(1) Do the Student evaluation Survey

(2) Sheet 6 Common problems:

**Exercise 6.2.** Let $K = \mathbb{Q}(\sqrt{13})$, $\alpha = \frac{3+\sqrt{13}}{2}$ and $\beta = 23382 + 6485\sqrt{13}$. Show that there exist $n, m \in \mathbb{Z}\backslash\{0\}$ such that $\alpha^n = \beta^m$, without computing $n, m$.

The key to this is to note that $\alpha, \beta$ are in $\mathcal{O}_K$ and have norm 1 therefore they are in $\mathcal{O}_K^\times$.

Must not forget to check they are actually alg. integers. Just because they have norm 1 doesn't mean that they are in $\mathcal{O}_K^\times$.

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$$

eg $\gamma = \frac{29}{3} + \frac{8}{3}\sqrt{13}$ has norm 1.

**Exercise* 6.10.** Let $K$ be a number field containing a non-real root of unity. Show that for all $\alpha \in K\backslash\{0\}$, $N_{K/\mathbb{Q}}(\alpha) > 0$.

Issue: Just because $K$ contains a root of unity doesn't mean its a cyclotomic field.

$K \supseteq \mathbb{Q}(\zeta_n)$.

Today: We will look at class groups and Diophantine equations.

First: look at the LMFDB: Use it to make your own examples!

Example: $K = \mathbb{Q}(\sqrt{-13})$ Want to compute its class group and then use this to find all solutions to $x^3 = y^2 + 13$.

Class group: Recall that

$$Cl_K = \frac{\{\text{group of all fractional ideals}\}}{\{\text{subgroup of all principal fractional ideals}\}}$$

The key to computing these is the following:

**Theorem 4.0.3.** *Let $K$ be a number field with $r_1$ real embeddings and $r_2$ conjugate pairs of complex embeddings. Let $[K : \mathbb{Q}] = n$ and let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Then there is an element $a \in \mathfrak{a}$ such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta(\mathcal{O}_K)|^{1/2} N(\mathfrak{a})$$

**Definition 4.0.4.** The quantity $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta(\mathcal{O}_K)|^{1/2}$ is known as the Minkowski bound and we will denote it by $M_K$.

Now, we have:

**Proposition 4.0.5.** *Let $K$ be a number field and let $C$ be an ideal class in $\mathrm{Cl}_K$. Then $C$ contains an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that*

$$N(\mathfrak{a}) \leq M_K.$$

Which means that if we want to compute $Cl_K$
we can start by computing all ideals of norm
less than $M_K$.

<u>Step: Find $M_K$</u> : $K = \mathbb{Q}(\sqrt{-13})$

- $n = 2$
- $r_2 = 1$ $\qquad r_1 = 0$

- what is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$ by Theorem 2.1.11
$-13 \equiv 3 \mod 4$

$\Delta(\mathcal{O}_K) = -4 \cdot 13$.

So $M_K = \frac{2!}{2^2} \cdot \left(\frac{4}{\pi}\right)^1 \cdot |-4 \cdot 13|^{\frac{1}{2}} \approx 4.59$

From this, we deduce that we only need to find all
ideals of norm $\leq 4$.

To do this we find all prime numbers less than 4
and factor the ideals they generate in $\mathcal{O}_K$.
(Why is this enough?)

- $(2) = (2, 1+\sqrt{-13})^2 = P_2^2$ $\qquad \boxed{\text{Theorem 3.5.7}}$

- $(3) = (3)$ inert i.e. $(3)$ is a prime ideal in $\mathcal{O}_K$

What are the ideals of norm $\leq 4$?

- $(1)$ has norm 1
- $P_2$ has norm 2 $\quad P_2 = (2, 1+\sqrt{-13})$
- $(3)$ has norm $3^2$
- $P_2^2$ has norm 4

Note that $(3)$ is principal
$P_2^2 = (2)$ is also principal
So in $Cl_K$ they both reduce to the trivial element

i.e $[P_2]^2 = [P_2^2] = [1]$ and $[(3)] = [1]$.

So have at most 2 elements in our class group $[1], [P_2]$ but we need to check if $[P_2] = [1]$ ie if $P_2$ is principal.

if it was principal say $P_2 = (\alpha)$ then we would have

$$2 = N(P_2) = |N_{K/\mathbb{Q}}(\alpha)| \quad \Rightarrow \quad N_{K/\mathbb{Q}}(\alpha) = \pm 2$$

i.e $\alpha = a + b\sqrt{-13}$ we would have $a^2 - 13b^2 = \pm 2$ $a, b \in \mathbb{Z}$. But this can't happen. So $P_2$ is not principal therefore

$[P_2] \neq [1]$.

We have $Cl_K = \{[1], [P_2]\} \cong C_2$

Lets use this to find all solutions to $x^3 = y^2 + 13$.
$(x, y) \in \mathbb{Z}^2$

First we observe the following: if $x, y$ is a solution

then • $x, y$ must be coprime (Consider $x^3 - y^2 = 13$)

• $x$ must be odd (Consider $x^3 = y^2 + 13 \mod 8$)

The Key idea to solving this is to look at this as an equality of ideals in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$

$$(x)^3 = (y + \sqrt{-13})(y - \sqrt{-13})$$

We next want to check that $(y + \sqrt{-13})$ and $(y - \sqrt{-13})$ are coprime.

Assume $\mathfrak{p}$ divided them both with $\mathfrak{p}$ a prime ideal
then $\mathfrak{p} \mid (y + \sqrt{-13})$ and $\mathfrak{p} \mid (y - \sqrt{-13})$
and also $\mathfrak{p} \mid (x)$

Note $2y \in (y + \sqrt{-13}) + (y - \sqrt{-13})$
$\Rightarrow (2y) \subseteq (\quad) + (\quad)$

$\Rightarrow (2y) \subseteq \mathfrak{p} \Rightarrow \mathfrak{p} \mid (2y)$

---

So $\mathfrak{p} \mid (x)$ and $\mathfrak{p} \mid (2y)$
Now, since $x$ is odd $\mathfrak{p} \nmid (2)$ (Convince yourself of this)

So $\mathfrak{P} \mid (x)$ and $\mathfrak{P} \mid (y)$

but as $x, y$ are coprime $(x)+(y)=(1)$

so $\mathfrak{P} \mid (1)$ $\times$.

Therefore since $(x)^3 = (y+\sqrt{-13})(y-\sqrt{-13})$

we have ideals $\mathfrak{a}, \mathfrak{b}$ s.t

$$\mathfrak{a}^3 = (y+\sqrt{-13}) \qquad \mathfrak{b}^3 = (y-\sqrt{-13})$$

[by lemma 5.0.2]

So in the $Cl_K$ this says

$$[\mathfrak{a}]^3 = [1] \qquad \text{and} \qquad [\mathfrak{b}]^3 = [1]$$

but $|Cl_K| = 2 \Rightarrow [\mathfrak{a}] = [1] \quad [\mathfrak{b}] = [1]$

Write $(a+b\sqrt{-13}) = \mathfrak{a}$

We have $(a+b\sqrt{-13})^3 = (y+\sqrt{-13})$ as ideals

$\Rightarrow$ as elements we have

$$u \cdot (a+b\sqrt{-13})^3 = (y+\sqrt{-13}) \qquad u \in \mathcal{O}_K^\times \cong \{\pm 1\}$$

Expand out and compare coefficients

and you get $a = \pm 2 \quad b = -1$

$\Rightarrow y = \pm 70 \quad x = 17.$