Théorie des Nombres - TD10
Idéaux d'un corps de nombres

Exercice 1 : On considère l'anneau $A := \mathbb{Z}[\sqrt{-3}]$. On va montrer que dans cet anneau, le théorème d'existence de la décomposition des idéaux en produit d'idéaux premiers n'est pas vérifié.

a) On définit l'idéal de A : $\mathfrak{a} := (2, 1+\sqrt{-3})$. Montrer que $\mathfrak{a}$ est un idéal premier et que $\mathfrak{a} \neq (2)$.

b) Montrer que $\mathfrak{a}^2 = (2)\mathfrak{a}$.

c) Montrer que les idéaux de A ne se décomposent pas de manière unique en produit d'idéaux premiers.

d) Montrer que $\mathfrak{a}$ est l'unique idéal premier contenant 2.

e) Montrer que (2) n'est pas produit d'idéaux premiers de A.

Solution de l'exercice 1.

a) On a un isomorphisme d'anneaux $A \cong \mathbb{Z}[X]/(X^2+3)$, où la classe de X correspond à $\sqrt{-3} \in A$. Par conséquent, le quotient $A/\mathfrak{a}$ est isomorphe au quotient $(\mathbb{Z}/2\mathbb{Z})[X]/(X^2+3, 1+X)$. Or dans $\mathbb{Z}/2\mathbb{Z}[X]$, on a $X^2+3 = X^2+1 = (X+1)^2$, donc $A/\mathfrak{a} \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X+1) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$. Par conséquent, $A/\mathfrak{a}$ est un corps, donc $\mathfrak{a}$ est un idéal maximal, donc premier.

L'élément $1+\sqrt{-3}$ est dans $\mathfrak{a}$, mais pas dans (2). En effet, si $1+\sqrt{-3} \in (2)$, alors $\frac{1+\sqrt{-3}}{2} \in A$, i.e. il existe $a, b \in \mathbb{Z}$ tels que $\frac{1+\sqrt{-3}}{2} = a + b\sqrt{-3}$. Or $(1, \sqrt{-3})$ est une base de $\mathbb{Q}(\sqrt{-3})$ sur $\mathbb{Q}$, donc $a = b = \frac{1}{2}$, ce qui est contradictoire. Donc $a \neq (2)$.

b) Par définition, l'idéal $\mathfrak{a}^2$ est engendré par les éléments $2^2 = 4$, $(1+\sqrt{-3})^2 = -2+2\sqrt{-3}$ et $2(1+\sqrt{-3})$. Donc $\mathfrak{a}^2 = (4, 2+2\sqrt{-3}) = (2)\mathfrak{a}$.

c) Supposons que tous les idéaux de $\mathfrak{a}$ se décomposent de façon unique en produit d'idéaux premiers. Alors $(2) = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$, avec $\mathfrak{p}_i$ premiers distincts et $n_i \in \mathbb{N} \setminus \{0\}$. Donc $\mathfrak{a}^2 = \mathfrak{a}\prod_{i=1}^r \mathfrak{p}_i^{n_i}$, donc par unicité $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$, donc $\mathfrak{a} = (2)$, ce qui contredit la question a). Par conséquent, dans l'anneau A, on n'a pas décomposition unique des idéaux en idéaux premiers.

d) On a montré en a) que $\mathfrak{a}$ est un idéal maximal, et il est clair qu'il contient 2. Soit $\mathfrak{p}$ un idéal premier de $\mathfrak{a}$ contenant 2. Alors $(1+\sqrt{-3})^2 = 2(-1+\sqrt{-3}) \in (2)$. Donc $(1+\sqrt{-3})^2 \in \mathfrak{p}$, or $\mathfrak{p}$ est premier, donc $1+\sqrt{-3} \in \mathfrak{p}$, donc $\mathfrak{a} \subset \mathfrak{p}$, donc par maximalité, $\mathfrak{a} = \mathfrak{p}$. D'où le résultat.

e) Supposons que (2) se décompose en produit d'idéaux premiers. La question d) assure que cette décomposition est de la forme $(2) = \mathfrak{a}^n$, avec $n \geq 2$. Alors $(2) = \mathfrak{a}^n \subset \mathfrak{a}^2 = (2)\mathfrak{a} \subset (2)$, donc ces inclusions sont des égalités, donc $(2)\mathfrak{a} = (2)$, donc $\mathfrak{a} = A$, ce qui n'est pas puisque $\mathfrak{a}$ est premier. Donc l'idéal (2) ne se décompose pas en produit d'idéaux premiers.

Exercice 2 : On considère le corps quadratique $K := \mathbb{Q}(\sqrt{-5})$, et $A := \mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$.

a) Montrer que l'anneau $\mathbb{Z}_K$ n'est pas factoriel.

[Indication : on pourra donner deux décompositions distinctes de 6 en produit d'irréductibles de A.]

b) Soit p premier. Montrer que $A/pA \cong \mathbb{F}_p \times \mathbb{F}_p$, $\mathbb{F}_{p^2}$ ou $\mathbb{F}_p[t]/(t^2)$ suivant la décomposition du polynôme X^2+5 dans $\mathbb{F}_p[X]$.

c) En calculant le discriminant de K, montrer que le troisième cas ($A/pA \cong \mathbb{F}_p[t]/(t^2)$) se produit si et seulement si $p = 2$ ou $p = 5$.

d) En étudiant $A/2A$, montrer qu'il existe un unique idéal maximal $\mathfrak{m}_2 \subset A$ contenant 2. Montrer en outre que $\mathfrak{m}_2 = (2, 1+\sqrt{-5})$ et que $2A = \mathfrak{m}_2^2$.

e) Montrer que les idéaux maximaux contenant 3 sont $\mathfrak{m}_3 := (3, -1+\sqrt{-5})$ et $\overline{\mathfrak{m}_3} := (3, 1+\sqrt{-5})$, puis décomposer $3A$ en produit d'idéaux premiers de A.

f) Donner la factorisation de $6A$ en produit d'idéaux premiers.

g) Montrer que $\mathfrak{m}_2$, $\mathfrak{m}_3$ et $\overline{\mathfrak{m}_3}$ ne sont pas principaux, alors que $\mathfrak{m}_2\mathfrak{m}_3$ et $\mathfrak{m}_2\overline{\mathfrak{m}_3}$ le sont. Expliquer ainsi l'existence de deux factorisations de 6 dans A.

h) En utilisant la constante de Minkowski, calculer le groupe des classes de K.

Solution de l'exercice 2.

a) On écrit
$$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})\,.$$
Or on a $N_{K/\mathbb{Q}}(2) = 4$, $N_{K/\mathbb{Q}}(3) = 9$ et $N(1\pm\sqrt{-5}) = 6$. Donc les éléments $2, 3, 1\pm\sqrt{-5} \in A$ sont irréductibles s'il n'existe pas d'éléments dans A qui ont pour norme 2 ou 3. Or l'équation $N_{K/\mathbb{Q}}(a+b\sqrt{-5}) = 2$ ou 3 (avec $a, b \in \mathbb{Z}$) s'écrit $a^2+5b^2 = 2$ ou 3, et il est clair que cette équation n'a pas de solution. Par conséquent, $2, 3, 1\pm\sqrt{-5} \in A$ sont irréductibles, et vu le calcul de leur norme, 2 (resp. 3) n'est pas associé à $1\pm\sqrt{-5}$. Donc on dispose bien de deux décompositions réellement distinctes (i.e. qui ne diffèrent pas d'une unité) de $6 \in A$ en produit de facteurs irréductibles. Donc A n'est pas factoriel.

b) On dispose d'un isomorphisme $\mathbb{Z}[X]/(X^2+5) \xrightarrow{\cong} A$. Donc pour tout nombre premier p, on a $A/pA \cong \mathbb{F}_p[X]/(X^2+5)$. Trois cas peuvent alors se produire :
- soit le polynôme X^2+5 est irréductible sur $\mathbb{F}_p$. Alors A/pA est un corps de degré 2 sur $\mathbb{F}_p$, donc $A/pA \cong \mathbb{F}_{p^2}$.
- soit le polynôme X^2+5 a deux racines distinctes dans $\mathbb{F}_p$, notées λ_1 et λ_2. Alors
$$A/pA \cong \mathbb{F}_p[X]/(X-\lambda_1)(X-\lambda_2) \cong \mathbb{F}_p[X]/(X-\lambda_1) \times \mathbb{F}_p[X]/(X-\lambda_2) \cong \mathbb{F}_p \times \mathbb{F}_p$$
où le deuxième isomorphisme provient du lemme chinois.
- soit le polynôme X^2+5 admet une racine double λ dans $\mathbb{F}_p$. Alors $A/pA \cong \mathbb{F}_p[X]/(X-\lambda)^2 \cong \mathbb{F}_p[X]/(X^2)$.

c) Le discriminant de K vaut $D_K = -45 = -20$. On est dans le troisième cas si et seulement si la réduction de X^2+5 modulo p a une racine double dans $\mathbb{F}_p$ si et seulement si la réduction de D_K modulo p est nulle si et seulement si p divise 20 si et seulement si $p = 2$ ou 5.

d) On a un isomorphisme $A/2A \cong \mathbb{F}_2[X]/((X+1)^2)$. Or l'anneau fini $\mathbb{F}_2[X]/((X+1)^2)$ admet pour unique idéal maximal l'idéal engendré par la classe de $X+1$, et le quotient de cet anneau par cet idéal maximal est $\mathbb{F}_2[X]/(X+1) \cong \mathbb{F}_2$. Par conséquent, un idéal $\mathfrak{m}$ de A contenant 2 est maximal si et seulement si $\mathfrak{m}$ est l'image réciproque de l'idéal maximal de $\mathbb{F}_2[X]/((X+1)^2)$ par le morphisme quotient $A \to A/2A$ si et seulement si $\mathfrak{m} = (2, \sqrt{-5}+1)$. Cela assure le résultat : $\mathfrak{m} = (2, \sqrt{-5}+1)$ est l'unique idéal maximal de A contenant 2.

Par conséquent, la décomposition de (2) en idéaux premiers est de la forme $(2) = \mathfrak{m}_2^r$, avec $r \geq 2$. On calcule alors les normes dans cette égalité : on trouve $4 = N(\mathfrak{m})^r = 2^r$, donc $r = 2$. Donc $(2) = \mathfrak{m}_2^2$.

e) On calcule $A/3A \cong \mathbb{F}_3[X]/(X^2+5) = \mathbb{F}_3[X]/((X-1)(X+1))$. On est donc dans le cas où X^2+5 a deux racines distinctes dans $\mathbb{F}_3$. Par conséquent, $A/3A \cong \mathbb{F}_3[X]/(X-1) \times \mathbb{F}_3[X]/(X+1)$, donc l'anneau $A/3A$ admet exactement deux idéaux maximaux, à savoir l'idéal engendré par la classe de $X-1$ et celui engendré par la classe de $X+1$. On obtient alors deux quotients isomorphes à $\mathbb{F}_3$. Par conséquent, l'anneau A admet exactement deux idéaux maximaux contenant 3, qui sont les images réciproques des deux idéaux maximaux de $A/3A$, à savoir les idéaux $\mathfrak{m}_3 := (3, \sqrt{-5}-1)$ et $\overline{\mathfrak{m}_3} := (3, \sqrt{-5}+1)$. Alors la décomposition de (3) est donnée par $(3) = \mathfrak{m}_3^r\overline{\mathfrak{m}_3}^s$, avec $r, s \geq 1$, donc en calculant les normes, on obtient $r = s = 1$, donc $(3) = \mathfrak{m}_3\overline{\mathfrak{m}_3}$.

f) Les questions d) et e), ainsi que l'unicité de la décomposition en idéaux premiers assurent que $6A = (2)(3) = \mathfrak{m}_2^2\mathfrak{m}_3\overline{\mathfrak{m}_3}$. C'est la décomposition en idéaux premiers de (6).

g) Si $\mathfrak{m}_2$ est principal, alors il est engendré par un élément de A de norme 2. Or on a vu qu'un tel élément n'existe pas. Donc $\mathfrak{m}_2$ n'est pas principal. De même pour $\mathfrak{m}_3$ et $\overline{\mathfrak{m}_3}$, puisque A ne contient pas d'élément de norme 3.

En revanche, on remarque que $\mathfrak{m}_2\overline{\mathfrak{m}_3}$ contient $1+\sqrt{-5}$ (on a $1+\sqrt{-5} = 3(1+\sqrt{-5})-2(1+\sqrt{-5})$), et $N_{K/\mathbb{Q}}(1+\sqrt{-5}) = 6 = N(\mathfrak{m}_2\overline{\mathfrak{m}_3})$, donc $\mathfrak{m}_2\overline{\mathfrak{m}_3} = (1+\sqrt{-5})$. De même, $\mathfrak{m}_2\mathfrak{m}_3 = (1-\sqrt{-5})$.

On a donc deux façons de regrouper les idéaux dans la décomposition en idéaux premiers de (6) : premièrement

$$(6) = (\mathfrak{m}_2^2)(\mathfrak{m}_3\overline{\mathfrak{m}_3}) = (2)(3)\,,$$

et deuxièmement

$$(6) = (\mathfrak{m}_2\overline{\mathfrak{m}_3})(\mathfrak{m}_2\mathfrak{m}_3) = (1+\sqrt{-5})(1-\sqrt{-5})\,.$$

On obtient ainsi les deux décompositions distinctes en facteurs irréductibles de $6 \in A$ comme deux "regroupements" de la décomposition de l'idéal (6) en produits de quatre idéaux premiers.

Cet exemple illustre le fait que le passage des entiers aux idéaux entiers permet de résoudre le problème de non-factorialité des anneaux d'entiers de corps de nombres...

h) On applique la majoration suivante : toute classe d'idéaux de A contient un représentant entier $\mathfrak{a}$ tel que $N(\mathfrak{a}) \leq M(K)|D_K|^{\frac{1}{2}}$, avec $M(K) := \left(\frac{2}{\pi}\right)^{r_2}$. Ici, on a $M(K)|D_K|^{\frac{1}{2}} = \frac{2\sqrt{20}}{\pi} \approx 2,85 < 3$. Par conséquent, il suffit de déterminer tous les idéaux entiers de norme ≤ 2. Or $N(\mathfrak{a}) = 1$ si et seulement si $\mathfrak{a} = A$. Et $N(\mathfrak{a}) = 2$ si et seulement si $\mathfrak{a}$ est maximal et $2 \in \mathfrak{a}$ si et seulement si $\mathfrak{a} = \mathfrak{m}_2$. En outre, on a montré que $\mathfrak{m}_2$ n'est pas principal, donc $h(K) = 2$ et $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z}$.

Exercice 3 : On considère $K := \mathbb{Q}(\sqrt{-23})$, $\alpha := \frac{1+\sqrt{-23}}{2}$ et $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

a) Calculer le polynôme minimal de α, le discriminant D_K et la constante de Minkowski de K.

b) Montrer que les idéaux $\mathfrak{p} := (2, \alpha)$ et $\mathfrak{q} := (3, \alpha)$ sont premiers non principaux.

c) Factoriser $2\mathbb{Z}_K$ et $3\mathbb{Z}_K$ en produits d'idéaux premiers.
[Indication : on pourra utiliser la factorisation du polynôme minimal de α modulo 2 et 3.]

d) Montrer que $\mathfrak{p}^3$ est principal.

e) Calculer le nombre de classes de K.

Solution de l'exercice 3.

a) On sait que puisque $-23 \equiv 1\ [4]$, on a $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ et $D_K = -23$. On vérifie immédiatement que le polynôme minimal de α est $X^2 - X + 6 \in \mathbb{Z}[X]$. Enfin, la constante de Minkowski vaut (puisque $r_2 = 1$) $M(K) = \frac{2}{\pi}$.

b) On calcule $\mathbb{Z}_K/\mathfrak{p} \cong \mathbb{F}_2[X]/(X^2+X, X) \cong \mathbb{F}_2[X]/(X) \cong \mathbb{F}_2$, donc $\mathfrak{p}$ est un idéal maximal. De même pour $\mathfrak{q}$. Si $\mathfrak{p}$ (resp. $\mathfrak{q}$) était principal, alors il existerait un élément dans $\mathbb{Z}_K$ de norme 2 (resp. de norme 3). Cela impliquerait que l'équation $a^2 + 23b^2 = 8$ (resp. $a^2 + 23b^2 = 12$) a une solution dans $\mathbb{Z}^2$, ce qui n'est pas le cas. Donc $\mathfrak{p}$ et $\mathfrak{q}$ ne sont pas principaux.

c) Modulo 2, le polynôme $X^2 - X + 6$ s'écrit $X^2 - X = X(X-1)$. Donc il a deux racines distinctes dans $\mathbb{F}_2$, donc on en déduit la décomposition de l'idéal (2) en idéaux premiers sous la forme $(2) = (2, \alpha)(2, \alpha - 1)$.

Modulo 3, le polynôme $X^2 - X + 6$ s'écrit $X^2 - X = X(X-1)$. Donc il a deux racines distinctes dans $\mathbb{F}_3$, donc on en déduit la décomposition de l'idéal (3) en idéaux premiers sous la forme $(3) = (3, \alpha)(3, \alpha - 1)$.

d) On a $N(\mathfrak{p}^3) = 8$, donc pour montrer que $\mathfrak{p}^3$ est principal, recherchons les entiers de norme 8. Soient $a, b \in \mathbb{Z}$. Alors $N(\frac{a+b\sqrt{-23}}{2}) = 8$ si et seulement si $a^2 + 23b^2 = 32$ si et seulement si $b = \pm 1$ et $a = \pm 3$ (les deux signes étant indépendants). Donc les éléments de norme 8 dans $\mathbb{Z}_K$ sont exactement $\pm(1+\alpha)$ et $\pm(\alpha - 2)$. Il y a donc exactement deux idéaux principaux distincts de norme 8 : $(1+\alpha)$ et $(\alpha - 2)$. Or on connaît tous les idéaux premiers contenant 2 : ce sont

$\mathfrak{p} = (2, \alpha)$ et $\mathfrak{p}' = (2, \alpha - 1)$. Donc les seules décompositions possibles pour les idéaux $(1+\alpha)$ et $(\alpha - 2)$ sont $\mathfrak{p}^3$, $\mathfrak{p}^2\mathfrak{p}' = (2)\mathfrak{p}$, $\mathfrak{p}\mathfrak{p}'^2 = (2)\mathfrak{p}'$ ou $\mathfrak{p}'^3$. Or on a montré que $\mathfrak{p}$ et $\mathfrak{p}'$ ne sont pas principaux, donc $(2)\mathfrak{p}$ et $(2)\mathfrak{p}'$ ne le sont pas non plus, donc nécessairement les idéaux principaux $(1+\alpha)$ et $(\alpha - 2)$ coïncident avec les idéaux $\mathfrak{p}^3$ et $\mathfrak{p}'^3$. En particulier, $\mathfrak{p}^3$ est principal.

e) La borne de Minkowski assure que toute classe d'idéaux contient un idéal entier de norme ≤ 3. Pour tout idéal $\mathfrak{a}$ de $\mathbb{Z}_K$, on a $N(\mathfrak{a}) = 2$ si et seulement si $\mathfrak{a} = \mathfrak{p}$ ou $\mathfrak{p}'$. De même, $N(\mathfrak{a}) = 3$ si et seulement si $\mathfrak{a} = \mathfrak{q}$ ou $\mathfrak{q}'$ (où $\mathfrak{q}' := (3, \alpha - 1)$). Donc en particulier $h(K) \leq 5$. Or $\mathrm{Cl}(K)$ contient un élément d'ordre 3 (à savoir la classe de $\mathfrak{p}$, voir question d)), donc $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$ (engendré par la classe de $\mathfrak{p}$) et $h(K) = 3$ (on peut vérifier en outre que $\mathfrak{q} = \mathfrak{p}^2$).

Exercice 4 : On note $K := \mathbb{Q}(\sqrt{-13})$ et σ l'élément non trivial du groupe de Galois de K sur $\mathbb{Q}$.

a) Donner $\mathbb{Z}_K$ et D_K.

b) Montrer que $2\mathbb{Z}_K = \mathfrak{p}^2$, où $\mathfrak{p}$ est un idéal premier non principal tel que $\sigma(\mathfrak{p}) = \mathfrak{p}$.

c) Montrer que $13\mathbb{Z}_K = \mathfrak{q}^2$, où $\mathfrak{q}$ est un idéal premier principal tel que $\sigma(\mathfrak{q}) = \mathfrak{q}$.

d) Montrer que $3\mathbb{Z}_K$ est un idéal premier.

e) Calculer $\mathbb{Z}_K^*$.

f) Calculer le nombre de classes de K.

g) Soit $y \in \mathbb{Z}$. Montrer que l'idéal $\mathfrak{d} := (y + \sqrt{-13}, y - \sqrt{-13})$ n'admet pas de diviseur premier autre que $\mathfrak{p}$ et $\mathfrak{q}$.

h) On écrit la décomposition de l'idéal $(y + \sqrt{-13})\mathbb{Z}_K = \mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta$, avec $\mathfrak{c}$ non divisible par $\mathfrak{p}$, ni par $\mathfrak{q}$. Montrer que $\mathfrak{c}$ et $\sigma(\mathfrak{c})$ n'ont pas de diviseur premier commun.

i) On considère désormais l'équation diophantienne $X^3 - Y^2 = 13$. Soit $(x, y) \in \mathbb{Z}^2$ une solution de cette équation.

   i) Montrer qu'il existe un idéal entier $\mathfrak{r}$ de $\mathbb{Z}_K$ et $a, b \in \mathbb{N}$ tels que $(y + \sqrt{-13})\mathbb{Z}_K = (\mathfrak{r}\mathfrak{p}^a\mathfrak{q}^b)^3$.

   ii) Montrer que l'idéal $\mathfrak{r}\mathfrak{p}^a\mathfrak{q}^b$ est principal.

   iii) En déduire qu'il existe $u, v \in \mathbb{Z}$ tels que $y = u^3 - 39uv^2$ et $1 = v(3u^2 - 13v^2)$.

   iv) Déterminer l'ensemble des solutions de l'équation diophantienne $X^3 - Y^2 = 13$.

Solution de l'exercice 4.

a) On sait que $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-13}]$ et $D_K = -4.13 = -52$.

b) Puisque modulo 2 le polynôme $X^2 + 13$ est égal à $X^2 + 1 = (X+1)^2$, il existe un unique idéal maximal $\mathfrak{p} = (2, 1 + \sqrt{-13})$ contenant 2, et un calcul de norme assure que $(2) = \mathfrak{p}^2$. Or $\mathfrak{p}$ est de norme 2, et il n'existe pas d'entier de norme 2 dans $\mathbb{Z}_K$ (l'équation $a^2 + 13b^2 = 2$ n'a pas de solution entière), donc $\mathfrak{p}$ n'est pas principal. Enfin, puisque $\sigma(1 + \sqrt{-13}) = 1 - \sqrt{-13} = 2 - (1 + \sqrt{-13}) \in \mathfrak{p}$, il est clair que $\sigma(\mathfrak{p}) = \mathfrak{p}$.

c) Dans $\mathbb{Z}_K$, on a $13 = -(\sqrt{-13})^2$, donc les idéaux (13) et $(\sqrt{-13})^2$ sont égaux. Notons $\mathfrak{q} := (\sqrt{-13})$ idéal principal. Alors $\mathfrak{q}$ est maximal car $\mathbb{Z}_K/\mathfrak{q} \cong \mathbb{F}_{13}[X]/(X) \cong \mathbb{F}_{13}$. Enfin, puisque $\sigma(\sqrt{-13}) = -\sqrt{-13}$, il est clair que $\sigma(\mathfrak{q}) = \mathfrak{q}$.

d) On a $\mathbb{Z}_K/(3) \cong \mathbb{F}_3[X]/(X^2 + 13) = \mathbb{F}_3[X]/(X^2 + 1)$. Or le polynôme $X^2 + 1$ est irréductible sur $\mathbb{F}_3$, donc $\mathbb{Z}_K/(3) \cong \mathbb{F}_9$, donc (3) est un idéal maximal, donc premier.

e) On a déjà montré dans la feuille de TD9, exercice 1, que $\mathbb{Z}_K^* = \{\pm 1\}$.

f) La borne de Minkowski vaut ici $M(K)\sqrt{|D_K|} = \frac{4\sqrt{13}}{\pi} \approx 4,6 < 5$. Par conséquent, il suffit d'étudier les idéaux entiers de norme ≤ 4. Or $N(\mathfrak{a}) = 2$ si et seulement si $\mathfrak{a} = \mathfrak{p}$; $N(\mathfrak{a}) = 3$ si et seulement si $\mathfrak{a} = (3)$ et $N(\mathfrak{a}) = 3$, or $N((3)) = 9$, donc il n'existe pas d'idéal entier de norme 3 ; $N(\mathfrak{a}) = 4$ si et seulement si $\mathfrak{a} = (2)$. Donc finalement, puisque l'idéal $\mathfrak{p}$ n'est pas principal, on en déduit que $h(K) = 2$.

g) Soit $\mathfrak{r}$ un idéal premier divisant $\mathfrak{d}$. Alors $2\sqrt{-13} = (y+\sqrt{-13}) - (y-\sqrt{-13}) \in \mathfrak{r}$, donc $2 \in \mathfrak{r}$ ou $\sqrt{-13} \in \mathfrak{r}$, donc $\mathfrak{r} = \mathfrak{p}$ ou $\mathfrak{r} = \mathfrak{q}$ (voir questions b) et c)). Donc $\mathfrak{d}$ n'admet pas de diviseur premier autre que $\mathfrak{p}$ et $\mathfrak{q}$.

h) Si $\mathfrak{r}$ est un idéal premier divisant $\mathfrak{c}$ et $\sigma(\mathfrak{c})$, alors $(y+\sqrt{-13}) = \mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta$ et $(y-\sqrt{-13}) = \sigma(\mathfrak{c})\mathfrak{p}^\alpha\mathfrak{q}^\beta$, donc $\mathfrak{r}$ divise $(y+\sqrt{-13})$ et $(y-\sqrt{-13})$, donc $\mathfrak{r}$ divise $\mathfrak{d}$, donc $\mathfrak{r} = \mathfrak{p}$ ou $\mathfrak{q}$, ce qui contredit le fait que $\mathfrak{c}$ ne soit pas divisible par $\mathfrak{p}$, ni par $\mathfrak{q}$. Donc $\mathfrak{c}$ et $\sigma(\mathfrak{c})$ n'ont pas de diviseur premier commun.

i) i) On dispose de l'égalité dans $\mathbb{Z}_K$: $x^3 = y^2 + 13 = (y+\sqrt{-13})(y-\sqrt{-13})$, donc en termes d'idéaux, on obtient $(x)^3 = (y+\sqrt{-13})(y-\sqrt{-13})$. On décompose l'idéal (x) en idéaux premiers : $(x) = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$. Alors $(x)^3 = \prod_{i=1}^r \mathfrak{p}_i^{3n_i}$. D'où avec les notations de la question h),

$$\prod_{i=1}^r \mathfrak{p}_i^{3n_i} = \mathfrak{c}\sigma(\mathfrak{c})\mathfrak{p}^{2\alpha}\mathfrak{q}^{2\beta}\,.$$

Par unicité de la décomposition en idéaux premiers, et en utilisant la question h), on en déduit qu'il existe un idéal entier $\mathfrak{c}'$ tel que $(\mathfrak{c}')^3 = \mathfrak{c}$ et que $3|2\alpha, 2\beta$. Donc il existe $a, b \in \mathbb{N}$ tels que $\alpha = 3a$ et $\beta = 3b$. Finalement, on a donc $(y+\sqrt{-13}) = (\mathfrak{c}'\mathfrak{p}^a\mathfrak{q}^b)^3$.

ii) La question précédente assure que le cube de l'idéal $\mathfrak{c}'\mathfrak{p}^a\mathfrak{q}^b$ est principal. Or la question f) assure que le groupe des classes est de cardinal 2, donc $\mathfrak{c}'\mathfrak{p}^a\mathfrak{q}^b$ lui-même est principal

iii) La question précédente assure qu'il existe $u, v \in \mathbb{Z}$ tels que $(y+\sqrt{-13}) = (u+u\sqrt{-13})^3$ (égalité d'idéaux). Quitte à changer le signe de u et v (voir question e)), on peut supposer que l'on a une égalité dans $\mathbb{Z}_K$: $(y+\sqrt{-13}) = (u+u\sqrt{-13})^3$. On développe le second membre et on identifie les deux écritures sur la base $(1, \sqrt{-13})$. On obtient les deux égalités suivantes : $u^3 - 39uv^2 = y$ et $v(3u^2 - 13v^2) = 1$.

iv) On déduit de la question précédente que $v = -1$ et que $u = \pm 2$. Alors on obtient finalement $y = \pm 70$, et $x^3 = y^2 + 13 = 4913 = 17^3$, donc $x = 17$. Finalement, on a démontré que les solutions de l'équation diophantienne considérée sont exactement les deux couples $(17, -70)$ et $(17, 70)$.

Exercice 5 : On considère le corps $K := \mathbb{Q}[\sqrt{-163}]$.

a) Calculer $\mathbb{Z}_K$, D_K et le polynôme minimal d'un générateur α de $\mathbb{Z}_K$.

b) Montrer que les idéaux premiers contenant 2, 3, 5 ou 7 sont principaux.

c) En déduire que $\mathbb{Z}_K$ est principal, donc factoriel.

d) Montrer que pour tout $a, b \in \mathbb{Z}$, $N_{K/\mathbb{Q}}(a+b\alpha) \geq 41$ si $b \neq 0$.

e) En déduire que pour tout $-39 \leq n \leq 40$, l'entier $n^2 - n + 41$ est premier.

Solution de l'exercice 5.

a) Puisque $-163 \equiv 1$ [4], on a $D_K = -163$ et $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, avec $\alpha := \frac{1+\sqrt{-163}}{2}$. Le polynôme minimal de α est $X^2 - X + 41$.

b) Montrons que pour $p = 2, 3, 5$ ou 7, l'idéal (p) de $\mathbb{Z}_K$ est maximal. Pour cela, il suffit de vérifier que la réduction de $X^2 - X + 41$ modulo p est irréductible, i.e. qu'elle n'a pas de racine, ce qui est immédiat. Donc les idéaux (p), avec $p = 2, 3, 5, 7$ sont maximaux, d'où le résultat.

c) Le résultat de Minkowski assure que toute classe d'idéaux admet un représentant entier de norme $\leq M(K)\sqrt{|D_K|} \approx 8,128 < 9$. Donc on va étudier tous les idéaux entiers de norme ≤ 8. Soit $\mathfrak{a}$ un idéal de $\mathbb{Z}_K$. On a $N(\mathfrak{a}) = 2$ si et seulement si $2 \in \mathfrak{a}$ et $N(\mathfrak{a}) = 2$. Or (2) est maximal de norme 4, donc il n'existe pas d'idéal de norme 2. De même, pour $p = 3, 5, 7$, (p) est maximal de norme p^2, donc il n'existe pas d'idéal de norme p. De même, il n'existe pas d'idéal entier de norme $6 = 2.3$. On a $N(\mathfrak{a}) = 4$ si et seulement si $\mathfrak{a} = (2)$. Il n'existe pas d'idéal entier de norme 8 puisque sinon il existerait un idéal de norme 2. Finalement, les seuls idéaux de norme ≤ 8 sont $\mathbb{Z}_K$ et (2). Ils sont tous les deux principaux, donc $h(K) = 1$, donc $\mathbb{Z}_K$ est principal.

d) Si $b \neq 0$, on a

$$N_{K/\mathbb{Q}}(a+b\alpha) = \left(a+\frac{b}{2}\right)^2 + 163\frac{b^2}{4} \geq \frac{163}{4} > 40\,.$$

Or $N_{K/\mathbb{Q}}(a+b\alpha) \in \mathbb{Z}$, donc $N_{K/\mathbb{Q}}(a+b\alpha) \geq 41$.

e) Soit $n \in \mathbb{Z}$, et p premier divisant n^2-n+41. Alors modulo p, le polynôme X^2-X+41 admet pour racine la classe de n modulo p. Donc le nombre premier p est soit ramifié, soit décomposé dans l'extension $K/\mathbb{Q}$, donc il existe un idéal premier $\mathfrak{p}$ divisant $p\mathbb{Z}_K$ tel que $N(\mathfrak{p}) = p$. Or $\mathfrak{p}$ est principal par la question c) : $\mathfrak{p} = (\beta)$, $\beta \in \mathbb{Z}_K$. Par la question d), on en déduit que $p = N_{K/\mathbb{Q}}(\beta) \geq 41$.

En particulier, si $n^2-n+41 < 41^2$ et si n^2-n+41 n'est pas premier, il admet un facteur premier $p < 41$, ce qui contredit les lignes précédentes. Donc si on a $n^2-n+41 < 41^2$, alors n^2-n+41 est premier.

Il suffit maintenant de résoudre l'inéquation suivante : $n^2-n+41 < 41^2$ si et seulement si $-40 < n < 41$ (il est clair que les cas d'égalité correspondent à $n = -40$ et $n = 41$). D'où le résultat.

Exercice 6 : L'objectif de cet exercice est de montrer ce que l'on appelle le "premier cas du théorème de Fermat", à savoir : pour un nombre premier impair p, si l'on note $K := \mathbb{Q}(\zeta_p)$ et si p ne divise pas $h(K)$, alors l'équation $X^p+Y^p=Z^p$ n'admet pas de solution $(x,y,z) \in \mathbb{Z}^3$ avec x, y et z premiers à p (i.e. pour toute solution $(x,y,z) \in \mathbb{Z}^3$, p divise xyz).
Pour cela, on raisonne par l'absurde et on suppose donc qu'il existe une solution $(x,y,z) \in \mathbb{Z}^3$ telle que p ne divise pas xyz.

a) Montrer que l'on peut supposer x, y et z premiers entre eux dans leur ensemble.

b) Si $p=3$ ou $p=5$, conclure en réduisant l'équation modulo p^2.

c) On suppose désormais $p > 5$. Montrer que l'on peut supposer que p ne divise pas $x-y$.
[Indication : montrer qu'il n'est pas possible d'avoir $x \equiv y \equiv -z$ $[p]$.]

d) Montrer que $z^p = \prod_{i=0}^{p-1}(x+\zeta_p^i y)$.

e) Décomposer l'idéal $p\mathbb{Z}_K$ en idéaux premiers. Plus précisément, montrer qu'il existe un idéal premier $\mathfrak{p}$ de $\mathbb{Z}_K$ tel que $p\mathbb{Z}_K = \mathfrak{p}^{p-1}$.

f) Montrer en outre que pour tout $1 \leq i \leq p-1$, $\mathfrak{p} = (1-\zeta_p^i)\mathbb{Z}_K$.

g) Montrer que les idéaux $(x+\zeta_p^i y)$ (pour $1 \leq i \leq p-1$) sont deux-à-deux premiers entre eux.
[Indication : on pourra raisonner par l'absurde et montrer qu'alors $x+y \in \mathfrak{p}$.]

h) Montrer que pour tout $1 \leq i \leq p-1$, il existe un idéal $\mathfrak{a}_i$ de $\mathbb{Z}_K$ tel que $(x+\zeta_p^i y)\mathbb{Z}_K = \mathfrak{a}_i^p$.

i) Montrer que pour tout $1 \leq i \leq p-1$, l'idéal $\mathfrak{a}_i$ est principal, engendré par $\alpha_i \in \mathbb{Z}_K$.

j) Montrer que pour tout $\alpha \in \mathbb{Z}_K$, $\alpha^p \in \mathbb{Z} + p\mathbb{Z}_K$.

k) En déduire qu'il existe $r \in \mathbb{Z}$ tel que $x+\zeta_p y - \zeta_p^{2r}x - \zeta_p^{2r-1}y \equiv 0$ $[p]$.
[Indication : on pourra utiliser la description de $\mathbb{Z}_K^*$ obtenue à l'exercice 2 de la feuille de TD9.]

l) En déduire que si les quatre nombres $1, \zeta_p, \zeta_p^{2r-1}, \zeta_p^{2r}$ sont distincts, alors x et y sont divisibles par p.

m) Montrer que dans le cas contraire, soit $p|y$, soit $p|x-y$, soit $p|x$.

n) Conclure.

Solution de l'exercice 6.

a) Si $d \in \mathbb{Z}$ divise x, y et z, alors le triplet $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ est solution de la même équation. Donc en divisant la solution initiale par le PGCD de (x,y,z), on peut supposer que x, y et z sont premiers entre eux.

b) Puisque si $x \equiv y\ [p]$, alors $x^p \equiv y^p\ [p^2]$, on connaît facilement les puissances p-ièmes dans $\mathbb{Z}/p^2\mathbb{Z}$, pour $p = 3$ ou 5. On trouve que les puissances p-ièmes modulo p^2 sont 1 et -1 (si $p = 3$) ou 1, -1, 7 et -7 (si $p = 5$). Il est alors clair que la somme de trois de ces classes modulo p^2 ne peut être nulle, on a donc une contradiction.

c) Supposons que $x \equiv y \equiv -z\ [p]$. Alors l'égalité $x^p + y^p + (-z)^p = 0$ devient $3x^p = 0$. Or par hypothèse p ne divise par x, donc p divise 3, ce qui contredit l'hypothèse $p > 5$. Donc l'une des deux congruences $x \equiv y\ [p]$ ou $x \equiv -z\ [p]$ n'est pas vérifiée. Donc si p divise $x - y$, alors p ne divise pas $x + z$. Donc quitte à remplacer y par $-z$ et z par $-y$, on peut supposer que p ne divise pas $x - y$.

d) On a $\left(\frac{z}{y}\right)^p = \left(\frac{x}{y}\right)^p + 1$. Or le polynôme $X^p + 1$ se décompose sous la forme $X^p + 1 = \prod_{i=0}^{p-1}(X + \zeta_p^i)$. On applique cette identité à $X = \frac{x}{y}$ et on obtient $\left(\frac{z}{y}\right)^p = \prod_{i=0}^{p-1}\left(\frac{x}{y} + \zeta_p^i\right)$. En multipliant les deux membres par y^p, il reste $z^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y)$.

e) On a montré à l'exercice 13 de la feuille de TD8 que $p \in (\lambda)^{p-1}$, avec $\lambda := 1 - \zeta_p$. Or on sait que l'idéal $\mathfrak{p} = (\lambda)$ est premier de norme p, donc un calcul de norme assure que $p\mathbb{Z}_K = \mathfrak{p}^{p-1}$.

f) Il est clair que les $1 - \zeta_p^i$ (pour $1 \leq i \leq p-1$) engendrent le même idéal $\mathfrak{p}$ puisque $\frac{1-\zeta_p^i}{1-\zeta_p}$ est une unité de $\mathbb{Z}_K$.

g) Soit $\mathfrak{q}$ un idéal premier divisant $(x + \zeta_p^i y)$ et $(x + \zeta_p^j y)$, pour $0 \leq i \neq j \leq p-1$. Alors $\mathfrak{q}$ divise $((\zeta_p^i - \zeta_p^j)y) = \mathfrak{p}(y)$ et $((\zeta_p^j - \zeta_p^i)x) = \mathfrak{p}(x)$. Or x et y sont premiers entre eux (dans $\mathbb{Z}$), donc les idéaux (x) et (y) n'ont pas de facteur premier en commun, donc $\mathfrak{q}$ divise $\mathfrak{p}$, donc $\mathfrak{q} = \mathfrak{p}$ par maximalité. Donc $x + y \equiv x + \zeta_p^i y \equiv 0 \pmod{\mathfrak{p}}$, donc $x + y \in \mathfrak{p} \cap \mathbb{Z} = (p)$. Or $z^p \equiv x^p + y^p \equiv x + y \equiv 0\ [p]$, donc p divise z. Ceci contredit l'hypothèse initiale, donc $(x + \zeta_p^i y)$ et $(x + \zeta_p^j y)$ n'ont pas de facteur commun.

h) La question d) assure que l'on a l'égalité suivante entre idéaux : $(z)^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y)$. Or les idéaux du second membre sont deux-à-deux premiers entre eux, donc l'unicité de la décomposition en idéaux premiers assure qu'il existe des idéaux $\mathfrak{a}_i$ tels que $(x + \zeta_p^i y) = \mathfrak{a}_i^p$ pour tout i.

i) On a, d'après la question h), l'égalité suivante pour tout i : ${\mathfrak{a}_\mathfrak{i}}^p = (x + \zeta_p^i y)$. Donc l'idéal $\mathfrak{a}_i$ devient principal quand on l'élève à la puissance p. Or par hypothèse p est premier au nombre de classes de K, donc $\mathfrak{a}_i$ lui-même est principal : il existe $\alpha_i \in \mathbb{Z}_K$ tel que $\mathfrak{a}_i = (\alpha_i)$.

j) Soit $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathbb{Z}_K$. Alors on développe avec la formule du multinôme de Newton : on obtient $\alpha^p = (a_0^p + a_1^p + \cdots + a_{p-2}^p) + p\beta$, avec $\beta \in \mathbb{Z}_K$. Donc clairement $\alpha^p \in \mathbb{Z} + p\mathbb{Z}_K$.

k) Les questions i) et j) assurent qu'il existe $u \in \mathbb{Z}_K^*$ et $a \in \mathbb{Z}$ tels que $x + \zeta_p y = u\alpha_1^p$ et $\alpha_1^p \equiv a \pmod{p\mathbb{Z}_K}$. Par l'exercice 2 de la feuille de TD9, on peut écrire u sous la forme $u = \zeta_p^r v$, avec $v \in \mathbb{Z}_K^*$ tel que $\overline{v} = v$. Alors on en déduit que $x + \zeta_p y \equiv \zeta_p^r va \pmod{p\mathbb{Z}_K}$ et $x + \overline{\zeta_p} y \equiv \zeta_p^{-r} va \pmod{p\mathbb{Z}_K}$. Donc en combinant ces deux congruences, on obtient $\zeta_p^{2r}(x + \zeta_p^{-1} y) \equiv x + \zeta_p y \pmod{p\mathbb{Z}_K}$. Donc finalement $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0\ [p]$.

l) On suppose que les quatre nombres en question sont deux-à-deux distincts. Alors la famille des quatre vecteurs $(1, \zeta_p, \zeta_p^{2r}, \zeta_p^{2r-1})$ se complète en une base de $\mathbb{Z}_K$ (puisque $p > 5$), donc la question k) assure que p divise x et y.

m) Si les quatre nombres ne sont pas deux-à-deux distincts, trois cas se présentent :
- soit $\zeta_p^{2r} = 1$, auquel cas $(\zeta_p - \zeta_p^{-1})y \equiv 0\ [p]$. Or (ζ_p, ζ_p^{-1}) se complète en une base de $\mathbb{Z}_K$, donc p divise y.
- soit $\zeta_p^{2r-1} = 1$, alors $(x - y) - (x - y)\zeta_p \equiv 0\ [p]$, donc comme dans le cas précédent, p divise $x - y$.
- soit $\zeta_p = \zeta_p^{2r-1}$, alors $x - \zeta_p^2 x \equiv 0\ [p]$, donc comme précédemment p divise x.

n) Les questions l) et m) assurent que p divise x, y ou $x - y$, ce qui contredit soit l'hypothèse initiale, soit la question c). Donc finalement il n'existe pas de solution (x, y, z) telle que p ne divise pas xyz.

o) Remarque : en utilisant ce résultat et des techniques analogues, on peut montrer ensuite qu'il n'existe pas de solution entière du tout (toujours sous l'hypothèse sur le nombre de classes).

La condition sur le nombre de classes est vérifiée par tous les nombres premiers ≤ 100, sauf 37, 59 et 67. On ne sait pas montrer qu'il y a une infinité de nombres premiers vérifiant cette condition sur le nombre de classes (on les appelle les nombres premiers réguliers). On conjecture cependant qu'environ 61 % des nombres premiers sont réguliers.