$

Among **all** of the coefficients of these two polynomials, we pick a coefficient τ such that $v_\pi(\tau)$ is minimal. Note that $v_\pi(\tau) \geq 1$. We work $\pmod{\tau}$ for the rest of the proof.

We will construct the polynomials g and h in the following form:

$$g = g_0 + p_1\tau + p_2\tau^2 + \dots, \tag{7.2}$$

$$h = h_0 + q_1\tau + q_2\tau^2 + \dots, \tag{7.3}$$

where p_i, $q_i \in R[x]$, and

$$\deg(p_i) < m, \quad \deg(q_i) \leq d - m.$$

To do this, we construct a sequence of polynomials

$$g_{n-1} = g_0 + p_1\tau + p_2\tau^2 + \dots + p_{n-1}\tau^{n-1}, \tag{7.4}$$

$$h_{n-1} = h_0 + q_1\tau + q_2\tau^2 + \dots + q_{n-1}\tau^{n-1}, \tag{7.5}$$

such that for all n we have

$$f \equiv g_{n-1}h_{n-1} \pmod{\tau^n}. \tag{7.6}$$

Passing to the limit, we will then obtain $f = gh$.

When $n = 1$, we have $f \equiv g_0h_0 \pmod{\tau}$ by the choice of τ. Suppose then that we have successfully constructed g_{n-1}, h_{n-1} for some $n > 1$. We write

$$g_n = g_{n-1} + p_n\tau^n, \quad h_n = h_{n-1} + q_n\tau^n,$$

and attempt to determine p_n, q_n. Substituting, we see that (7.6) reduces to the condition

$$f - g_{n-1}h_{n-1} \equiv \tau^n(g_{n-1}q_n + h_{n-1}p_n) \pmod{\tau^{n+1}}. \tag{7.7}$$

Set

$$f_n := \tau^{-n}(f - g_{n-1}h_{n-1}) \in R[x].$$

Dividing (7.7) by τ^n, our condition reduces to

$$f_n \equiv g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \pmod{\tau}. \tag{7.8}$$

By the definition of τ, we have

$$g_0a + h_0b \equiv 1 \pmod{\tau}.$$

Therefore

$$f_n \equiv g_0af_n + h_0bf_n \pmod{\tau}.$$

We would like to set

$$q_n = af_n, \quad p_n = bf_n,$$

but the degrees may be too large. To address this, we set

$$b(x)f_n(x) = q(x)g_0(x) + p_n(x),$$

where $\deg(p_n) < \deg(g_0) = m$. Note that, since $g_0 \equiv \overline{g} \pmod{\tau}$ and since $\deg(g_0) = \deg(\overline{g})$, it must be the case that the leading coefficient of g_0 is a unit. Therefore we have $q(x) \in R[x]$, and we get the congruence

$$f_n \equiv g_0(af_n + h_0q) + h_0p_n \pmod{\tau}.$$

We now omit from the polynomial $af_n + h_0q$ all of those terms whose coefficients are divisible by τ. This gives a polynomial q_n such that

$$f_n \equiv g_0q_n + h_0p_n \pmod{\tau}.$$

Since $\deg f_n \leq d$, $\deg(g_0) = m$, and $\deg(h_0p_n) < (d-m)+m = d$, we see that $\deg(q_n) \leq d-m$, as desired. □

Lemma 7.14. *Suppose K complete with respect to discrete non-archimedian valuation $|\cdot|$. Suppose that*

$$f(x) = a_nx^n + \cdots + a_1x + a_0 \in K[x]$$

is irreducible, and that $a_na_0 \neq 0$. Then we have

$$v_\pi(f) = \min\{v_\pi(a_n), v_\pi(a_0)\}.$$

In particular, if f is monic and $a_0 \in R$ then we must have $f(x) \in R[x]$.

Proof. After multiplying by a power of π, we may assume without loss of generality that $f(x) \in R[x]$. Let r be the smallest index with $v_\pi(a_r) = 0$. Then

$$f \equiv x^r(a_nx^{n-r} + \cdots + a_{r+1}x + a_r) \pmod{\pi}.$$

If $v_\pi(a_0) > 0$ or $v_\pi(a_n) > 0$ then f would be reducible by Hensel's lemms. □

The following lemmas were not presented in class, but are still handy.

Lemma 7.15. *(Eisenstein criterion) Suppose that R a complete DVR and that*

$$f(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x].$$

Suppose that $v_\pi(a_n) = 0$, that $v_\pi(a_0) = 1$, and that $v_\pi(a_i) \geq 1$ for $i = 1, \ldots, n-1$. Then f is irreducible over K.

Note: To prove this, copy the usual proof in the case when $f \in \mathbb{Z}[x]$.

Lemma 7.16. *(Non-archimedian Newton's method). Suppose that R a complete DVR and that $f(x) \in R[x]$. Suppose that $a_0 \in R$ has*

$$|f(a_0)| < |f'(a_0)|^2.$$

Then f has a unique root $a \in R$ such that

$$|a - a_0| \leq \left| \frac{f(a_0)}{f'(a_0)^2} \right|.$$

Proof. This is essentially Newton's method. Set

$$a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)}.$$

Follow the proof of the weak Hensel's lemma, but be more careful, and show that

1) $|f(a_{n+1})| < |f(a_n)|$ (this shows $f(a_n) \to 0$).
2) $|f'(a_n)| = |f'(a_0)|$ for all n.
3) $\{a_n\}$ is a Cauchy sequence. □

Theorem 7.17 (Ostrowski's Theorem). *If K is complete with respect to an archimedian valuation $|\cdot|$ then K is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ and the valuation on K is equivalent to the usual absolute value.*

Theorem 7.18. *If K is complete with respect to a non-archimedian valuation v and L is an algebraic extension then there is a unique extension w of v to L. If L/K is finite then L is complete with respect to w, and we have*

$$|x|_w = \left(\left|\mathrm{N}_{L/K}(x)\right|_v\right)^{1/[L:K]}.$$

Suppose that L/K is a finite separable extension and that v is a valuation on K. Then v extends uniquely to a valuation $\overline{v}$ of $\overline{K}_v$. Suppose that

$$\tau \ : \ L \to \overline{K}_v$$

is an embedding which fixes K. Then we define a valuation w on L by

$$w = \overline{v} \circ \tau;$$

i.e.

$$|x|_w = |\tau(x)|_{\overline{v}} \text{ for } x \in L.$$

Note that τ is continuous with respect to w, and therefore extends uniquely to an embedding

$$\tau \ : \ L_w \to \overline{K}_v$$

If σ is a an automorphism of $\overline{K}_v$ fixing K_v then $\tau' := \sigma \circ \tau$ gives another K-embedding of L into K_v. We call τ and τ' conjugate over K_v. We then have the

Theorem 7.19 (Extension Theorem). *With notation as above,*

1. *Every extension w of v to L arises as $w = \overline{v} \circ \tau$ for some K-embedding $\tau \ : \ L \to \overline{K}_v$.*
2. *Two such extensions are equal if and only if the corresponding embeddings are conjugate over K_v.*

Concretely, suppose that $L = K(\alpha)$ and that $f(x) \in K[x]$ is the minimal polynomial of α. Suppose that the factorization of $f(x)$ in $K_v[x]$ is given by

$$f(x) = f_1(x) \dots f_r(x).$$

Choosing for each i a root α_i of $f_i(x)$ gives a K-embedding

$$\tau_i \ : \ L \to \overline{K}_v$$

defined by $\tau_i(\alpha) = \alpha_i$. Note that a different choice of α_i gives a conjugate embedding, and hence the same valuation. This gives r extensions $w_1, \dots, w_r$ of v to L given by $w_i = \overline{v} \circ \tau_i$. Note that each τ_i extends to an isomorphism

$$\tau_i \ : \ L_{w_i} \to K_v(\alpha_i)$$

.