Théorie des Nombres TD6

M2 AAG 2021-2022

Exercice 1 (Minkowski's bound). Let K be a number field. The goal is to show the following statement

Theorem 1 (Minkowski). *Let $\alpha \in Cl(K)$. Then there exists an ideal I of $\mathcal{O}_K$ with class α such that*

$$N_{K/\mathbb{Q}}(I) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}.$$

Let $\tau_1, \dots, \tau_{r_1}, \sigma_1, \dots, \sigma_{r_2}$ the real, resp. complex up to conjugacy, embeddings of K, and denote

$$i : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, x \mapsto (\tau_1(x), \dots, \tau_{r_1}(x), \sigma_1(x), \dots, \sigma_{r_2}(x)).$$

We identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^d =: V$ with $d = r_1 + 2r_2$ in the obvious way.

1. Show that, if $i(x) = (t_1, \dots, t_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2}) \in V$, then
$$\begin{aligned} |N_{K/\mathbb{Q}}(x)| &\leqslant \frac{1}{n^n}(|t_1| + \cdots + |t_{r_1}| + 2|x_1 + iy_1| + \cdots + 2|x_{r_2} + iy_{r_2}|)^n \\ &\leqslant n^{-n/2}\left(\sqrt{t_1^2 + \cdots + t_{r_1}^2 + 2(x_1^2 + y_1^2) + \cdots + 2(x_{r_2}^2 + y_{r_2}^2)}\right)^n. \end{aligned}$$

We then set the norm $||.||$ on V by $||(t_1, \dots, t_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2})|| = t_1^2 + \cdots + t_{r_1}^2 + 2(x_1^2 + y_1^2) + \cdots + 2(x_{r_2}^2 + y_{r_2}^2)$.

2. For I an ideal of $\mathcal{O}_K$, show that $N_{K/\mathbb{Q}}(I) = (|\mathcal{O}_K/I|)$.
3. Let I be a fractional ideal of K, show that
$$\text{covol}(I) = \sqrt{|d_K|}N_{K/Q}(I).$$
4. Show that the volume for the mesure coming from $||.||$ of the unit ball for $||.||_1$, i.e. the volume of
$$\{x \in \mathbb{R}^n | \sum_i |x_i| \leqslant 1\},$$
is
$$V_n = 2^{r_1}\pi^{r_2}\frac{1}{n!}.$$

5. Let I be a fractional ideal of K. Show that I contains a non-zero element of norm at most
$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}|N_{K/\mathbb{Q}}(I)|$$
6. Prove the theorem.

Exercice 2 (Calculation of some class groups). 1. Let $K = \mathbb{Q}(i\sqrt{7})$. Show that $h_K := |C\ell(\mathcal{O}_K)| = 1$.

2. Let $K = \mathbb{Q}(\sqrt{-5})$. Show that $C\ell(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$.
3. Deduce that $Y^3 = X^2 + 5$ has no integral solution.
4. Let $K = \mathbb{Q}(\sqrt{-14})$. Show that $C\ell(\mathcal{O}_K) = \mathbb{Z}/4\mathbb{Z}$.
5. Let $K = \mathbb{Q}(\sqrt{2})$ or $K = \mathbb{Q}(\sqrt{7})$. Show that $h_K := |C\ell(\mathcal{O}_K)| = 1$.

Exercice 3. Compute the class group of $\mathbb{Z}[\sqrt[3]{7}]$.

Remark 1. Actually we know the full list of quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for which the norm gives the structure of a euclidean ring for $\mathcal{O}_K$ (such a ring is called *norm euclidean*):

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

But the story doesn't stop here : while we know that for quadratic *imaginary* field (i.e. $d < 0$) euclidean and norm euclidean are equivalent, thus giving the full list of quadratic imaginary field for which integral elements form an euclidean ring, the result is completely different for *real* quadratic fields ($d > 0$), as for $d = 14, 69$ the corresponding rings are euclidean but not Norm euclidean (a theorem of Harper and Clark respectively). Also, we know completely the list of *principal* integer rings for *imaginary* quadratic fields, adding

$$-19, -43, -67, -163,$$

to the previous list and we know that when $d \to -\infty$ then the class number h_K goes to infinity (Heilbronn), while for *real* quadratic fields this is widely open, and there is a conjecture of Gauss that $\mathcal{O}_K$ will be principal for an infinite number of real quadratic field (actually $\sim 75,4\%$ of them).

Exercice 4. Let F be a number field, and $\chi : \mathbb{A}_F^\times/F^\times \longrightarrow \mathbb{C}^\times$ be a character.

1. Show that there exists $\chi_v : F_v^\times \longrightarrow \mathbb{C}^\times$ unramified for almost all v such that $\chi = \bigotimes_v \chi_v$, i.e.

$$\chi((x_v)_v) = \prod_v \chi_v(x_v).$$

Let $\mathfrak{m} = \prod_v \mathfrak{p}_v^{c_v}$ where $\mathfrak{p}_v$ corresponds to the finite place v of F and c_v is the conductor of χ_v. Let χ_∞ the induced character of $\prod_{v|\infty} \chi_v$. Denote $I^{\mathfrak{m}} := I^{\mathfrak{m}}(F)$ the group of prime to $\mathfrak{m}$ fractional ideals of F.

1. Show that

$$\omega : \begin{array}{ccc} I^{\mathfrak{m}} & \longrightarrow & \mathbb{C}^\times \\ \mathfrak{a} & \longmapsto & \prod_{v\nmid\infty} \chi_v(\pi_v^{v_{\mathfrak{p}_v}(\mathfrak{a})}) \end{array},$$

is well defined.

2. Show that if $F_{\mathfrak{m}}^\times = \{\alpha \in F^\times | a \equiv 1 \mod \mathfrak{m}\}$ then

$$\omega((\alpha)) = \chi_\infty(\alpha)^{-1}.$$

3. Show that $\chi_{\infty|\mathcal{O}_F^\times \cap F_{\mathfrak{m}}^\times} = 1$.

4. Conversely show that if we have $\mathfrak{m}$ a non zero ideal of $\mathcal{O}_F$, ω_∞ a character of $F_\infty^\times$, trivial on $\mathcal{O}_F^\times \cap F_{\mathfrak{m}}^\times$, and a character

$$\omega : I^{\mathfrak{m}} \longrightarrow \mathbb{C}^\times,$$

such that $\omega((\alpha)) = \omega_\infty(\alpha)^{-1}$ for all $\alpha \in F_{\mathfrak{m}}^\times$, then there exists a unique

$$\chi : \mathbb{A}_F^\times / F^\times \longrightarrow \mathbb{C}^\times,$$

inducing ω, whose character divides $\mathfrak{m}$.

5. Show that characters of the class group of F corresponds to idele characters with $\mathfrak{m} = \mathcal{O}_F$ and $\chi_\infty = 1$.

Exercice 5. Let $F = \mathbb{Q}$ here.

1. What are the possibilities for χ_∞ ?

2. Show that Hecke characters of weight $\omega_\infty = 1$ and conductor dividing N corresponds to Dirichlet characters of $(\mathbb{Z}/N\mathbb{Z})^\times$.

3. Show that if χ correspond to $\theta : \mathbb{Z}/N\mathbb{Z}^\times \longrightarrow \mathbb{C}^\times$ then $\chi_\infty = \mathrm{sgn}^a$ where $\theta(-1) = (-1)^a$.

4. Compute the L-function of such a character and its completed L-function.

5. Show that χ has conductor exactly N iff θ is primitive.

Exercice 6. Here $F = \mathbb{Q}(\sqrt{5})$. We denote $\varepsilon = \frac{1+\sqrt{5}}{2}$.

1. Show that $\mathcal{O}_F = \mathbb{Z}[\varepsilon]$ and $\mathcal{O}_F^\times = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$.

2. What are the characters with modulus $\mathfrak{m} = \mathcal{O}_F$ and $\omega_\infty = 1$?

3. Assume $\mathfrak{m} = \mathcal{O}_F$ and

$$\omega_\infty(x_1, x_2) = \left|\frac{x_1}{x_2}\right|^{\frac{-i\pi}{\log \varepsilon}}.$$

Show that this defines a character χ of I by

$$\chi((\alpha)) = \omega_\infty(\alpha) = \left|\frac{\alpha}{\sigma(\alpha)}\right|^{\frac{i\pi}{\log \varepsilon}},$$

where $\mathrm{Gal}(F/\mathbb{Q}) =< \sigma >$.

4. Write down its L-function and functional equation.

Exercice 7. Let $N > 1$ an integer and for $a \in \mathbb{Z}/N\mathbb{Z}$ we define the partial zeta function

$$\zeta_a(s) = \sum_{n \geqslant 1, n \equiv a \mod N} n^{-s}.$$

For $x > 0$ the Hurwitz zeta function $\zeta(s, x)$ is given by

$$\zeta(s, x) = \sum_{n=0}^{\infty} \frac{1}{(n+x)^s}.$$

Let $\chi : \mathbb{Z}/N\mathbb{Z}^\times \longrightarrow \mathbb{C}^\times$ a Dirichlet character, which we extend to $\mathbb{N}$ by $\chi(a) = 0$ if $\overline{a} \notin \mathbb{Z}/N\mathbb{Z}^\times$.

1. Give an expression for $L(s, \chi)$ in terms of $\zeta_a(s)$ and of $\zeta_a(s)$ in terms of $\zeta(s, x)$ for some x.

2. Show that

$$\Gamma(s)\zeta(s, x) = \int_0^{+\infty} \frac{e^{-xt}}{1 - e^{-t}} t^s \frac{\mathrm{d}t}{t}, \quad \text{for } \Re(s) > 1$$

For $n \in \mathbb{N}$, denote by $B_n(x) \in \mathbb{C}[x]$ the n-th Bernouilli polynomial, defined by

$$\frac{te^{xt}}{e^t - 1} = \sum_{n \geqslant 0} B_n(x) \frac{t^n}{n!} \in \mathbb{C}[x][[t]].$$

3. Show that if $B_n := B_n(0)$ then $B_0 = 1$, and $(n+1)B_n = -\sum_{n=0}^{n-1} \binom{n+1}{s} B_s$ [redacted]

   for $n > 0$.

4. Calculate B_1, show that

$$B_n(x) = \sum_{s=0}^{n} \binom{n}{s} B_s x^{n-s},$$

   and deduce $B_1(x)$.

5. Show that

$$\int_0^1 \frac{e^{-xt}}{1 - e^{-t}} t^s \frac{\mathrm{d}t}{t} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} \frac{(-1)^n}{s + n - 1},$$

   and deduce that $\Gamma(s)\zeta(s, x)$ as meromorphic continuation on $\mathbb{C}$. Where are the poles ?

6. Let $n \in \mathbb{N}_{>0}$. Compute $\lim_{s \to 1-n} (s + n - 1)\Gamma(s)$ and deduce

$$\zeta(1 - n, x) = -\frac{B_n(x)}{n}.$$

7. Deduce finally the equality

$$L(0, \chi) = -\frac{1}{N} \sum_{s=1}^{N-1} s\chi(s).$$

Exercice 8. Let $F = \mathbb{Q}(\sqrt{-26})$.

1. What are the integer ring and the discriminant of F ? What is $|\mathcal{O}_K^{tors}|$?

2. What is the class group of F ?

3. Let $\phi : \{p \in \mathbb{Z} \text{ prime}\} \longrightarrow \mathbb{Z}$ the function defined by

$$\phi(p) = \begin{cases} 1 & \textit{if p is (totally) split} \\ -1 & \textit{if p is inert} \\ 0 & \textit{if p is ramified} \end{cases}$$

Denote

$$L(s) = \prod_p \frac{1}{1 - \phi(p)p^{-s}}.$$

Show that $L(s)$ is absolutely convergent for $\Re(s) > 1$ and

$$\zeta_F(s) = \zeta(s)L(s).$$

4. Our goal is to show that there exists a character $\chi : \mathrm{Gal}(\mathbb{Q}(\sqrt{-26})/\mathbb{Q}) \longrightarrow \{\pm 1\}$ such that $L(s) = L(\chi, s)$ for $\Re(s) > 1$.

   (a) Show that $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$. ***Hint : Show that*** $\zeta_8^2 + \zeta_8^{-2} = 0$.

   (b) Show that $\mathbb{Q}(\sqrt{13}) \subset \mathbb{Q}(\zeta_{13})$. ***Hint : consider*** $g_k = \sum_{a\in\mathbb{Z}/13\mathbb{Z}^\times} \left(\frac{a}{p}\right) \zeta_{13}^{ka}$ ***and show that*** $g_1^2 = 13$.

   (c) Deduce that $\mathbb{Q}(i\sqrt{26}) \subset \mathbb{Q}(\zeta_{104})$. How many quadratic extensions in $\mathbb{Q}(\zeta_{104})$ are there ?

   (d) Construct a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_{104})/\mathbb{Q}) \longrightarrow \{\pm 1\}$ which sends a prime p coprime to 104 to $\phi(p)$.

   (e) Show that this factors through the extension $\mathrm{Gal}(\mathbb{Q}(i\sqrt{26})/\mathbb{Q})$. ***Hint : Look at primes 5 and 7 and use previous questions.***

5. What is the value $L(1, \chi)$?

6. Deduce $L(0, \chi)$ and $\sum_{s=1}^{103} s\ \chi(s)$.