Now $N(\mathfrak{p}^\nu) \overset{\text{def}}{=} [\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O}_K:\mathfrak{p}][\mathfrak{p}:\mathfrak{p}^2]\cdots[\mathfrak{p}^{\nu-1}:\mathfrak{p}^\nu]$

so done if we can show $\mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq \mathcal{O}_K/\mathfrak{p} \quad \forall\ i=1,\dots,\nu-1$.

Know $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$, by uniqueness of prime factorization. Take elt $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, consider ideal $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$ then $\mathfrak{p}^{i+1} \subsetneq \mathfrak{b} \subseteq \mathfrak{p}^i$

<u>Claim</u>: $\mathfrak{p}^i = \mathfrak{b}$ <u>pf</u>: else $\mathfrak{b}\mathfrak{p}^{-i}$ is a proper divisor of $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$ and $\mathfrak{p}$ maximal. ↯.

so $a \pmod{\mathfrak{p}^{i+1}}$ is one-dim'l basis for $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ as $\mathcal{O}_K/\mathfrak{p}$ vector space, i.e. $\mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq \mathcal{O}_K/\mathfrak{p}$ as desired.

So absolute norm N is group homomorphism (upon extending definition to fractional ideals)

$$N : J_K \longrightarrow \mathbb{R}_+^\times$$

<u>Thm</u>: $J_K/K^\times$ is finite gp. (Its order is called "class number of K")

<u>pf</u>: Given non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ then $\mathfrak{p} \cap \mathbb{Z} = (p) \leftarrow$ meaning $p\cdot\mathbb{Z}$, p : rational prime

and $\mathcal{O}_K/\mathfrak{p}$ is finite extension of field $\mathbb{Z}/p\mathbb{Z}$ so is a finite field itself, say with p^f elements some f.

i.e. $N(\mathfrak{p}) = p^f$. Moreover the $\mathcal{O}_K$ ideal $p\cdot\mathcal{O}_K = \mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_r^{\nu_r}$ so only finitely many prime ideals can have $\mathfrak{p}\cap\mathbb{Z} = p\cdot\mathbb{Z}$ (which implies $\mathfrak{p} \mid p\cdot\mathcal{O}_K$.)

$\Rightarrow$ Only finitely many prime ideals have absolute norm bounded by fixed constant

$\Rightarrow$ (since if $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ then $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\nu_1} \cdots N(\mathfrak{p}_r)^{\nu_r}$),

there are only finitely many integral ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with absolute norm bounded by fixed constant.

So strategy: show that every ideal class contains a member that is an integral ideal with norm smaller than fixed absolute constant (which we can concoct however we want, from data depending on $\mathcal{O}_K$.)

freedom in ideal class is multiplication by elt. of $K^\times$, quotient of elts in $\mathcal{O}_K$, so need to analyze norms of elements using lattices.

——— recall definition of lattice ———

Lattice arises from embeddings of K into $\mathbb{C}$. $[K:\mathbb{Q}] = n$, nec. separable, then have n embeddings: $\tau_1, \dots, \tau_n$

$$K \longrightarrow \prod_{i=1}^{n} \mathbb{C} \overset{\text{Neukirch}}{=:} K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$$

$$\beta \longmapsto (\tau_1(\beta), \dots, \tau_2(\beta))$$

Overkill, since a complex embedding τ (not in $\mathbb{R}$) comes with conjugate pair $\bar{\tau}$ with $\overline{\tau(\beta)} = \bar{\tau}(\beta)$.

So we can restrict to conjugation invariant pts. of $K_{\mathbb{C}}$, call it $K_{\mathbb{R}}$. ($= K \otimes_{\mathbb{Q}} \mathbb{R}$)

Write $n = r + 2s$ where r: real embeddings
$2s$: cx. embeddings (even since occur in pairs)

$K_{\mathbb{R}} \simeq \mathbb{R}^{r+2s}$ where $\mathbb{R}^{2s} \cong \mathbb{C}^{s}$ records cx. embedding for τ from each pair $\tau, \bar{\tau}$

How to attach measure to $K_{\mathbb{R}}$?

Option 1 : Use isomorphism $K_{\mathbb{R}} \overset{\phi}{\simeq} \mathbb{R}^{r+2s}$, with Lebesgue measure on $\mathbb{R}^{r+2s}$

Option 2 : Use canonical measure on $K_{\mathbb{R}}$ from scalar product ; on ~~meaning~~ $K_{\mathbb{R}}$

In general, given such a fin dim'l $\mathbb{R}$-vector space v.s. V and positive definite bilinear form $\langle\ ,\ \rangle : V \times V \longrightarrow \mathbb{R}$.

then assign cube spanned by orthonormal basis $e_1, \dots, e_n$ volume of 1.

Then parallelepiped P spanned by $v_1, \dots, v_n$ has volume

$$\mathrm{vol}(P) = |\det(A)|$$

where A is change of basis matrix from $e_1, \dots, e_n$ to $v_1, \dots, v_n$

i.e. $v_i = \sum_j a_{ij} e_j$

This can be written without reference to e_i:

$$\mathrm{vol}(P) = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

claim : $\mathrm{vol}_{can.}(X) = \mathrm{vol}_{Leb.}(\phi(X)) \cdot 2^s$ if $\mathrm{vol}_{can.}$ arises from

Inner product : $\langle x, y \rangle = \sum_{\tau} x_{\tau} \bar{y}_{\tau}$ (easy check.)

Neukirch using this canonical measure, so we will do same.

Prop : If $\mathfrak{a} \neq 0$ ideal of $\mathcal{O}_K$, then $\phi(\mathfrak{a})$ is full lattice in $K_{\mathbb{R}} \simeq \mathbb{R}^n$

and $\mathrm{vol}(\phi(\mathfrak{a})) = \sqrt{|d_K|} \cdot N(\mathfrak{a})$.

pf : Given $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ for $\mathfrak{a}$ then $\phi(\alpha_1), \dots, \phi(\alpha_n)$ are gens for lattice $\phi(\mathfrak{a})$. Now if $A = (\tau_i \alpha_j)$ τ_i : embeddings

$$d(\alpha_1, \dots, \alpha_n) = \det(A)^2 = [\mathcal{O}_K : \mathfrak{a}]^2\, d(\mathcal{O}_K) = N(\mathfrak{a})^2 \cdot d_K$$

But $\mathrm{vol}(\phi(\mathfrak{a})) = \mathrm{vol}\left(\begin{array}{c}\text{parallelopiped} \\ \text{spanned by basis}\end{array}\right) = \left|\det(\langle v_i, v_j\rangle)\right|^{1/2}$

And in our case $(\langle \phi(\alpha_i), \phi(\alpha_j)\rangle) = \left(\sum_{k=1}^{n} \tau_k\alpha_i \overline{\tau_k}\alpha_j\right) = A \cdot \overline{A}^T$

so $\mathrm{vol}(\phi(\mathfrak{a})) = \det(A)$ and result follows //

Want to give upper bound on norms of elts. in ideals :

<u>Thm</u> : For any non-zero ideal $\mathfrak{a}$, choose pos. real #'s c_τ for each real / cx. embeds ~~()~~

with $c_{\bar{\tau}} = c_\tau$ for cx. pairs., such that

$$\prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \cdot N(\mathfrak{a}) \qquad (*)$$

Then $\exists\ a \in \mathfrak{a}, \neq 0$, s.t. $|\tau(a)| < c_\tau \quad \forall\ \tau \in \mathrm{Hom}(K, \mathbb{C})$

<u>Pf</u> : $\phi(\mathfrak{a})$ is lattice. Show set $X = \{ (z_\tau)_\tau \in K_\mathbb{R} \mid |z_\tau| < c_\tau \}$

contains a lattice pt. $\mathrm{vol}(X) = 2^{r+s}\pi^s \prod_\tau c_\tau$ (real abs. values intervals $2 \cdot c_\tau$. cx. abs. value are circles $\pi \cdot c_\tau^2$)

so $\mathrm{vol}(X) > \underbrace{2^{r+2s} \cdot \sqrt{|d_K|}\, N(\mathfrak{a})}_{\displaystyle \underset{\displaystyle 2^n \cdot \mathrm{vol}(\phi(\mathfrak{a}))}{\shortparallel}}$

Now classical fact <u>of Minkowski</u> : if X "nice" and vol satisfies this bound then it contains lattice point

"nice" means : centrally symmetric, convex subset

if $x \in X$, $-x \in X$ ($X \subseteq$ real vector space so $-x$ makes sense)

lines between any two points in X remain in X.

(Thm. 4.4 in Neukirch)

Clearly our set X above satisfies these properties, so we're done. //

Thm. 4.4 is corollary to result that, given any measurable set S in Euclidean space, if $\mu(S) > \mathrm{vol}(\Gamma)$ then $\exists\, x, y \in S$ s.t. $x - y \in \Gamma$.

To show Thm 4.4 apply result to $S = \frac{1}{2}X$ (scale all distances by $1/2$) so that $x - y \in X$ if $x, y \in S$. Note: $\mu(S) = 2^{-n}\mu(X)$.

Corollary: For every ideal $\mathfrak{a} \neq 0$ in $\mathcal{O}_K$, $\exists\, a \neq 0 \in \mathfrak{a}$ s.t.

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{a})$$

pf: choose c_τ with $c_\tau = c_{\bar{\tau}}$ and $\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{a}) + \varepsilon$ for any $\varepsilon > 0$. Apply previous result. Since true for all ε, and $|N_{K/\mathbb{Q}}(a)|$ is positive integer, then we obtain desired inequality $\leq$.

To finish finiteness of class gp, recall we wanted to show each class in $J_K/K^\times$ contains an integral ideal with abs. norm $\leq$ some fixed const. (depending on K, but not on $\mathfrak{a}$)

Given fractional ideal $\mathfrak{a}$, find "denominator" γ so that $\mathfrak{b} = \gamma \cdot \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$.

$$\left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} = C_K$$

Now $\exists\ \beta \in \mathfrak{b}, \neq 0$ with $|N_{K/\mathbb{Q}}(\beta)| \leq C_K \cdot N(\mathfrak{b})$ (by corollary)

i.e. $N((\beta)\mathfrak{b}^{-1}) = N \cdot (\beta \cdot \mathfrak{b}^{-1}) \leq C_K$

and $\beta \cdot \mathfrak{b}^{-1} = \beta/\gamma \cdot \mathfrak{a} \in [\mathfrak{a}]$ in $J_K/K^\times$.