Any element of $Cl(K)$ is represented by an ideal $\mathfrak{a} \subset \mathcal{O}_K$ with

$$\mathrm{Norm}(\mathfrak{a}) \leq C_{r_1, r_2} \cdot |d_K|^{\frac{1}{2}}$$

If we choose the subsets S explicitly, then we can find the constants C_{r_1, r_2}

<u>Minkowski's bound</u> (without proof):

Choose

$$S = \left\{ x \in \mathbb{R}^{r_1 + 2r_2} \,\middle|\, \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} \left(x_{r_1+2j}^2 + x_{r_1+2j-1}^2 \right)^{\frac{1}{2}} < 1 \right\}$$

then compute $\mathrm{Vol}(S)$, M, and deduce

$$C_{r_1, r_2} = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}, \quad n = r_1 + 2r_2$$

<u>Cor. 1</u> $\forall$ element of $Cl(K)$ is represented by an ideal of $\mathrm{Norm} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \cdot |d_K|^{\frac{1}{2}}$

(This is called Minkowski's bound)

<u>Cor. 2</u> $\forall$ number field $K \neq \mathbb{Q}$

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

<u>Proof</u> $1 \in Cl(K)$ is repr. by some ideal $\mathfrak{a}$

$$1 \le \underset{\underset{\mathbb{Z}}{\cap}}{\mathrm{Norm}(\alpha)} \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d_K|^{\frac{1}{2}}$$

$$\Rightarrow |d_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}$$

$$\left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2} \underset{2r_2 \le n}{\geq} \underbrace{\left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2}}_{\alpha_n}$$

$$\alpha_2 = \left(\frac{\pi}{4}\right)^2 \cdot \frac{16}{4} > \frac{9}{\cancel{16}} \cdot \frac{\cancel{16}}{4} > 1$$

$$\frac{\alpha_{n+1}}{\alpha_n} = \frac{\pi}{4} \cdot \frac{(n+1)^{2n+2}}{n^{2n}} \frac{(n!)^2}{((n+1)!)^2} =$$

$$= \frac{\pi}{4} \frac{(n+1)^{2n}}{n^{2n}} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} > \frac{3}{4} \cdot \left(1+\frac{1}{2}\right)^4 = \frac{3^5}{2^6} > 1$$

since $\left(1+\frac{1}{x}\right)^{2x}$ is monotone increasing for $x>1$ $\square$

$$\alpha_{n+1} > \alpha_n > \dots > \alpha_2 > 1$$

How to find all ideals with bounded norm? Enough to consider prime ideals

$(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ prime ideal $\mathfrak{p} \cap \mathbb{Z} = (p)$

$\mathbb{F}_p = \mathbb{Z}/(p) \longrightarrow \mathcal{O}_K/\mathfrak{p}$, $\mathrm{Norm}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p^f$

for some $f \geq 1$.

$p \le p^f \le$ Minkowski's constant

$\Rightarrow$ we only need to consider ideals $\mathfrak{p}$, s.t. $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p bounded

Consider $(p) = \prod \mathfrak{p}_i$ for all prime numbers $p \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d_K|^{\frac{1}{2}}$, then $[\mathfrak{p}_i]$ appearing in all these decompositions generate $Cl(K)$

<u>Examples</u> Quadratic fields. Let $d \in \mathbb{Z}$ square-free, $K = \mathbb{Q}(\sqrt{d})$. Then

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

(see solutions to exercise sheet 3)

$d_K - ?$ $\quad \mathcal{O}_K = \langle 1, \alpha \rangle$

$d \equiv 2,3 \pmod 4 \Rightarrow B = \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}$, $d_K = (\det B)^2 = 4d$

$d \equiv 1 \pmod 4 \Rightarrow B = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}$, $d_K = d$

<u>Case 1</u> $d > 0 \Rightarrow \exists\ 2$ real embedding $K \hookrightarrow \mathbb{C}$

$r_1 = 2$, $r_2 = 0$

Minkowski's bound:

$$p \leq \frac{1}{2} |d_K|^{\frac{1}{2}} = \begin{cases} \sqrt{d}, & d \equiv 2,3 \pmod 4 \\ \frac{1}{2}\sqrt{d}, & d \equiv 1 \pmod 4 \end{cases}$$

E.g. $d=2,3,5,13$ there are no primes p, that satisfy the bound $\Rightarrow Cl(K)=1$ and $\mathcal{O}_K$ is PID

Case 2 $d<0 \Rightarrow \exists$ one pair of complex-conj. embeddings, $r_1=0$, $r_2=1$

$$p \leq \frac{4}{\pi}\frac{1}{2}\cdot |d_K|^{\frac{1}{2}} = \begin{cases} \frac{4}{\pi}\sqrt{|d|}, & d\equiv 2,3 \pmod 4 \\ \frac{2}{\pi}\sqrt{|d|}, & d\equiv 1 \pmod 4 \end{cases}$$

E.g. for $d=-1,-2,-3,-7$ no primes p.

$\Rightarrow \mathcal{O}_K$ is PID

Consider $d=-14$, $K=\mathbb{Q}(\sqrt{-14})$, $d\equiv 2 \pmod 4$

$\mathcal{O}_K=\mathbb{Z}[\sqrt{-14}]$, $d_K=-56$

We need to consider $p\leq \frac{4}{\pi}\sqrt{14}<5$,

i.e. $p=2,3$

How to factorize $(p)=\prod \mathfrak{p}_i^{n_i}$ in $\mathcal{O}_K$?

By CRT: $\mathcal{O}_K/(p) \simeq \prod \mathcal{O}_K/\mathfrak{p}_i^{n_i}$

Every $\mathcal{O}_K/\mathfrak{p}_i^{n_i}$ is a local ring (i.e. it has unique max. ideal) with the maximal ideal $\mathfrak{m}_i=\mathfrak{p}_i/\mathfrak{p}_i^{n_i}$, and

$\mathfrak{p}_i$ is the preimage of $\mathfrak{m}_i$ under the projection $\mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}_i^{n_i}$

We need to find all factors of $\mathcal{O}_K/(p)$ and their maximal ideals.

We are in the following setting

$\mathcal{O}_K = \mathbb{Z}[\alpha]$, α has monic min. poly $f \in \mathbb{Z}[x]$

$$\mathcal{O}_K \simeq \frac{\mathbb{Z}[x]}{(f)}$$

$$\mathcal{O}_K/(p) \simeq \frac{\mathbb{Z}[x]}{(p, f)} \simeq \frac{\mathbb{F}_p[x]}{(f)}$$

Decompose f in $\mathbb{F}_p[x]$:

$f \equiv \prod f_i^{k_i} \pmod{p}$ for some $f_i \in \mathbb{Z}[x]$ that are irreducible in $\mathbb{F}_p[x]$, pairwise coprime

Then by CRT

$$\mathcal{O}_K/(p) \simeq \prod \frac{\mathbb{F}_p[x]}{(f_i^{k_i})}$$

The factors are $\frac{\mathbb{F}_p[x]}{(f_i^{k_i})}$ with $\mathfrak{m}_i = (f_i)$

$$\Rightarrow \mathfrak{p}_i = \ker\Big(\underset{\underset{\mathbb{Z}[x]/(f)}{\text{\rotatebox{90}{$\cong$}}}}{\mathcal{O}_K} \longrightarrow \frac{\mathbb{F}_p[x]}{(f_i)} \Big)$$

$$= (p, f_i(\alpha))$$

How to find the exponents n_i?

$R = \mathcal{O}_K / \mathfrak{p}_i^{n_i}$ n_i is uniquely determined by the following property:

$$n_i = \min\{ n \geq 1 \mid m_i^n = 0 \}$$

$$\Rightarrow n_i = \min\{ n \geq 1 \mid f_i^n = 0 \text{ in } \frac{\mathbb{F}_p[x]}{(f_i^{k_i})} \} = k_i$$

<u>In our example:</u> $f = X^2 + 14$

$p = 2$ $f \equiv X^2 \pmod 2$ $f_1 = X$, $k_1 = n_1 = 2$

$(2) = (2, \sqrt{-14})^2$ $\mathfrak{p}_1 = (2, \sqrt{-14})$

$p = 3$ $f \equiv X^2 - 1 \pmod 3$

$f_2 = X - 1$ $f_3 = X + 1$

$\mathfrak{p}_2 = (3, \sqrt{-14} - 1)$ $\mathfrak{p}_3 = (3, \sqrt{-14} + 1)$

$(3) = (3, \sqrt{-14} - 1) \cdot (3, \sqrt{-14} + 1)$

$[\mathfrak{p}_1], [\mathfrak{p}_2], [\mathfrak{p}_3]$ generate $Cl(K)$

$[\mathfrak{p}_1]^2 = 1$,

Note: $\mathfrak{p}_1$ is not principal

if $\mathfrak{p}_1 = (a + b\sqrt{-14})$, then

$N_{K/\mathbb{Q}}(2) = 4$ is divisible by $a^2 + 14b^2$

$\Rightarrow b = 0$, $\underbrace{a = \pm 1 \text{ or } \pm 2}$

$\Downarrow$

either $\mathfrak{p}_1 = (1)$, or $\mathfrak{p}_1 = (2)$

which is not true

$\Rightarrow \mathfrak{p}_1$ is not principal $\Rightarrow [\mathfrak{p}_1] \neq 1$

$[\mathfrak{p}_2] \cdot [\mathfrak{p}_3] = 1$

More relations: one can compute (exercise):

$\mathfrak{p}_1 \cdot \mathfrak{p}_2^2 = (2 + \sqrt{-14})$

$\Rightarrow [\mathfrak{p}_1] \cdot [\mathfrak{p}_2]^2 = 1 \Longrightarrow [\mathfrak{p}_2]^2 = [\mathfrak{p}_1]$

$[\mathfrak{p}_3] = [\mathfrak{p}_1] \cdot [\mathfrak{p}_2]^2 \cdot [\mathfrak{p}_3] = [\mathfrak{p}_1] \cdot [\mathfrak{p}_2] = [\mathfrak{p}_2]^3$

$\Rightarrow Cl(K)$ is generated by $[\mathfrak{p}_2]$

$\cong \mathbb{Z}/4\mathbb{Z}$