Feuille 4 : Unités, groupe des classes

1 Outils en vrac

— La borne de Minkowski d'un corps K de degré n et de signature (r_1, r_2) est

$$M_K = \sqrt{|\mathrm{disc}(K)|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n} \tag{1}$$

Tout idéal fractionnaire $\mathfrak{a}$ de $\mathbb{Z}_K$ contient un élément α tel que $\left|N_{K/\mathbb{Q}}(\alpha)\right| \leqslant M_K N(\mathfrak{a})$.

— Quelques constantes de Minkowski

Signature (r_1, r_2)	(2,0)	(0,1)	(3,0)	(1,1)	(4,0)	(2,1)	(0,2)
$(\frac{\pi}{4})^{-r_2}\frac{n!}{n^n}$	0.5	0.63661	0.2222	0.28299	0.09375	0.11937	0.15198

— Le discriminant de $x^3 + px + q$ est $-4p^3 - 27q^2$.

— Si un polynôme unitaire $f(x) \in \mathbb{Z}[x]$ est un polynôme d'Eisenstein en un premier p, alors en notant α une racine de f, (p) est totalement ramifié dans l'anneau d'entiers de $\mathbb{Q}(\alpha)$ et $\mathbb{Z}[\alpha]$ y est p-maximal.

— Soit $f(x) \in \mathbb{Z}[x]$ irréductible unitaire, dans $K = \mathbb{Q}(\alpha)$ on a $N_{K/\mathbb{Q}}(k - \alpha) = f(k)$.

— Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, où $d \in \mathbb{Z}$ est sans facteur carré. On note d_K son discriminant : si $d \equiv 1 \bmod 4$ on a $d_K = d$ et $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, sinon $d_K = 4d$ et $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$. Un premier $p \geqslant 3$ qui ne divise pas d_K est décomposé dans K si d_K est un carré modulo p, et inerte sinon.

2 Groupe des classes

Exercice 1 :

Montrer que toute classe d'idéaux contient un idéal entier $\mathfrak{a}$ de norme $N(\mathfrak{a}) \leqslant M_K$ (considérer un élément $\alpha \in I^{-1}$).

> Soit I un idéal fractionnaire, et $\alpha \in I^{-1}$ tel que $|N(\alpha)| \leqslant M_K N(I^{-1})$. Alors $\mathfrak{a} = \alpha I$ est un idéal de la classe de I, c'est un idéal entier puisque $\mathfrak{a} \subset II^{-1} = \mathbb{Z}_K$, et $N(\mathfrak{a}) = N(\alpha I) = |N(\alpha)|\, N(I) \leqslant M_K$ (la norme est multiplicative).

Exercice 2 :

On considère le corps $K = \mathbb{Q}(\sqrt{-43})$.

1. Calculer la décomposition de 2 et 3 dans K.

> Puisque $-43 \equiv 1 \bmod 4$, on a $d_K = -43$ et $\mathbb{Z}_K = \mathbb{Z}[\theta]$ où $\theta = \frac{1+\sqrt{-43}}{2}$ vérifie $\theta^2 - \theta + 11 = 0$.
> $x^2 - x + 11$ est irréductible modulo 2, donc (2) est inerte.
> $x^2 - x + 11$ est également irréductible modulo 3 (ou $-43 \equiv -1$ n'est pas un carré) donc 3 est également inerte.

2. Calculer M_K, et montrer que $\mathbb{Z}_K$ est principal.

> La borne vaut $M_K = \frac{\sqrt{43}}{2} < 4$, donc toute classe d'idéaux contient un idéal de norme inférieure à 4. Or 2 et 3 sont de norme 4 et 9 (et principaux par dessus le marché), donc le groupe des classes est trivial.

Pascal Molin, version 14 octobre 2021.

3. Soit $\alpha \in \mathbb{Z}_K \setminus \mathbb{Z}$ qui engendre un idéal premier, montrer que $N_{K/\mathbb{Q}}(\alpha)$ est un nombre premier.

Si $(\alpha) = (p)$ est un premier inerte, alors α/p est une unité de K. Or les unités de K sont ± 1, donc $\alpha \in \mathbb{Z}$, impossible. (le raisonnement interdit également à (α) d'être un premier ramifié).
Donc (α) est un premier décomposé, et sa norme vaut p.

4. Montrer que si $\alpha \in \mathbb{Z}_K \setminus \mathbb{Z}$, $N(\alpha) \geqslant 11$.

Notons $\alpha = x + y\theta$ avec $y \neq 0$ dans $\mathbb{Z}$. Alors $N(\alpha) = x^2 + xy + 11y^2$ où $10y^2 \geqslant 10$ et $x^2 + xy + y^2 \geqslant 1$.

5. Soient x et $y \neq 0$ deux entiers premiers entre eux tels que $x^2 + xy + 11y^2 < 121$. Montrer que $x^2 + xy + 11y^2$ est un nombre premier.

Notons toujours $\alpha = x + y\theta$.
Par hypothèse, (α) n'est divisible par aucun premier inerte,
Si $N(\alpha)$ n'est pas un nombre premier, soit $\mathfrak{p}$ un diviseur premier de (α) de norme $N(\mathfrak{p}) < 11$. Puisque $\mathfrak{p} = (\beta)$, on doit avoir $\beta \in \mathbb{Z}$, c'est un diviseur commun à x et y, impossible.
Ainsi, les $x^2 + x + 11$ sont premiers pour $0 \leqslant x \leqslant 9$.

remarque : on montre de la même manière que $x^2 + x + 41$ est premier pour $0 \leqslant x \leqslant 39$, mais la construction s'arrête là.

Exercice 3 :

Soit $K = \mathbb{Q}(\alpha)$, où α est une racine de $x^3 + 6x + 6$.

1. Déterminer le discriminant d_K de K et son anneau d'entiers.

Le discriminant de $x^3 + 6x + 6$ vaut $-4.6^3 - 27.6^2 = -2^2.3^3.(8+9) = -2^2.3^3.17$. Ce polynôme étant d'Eisenstein en 2 et 3, et puisque 17 apparaît sans carré on a $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

2. Déterminer la signature de K, et sa constante de Minkowski M_K.

Le discriminant est négatif, donc le corps n'est pas réel, la signature est $(1,1)$ et la constante de Minkowski vaut 12.123.

3. Déterminer les idéaux premiers de norme inférieure à M_K

On sait que $(2) = \mathfrak{p}_2^3$ est totalement ramifié, ainsi que $(3) = \mathfrak{p}_3^3$.
On applique le lemme de Dedekind en 5 : $x^3 + x + 1$ est irréductible modulo 5 car sans racine, donc (5) est inerte.
On décompose (7) : $x^3 - x - 1 = (x+2)(x^3 - 2x + 3)$, donc il y a un premier $\mathfrak{p}_7 = (7, \alpha + 2)$ de norme 7.
Enfin $x^3 + 6x + 6$ n'a pas de racine modulo 11, donc (11) est inerte.
Ainsi, $\mathfrak{p}_2$, $\mathfrak{p}_3$ et $\mathfrak{p}_7$ engendrent $\mathrm{Cl}(K)$.

4. Calculer $N(\alpha)$ et $N(\alpha + 2)$, en déduire que $\mathrm{Cl}(K)$ est cyclique.

Pascal Molin, version 14 octobre 2021.

$N(\alpha) = 6$ donc $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$, donc $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$ dans le groupe des classes.
De même, $N(\alpha+2) = 14$ donc $\mathfrak{p}_2\mathfrak{p}_7$ est principal. Ainsi, $\mathrm{Cl}(K)$ est engendré par $\mathfrak{p}_2$.

5. Montrer que $u = \alpha + 1 \in \mathbb{Z}_K^\times$ est une unité. On admet qu'elle est non triviale dans $\mathbb{Z}_K^\times/(\mathbb{Z}_K^\times)^3$ (il se trouve que c'est une unité fondamentale).

$N(u) = -1$ donc c'est une unité.

6. Montrer que 2, $2u$ et $2u^2$ ne sont pas des cubes dans $\mathbb{Z}_K$ (regarder modulo $\mathfrak{p}_7$).

7. En déduire $\mathrm{Cl}(K)$.

Il faut voir si $\mathfrak{p}_2$ est principal, ou d'ordre 3 dans $\mathrm{Cl}(K)$ (puisque $(2) = \mathfrak{p}_2^3$ est principal).
Si $\mathfrak{p}_2 = (\beta)$, on aurait $(\beta^3) = (2)$, donc l'existence

Exercice 4 :

Soit $d > 1$ un entier sans facteur carré, $K = \mathbb{Q}(\sqrt{-d})$ et d_K son discriminant. Soit p un nombre premier décomposé dans K, et $\mathfrak{p}$ un idéal au dessus de p.

1. Montrer que pour tout $i \geqslant 1$ tel que $p^i < \frac{|d_K|}{4}$, $\mathfrak{p}^i$ n'est pas principal.

Puisque p est décomposé, $N(\mathfrak{p}) = p$. On suppose que $\mathfrak{p}^i = (z)$, de sorte que $N(z) = p^i$.
Si $d_K = -4d$, on décompose $z = x + y\sqrt{-d}$ et $x^2 + dy^2 = p^i$, en particulier $y^2 < p^i/d$ donc $y = 0$ et $p \mid z$, impossible.
Si $d_K = -d$, on obtient plutôt $(x + \frac{y}{2})^2 + d(\frac{y}{2})^2 = p^i$. On déduit de même $y^2 < 4p^i/d < 1$ donc $y = 0$, impossible.

2. En déduire que $h_K \geqslant 1 + \lfloor \frac{\log|d_K|}{\log p} \rfloor$.

Les puissances $\mathfrak{p}^i$ sont donc distinctes dans le groupe des classes. En ajoutant la classe triviale on obtient l'inégalité.
Remarque : cette observation ne mène pas à une borne inférieure sur h_K (un problème difficile), cela montre au contraire qu'on a peu de contrôle sur le plus petit premier qui soit résidu quadratique modulo d.

3 Unités

Exercice 5 : Unités des corps cubiques

Soit K un corps de nombres cubique, tel que $\mathrm{disc}(K) < 0$.

1. Montrer que la signature de K est $(1,1)$ (commencer par supposer $\mathbb{Z}_K$ monogène).

Soit α un entier algébrique tel que $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, et $\alpha_1, \alpha_2, \alpha_3$ ses conjugués, alors $\mathrm{disc}(K) = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Si on avait $r_1 = 3$, le discriminant serait un produit de carrés dans $\mathbb{R}$, donc serait positif. L'argument subsiste si $\mathbb{Z}[\alpha]$ est d'indice fini, puisque son discriminant diffère d'un carré de celui de K, donc a le même signe.
Plus généralement, le discriminant d'un corps de nombres est toujours de signe $(-1)^{r_2}$.

Pascal Molin, version 14 octobre 2021.

2. Désormais, on utilise le plongement réel pour voir K comme un sous-corps de $\mathbb{R}$. Montrer qu'il existe $\epsilon > 1$ tel que $\mathbb{Z}_K^\times = \left\{\pm\epsilon^k, k \in \mathbb{Z}\right\}$.

> Les racines de l'unité se plongent dans $\mathbb{R}$, ce sont donc ± 1. Le théorème des unités énonce que le rang vaut 1, il existe donc une unité fondamentale ϵ telle que $\mathbb{Z}_K^\times = \left\{\pm\epsilon^k, k \in \mathbb{Z}\right\}$. Quitte à changer ϵ par $\pm\epsilon^{\pm 1}$, on peut supposer $\epsilon > 1$.

3. Montrer que $K = \mathbb{Q}(\epsilon)$, et que le polynôme minimal de ϵ est de la forme $g(x) = (x-\epsilon)(x - \frac{e^{it}}{\sqrt{\epsilon}})(x - \frac{e^{-it}}{\sqrt{\epsilon}})$ pour $t \in \mathbb{R}$.

> On a $\epsilon \notin \mathbb{Q}$, car $\mathbb{Q}$ n'a pas d'unité d'ordre infini. Puisque $\mathbb{Q}(\epsilon) \subset K$ est de degré divisant 3, on a égalité.
> On écrit le minimal $g(x) = (x-\epsilon)(x-z)(x-\bar{z})$, avec la norme $N(\epsilon) = \pm 1 = \epsilon\,|z|^2 > 0$, donc $|z|^2 = \epsilon^{-1}$. En écrivant une décomposition polaire on a l'écriture souhaitée.

4. Montrer l'inégalité d'Artin : $|\mathrm{disc}(g(x))| < 4(\epsilon^3+6)$ (utiliser sans preuve l'inégalité magique $\left(\frac{u^3+u^{-3}}{2} - \cos t\right)^2 \sin^2 t < \frac{u^6+6}{4}$, valable pour tous réels u, t).

> Poser $u = \sqrt{\epsilon}$, et faire le calcul $\mathrm{disc}(g(x)) = \left((u^2 - \frac{e^{it}}{u})(u^2 - \frac{e^{-it}}{u})(\frac{e^{it}-e^{-it}}{u})\right)^2 = \left(\frac{(u^6-2\cos(t)+1)(2i\sin(t))}{u}^3\right)^2$, donc $|\mathrm{disc}(g(x))| = 4^2\left(\frac{u^3+u^{-3}}{2} - \cos t\right)^2 \sin^2 t < 4(u^6+6) = 4(\epsilon^3+6)$.

5. Montrer que si $u > 1$ est une unité et vérifie $4(u^{\frac{3}{2}}+6) < |\mathrm{disc}(K)|$, alors $u = \epsilon$.

> Puisque $\mathrm{disc}(K) < \mathrm{disc}(g(x)$, une unité fondamentale vérifie $|\mathrm{disc}(K)| < 4(\epsilon^3+6)$. Si $u = \epsilon^k$ avec $k \geqslant 2$, alors ϵ violerait l'inégalité d'Artin.

6. Soit $K = \mathbb{Q}(\alpha)$ où $\alpha^3 + \alpha = 1$. Déterminer une unité fondamentale de K (on donne $\alpha \approx 0.682$ dans $\mathbb{R}$).

> Soit $f(x) = x^3 + x - 1$, $\mathrm{disc}(f) = -31$ est sans facteur carré, donc il est égal à $\mathrm{disc}(K)$.
> Étant donné la forme de l'équation, α et α^2+1 sont des unités. La seconde vérifie $\alpha^2+1 \approx 1.36$.

Pascal Molin, version 14 octobre 2021.