ZAHLENTHEORIE NOTE 12

• NUMERICAL/ABSOLUTE NORM

K = number field, $\mathcal{O}_K$ = ring of integers

$I \subseteq \mathcal{O}_K$ nonzero ideal. We observe that the ring $\mathcal{O}_K/I$ is finite. Indeed, since $\mathcal{O}_K$ is a finite extension of $\mathbb{Z}$, $\mathcal{O}_K/I$ is a finite extension of $\mathbb{Z}/I\cap\mathbb{Z}$. Furthermore, $I \cap \mathbb{Z} \neq (0)$ (why?), hence $\mathbb{Z}/I\cap\mathbb{Z}$ is a finite ring, and $\mathcal{O}_K/I$ is a finite ring as well.

def: NUMERICAL/ABSOLUTE NORM
K = number field, $I \subseteq \mathcal{O}_K$ nonzero ideal.
The numerical/absolute norm of I is defined as

$$\|I\| \overset{\text{def}}{:=} \left|\mathcal{O}_K/I\right|.$$

Rmk: (1) $\|I\| = 1 \iff I = \mathcal{O}_K$.
(2) If $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, then $\|(d)\| = |d|$.

Prop: K = number field, $I \subseteq \mathcal{O}_K$ nonzero ideal. Then

$$N_{K/\mathbb{Q}}(I) = \left(\|I\|\right)$$

In particular, if $I, J \subseteq \mathcal{O}_K$ are two nonzero

ideals, then

$$\|I \cdot J\| = \|I\| \cdot \|J\|.$$

proof: write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then

$$\|I\| = \left| \mathcal{O}_k / \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \right| = \left| \mathcal{O}_k / \mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_k / \mathfrak{p}_r^{e_r} \right| = \prod \|\mathfrak{p}_i^{e_i}\|$$

$$N_{K/\mathbb{Q}}(I) = \prod N_{K/\mathbb{Q}}(\mathfrak{p}_i^{e_i})$$

Hence, we can suppose that $I = \mathfrak{p}^e$ is the power of a nonzero prime. Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$, and let $f = f_{\mathfrak{p}}(p)$. Then

$$N_{K/\mathbb{Q}}(\mathfrak{p}^e) = N_{K/\mathbb{Q}}(\mathfrak{p})^e = p^{e \cdot f}$$

We need to prove that $\left| \mathcal{O}_k / \mathfrak{p}^e \right| = p^{ef}$. However we have seen two lectures ago that

$$\dim_{\mathbb{F}_p} \mathcal{O}_k / \mathfrak{p}^e = e \cdot f$$

hence

$$\left| \mathcal{O}_k / \mathfrak{p}^e \right| = \left| \mathbb{F}_p^{ef} \right| = p^{ef}. \qquad \square$$

Cor: If $\|I\|$ is prime, then I is prime.

Moreover we can also consider the situation where $I \subseteq J$ are two fractional ideals for $\mathcal{O}_K$. Then there is a $d \in \mathcal{O}_K$ s.t. $dJ \subseteq \mathcal{O}_K$ (hence $IJ \subseteq \mathcal{O}_K$). Then we get that

$dI \subseteq \mathcal{O}_K$ as well). Then we see that

$$J/I \cong dJ/dI \cong \frac{(\mathcal{O}_K/dI)}{(\mathcal{O}_K/dJ)} \text{ is finite}$$

Moreover $IJ^{-1} \subseteq \mathcal{O}_K$ is a nonzero ideal in $\mathcal{O}_K$.

Lemma: In the previous situation

$$\|IJ^{-1}\| = |J/I|$$

proof: we have

$$|J/I| = \left|\frac{\mathcal{O}_K/dI}{\mathcal{O}_K/dJ}\right| = \frac{\|dI\|}{\|dJ\|}.$$

Moreover we see that

$$IJ^{-1} \cdot (dJ) = (dI)(dJ)^{-1} \cdot (dJ) = dI$$

so

$$\|dI\| = \|IJ^{-1} \cdot dJ\| = \|IJ^{-1}\| \cdot \|dJ\|$$

and we are done. □

An useful property of the numerical norm is the following:

Lemma: Let $M > 0$ be a positive integer. Then the set

$$\{I \subseteq \mathcal{O}_K \text{ nonzero ideal} \mid \|I\| \leq M\}$$

is finite.

proof: suppose $\|I\| \leq M$ and write

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$

If we can show that there are only finitely many possibilities for the $\mathfrak{p}_i$ and the e_i, we are done. Suppose $\mathfrak{p}_i \cap \mathbb{Z} = (p_i)$, with $p_i > 0$ positive primes. Let also $f_i = f_{\mathfrak{p}_i}(p_i)$. Then

$$\|I\| = \|\mathfrak{p}_1\|^{e_1} \cdots \|\mathfrak{p}_r\|^{e_r} = p_1^{e_1 f_1} \cdots p_r^{e_r f_r}$$

Since this is bounded by M, there are only finitely many possibilities for the p_i, hence also for the $\mathfrak{p}_i$: they must be one of the finitely many primes in $\mathcal{O}_K$ lying over the finitely many p_i in $\mathbb{Z}$.

Moreover, since $\|I\| = \|\mathfrak{p}_1\|^{e_1} \cdots \|\mathfrak{p}_r\|^{e_r}$, there are only finitely many possibilities for the exponents e_i. □

Example: (1) Let us take $K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We want to find all the ideals I s.t. $\|I\| \leq 2$:

- $\|I\| = 1$: $I = \mathcal{O}_K$.
- $\|I\| = 2$: since 2 is prime, I must be a prime ideal. Moreover, if $I \cap \mathbb{Z} = (p)$

$$\|I\| = p^{f_I(p)}$$

hence $p = 2$, so that I lies over 2.

However $2\mathcal{O}_K = (2, 1+\sqrt{-5})^2$, where

$(2, 1+\sqrt{-5})$ is prime, and
$\|2\cdot\mathcal{O}_k\| = 2^{[k:\mathbb{Q}]} = 4$, so that
$\|(2, 1+\sqrt{-5})\| = 2$.
Hence, the only ideal with $\|I\| = 2$ is
$I = (2, 1+\sqrt{-5})$.

- MINKOWSKI'S BOUND and FINITENESS of the CLASS GROUP

Now we want to prove that the ideal class group $Cl(k) := Cl(\mathcal{O}_k)$ of a number field is finite, and we want to give an effective bound on its size. The key result is the following:

Thm: MINKOWSKI'S BOUND
Let K be a number field of degree $[k:\mathbb{Q}] = n$ and discriminant Δ_k. Let also
$2s = |\{\sigma : K \hookrightarrow \mathbb{C} \mid \sigma \text{ not real } (\sigma(K) \not\subseteq \mathbb{R})\}|$
Then there are representatives for the ideal class group of K given by ideals $I \subseteq \mathcal{O}_k$ s.t.

$$\|I\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\Delta_k|^{1/2}$$

Let's first check that we understand the statement: the only thing to remark is on the number of non-real embeddings. Suppose $K = \mathbb{Q}(\alpha)$, where α has minimal polynomial $m_\alpha(X)$. The embeddings $\sigma : K \hookrightarrow \mathbb{C}$ correspond to the roots of $m_\alpha(X)$: since $m_\alpha(X)$ has rational coefficients, if it has a root $z \in \mathbb{C}$, then it also has the conjugate root $\bar{z}$. Hence

$$\left\{ \begin{array}{c} \text{non-real roots} \\ \text{of } m_\alpha(X) \end{array} \right\} \text{ is even.}$$

Let's list some consequences of Minkowski's bound:

Thm: K = number field. The ideal class group $Cl(K)$ is finite.

proof: Minkowski's bound gives representatives I for the ideal class group s.t. $\|I\| \leq B_K$. and we proved before that the set of ideals $\{ I \mid \|I\| \leq B_K \}$ is finite. ☐

def: IDEAL CLASS NUMBER
K = number field. The ideal class number is defined as

$$h_K = |Cl(K)|$$

Example: (1) $h_K = 1 \iff Cl(K) = 0$

$\iff \mathcal{O}_K$ is an UFD.

Minkowski's bound can be also used to compute h_K:

(2) $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$.

Minkowski's bound gives a set of representatives for $Cl(K)$ s.t.

$$\|I\| \leq \frac{2}{4}\left(\frac{4}{\pi}\right)\sqrt{4} = \frac{4}{\pi} < 2$$

hence $\|I\| = 1$. However the only ideal with norm 1 is $I = \mathcal{O}_K$. Hence $Cl(K)$ has one element and it must be that

$$Cl(K) = 0.$$

Of course, we know this already, but this works also for other number fields.

(3) $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

We know that $\mathcal{O}_K$ is not an UFD so that $h_K > 1$.

Moreover, Minkowski's bound says that there is a set of representatives for $Cl(K)$ s.t.

$$\|I\| \leq 2 \quad \text{(do the explicit computation of the bound}$$

We have seen already that

$$\{ I \mid \|I\| \leq 2 \} = \{ \mathcal{O}_k, (1+\sqrt{-5}, 2) \}$$

hence $h_k \leq 2$. So, it must so that

$$Cl(k) = \mathbb{Z}/2\mathbb{Z}$$

generated by one non-principal ideal. In the set of representatives $\{ \mathcal{O}_k, (1+\sqrt{-5}, 2) \}$, the first ideal is principal, so $(1+\sqrt{-5}, 2)$ must be not principal.

Another consequence of Minkowski's bound is the following:

Thm: There is no nontrivial unramified finite extension of $\mathbb{Q}$.

proof: Suppose K is an unramified extension of $\mathbb{Q}$ s.t. $n = [K:\mathbb{Q}]$, $n \geq 2$.

Then this means that no prime $p \in \mathbb{Z}$ ramifies in K, equivalently, no prime p divides the discriminant Δ_K, so that $\Delta_K = \pm 1$.

To prove that this is impossible, consider Minkowski's bound: the class group $Cl(K)$ has at least one element, hence we can find an ideal $I \subseteq \mathcal{O}_K$ s.t.

$$\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|} \geq \|I\| \geq 1$$

hence

$$\sqrt{|\Delta_K|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s$$

$$\sqrt{|\Delta_k|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)$$

Moreover, if n is the degree of the field extension $\mathbb{Q} \subset k$, we have that $n = r + 2s$, where $r = \#\{\sigma : k \hookrightarrow \mathbb{C} \mid \sigma \text{ real}\}$ (look at the roots of the minimal polynomial for a generator $\mathbb{Q}(\alpha) = k$). Hence

$$\sqrt{|\Delta_k|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$$

Check that this last number is > 1 for each $n \geq 2$ hence

$$|\Delta_k| > 1 \text{ as well.} \qquad \square$$

Now we start with the proof of the theorem.

Ultima modifica: 11:31