Université Paris Cité (Diderot Paris 7)

Cours d'arithmétique (M1), janvier-avril 2026

Feuille TD3 : Anneaux d'entiers

Sommes de carrés.

Exercice 1.

1. Quels entiers sont sommes de deux carrés ? Savez-vous le démontrer ?
2. Soit p un nombre premier. Combien de couples $(x, y) \in \mathbb{Z}^2$ y a-t'il tels que $p = x^2 + y^2$?
3. Soit n un entier strictement positif. On écrit $n = 2^\alpha n_1 n_2$ de sorte que tous les facteurs premiers de n_1 sont congrus à 1 modulo 4 et ceux de n_2 sont congrus à 3 modulo 4. Soit $r(n)$ le nombre de solutions entières de l'équation $n = x^2 + y^2$.
   (a) Montrer que, si n_2 est un carré parfait, alors $r(n) = 4d(n_1)$, où $d(n_1)$ désigne le nombre de diviseurs positifs de n_1. On pourra décomposer n en produit d'irréductibles dans $\mathbb{Z}[i]$.
   (b) Que vaut $r(n)$ si n_2 n'est pas un carré parfait ?

Exercice 2. Dans cet exercice, on cherche à déterminer ques entiers naturels n s'écrivent sous la forme $a^2 - ab + b^2$ avec $a, b \in \mathbb{Z}$. Pour ce faire, on commence par étudier l'anneau des entiers d'Eisenstein $\mathbb{Z}[j]$, avec $j = e^{2i\pi/3}$.

1. Montrer que l'anneau $\mathbb{Z}[j]$ est principal. Quelles sont ses unités ?
2. Soit p un nombre premier différent de 3. Montrer que les assertions suivantes sont équivalentes :
   (a) p n'est pas irréductible dans $\mathbb{Z}[j]$.
   (b) Il existe $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 - ab + b^2$.
   (c) Le polynôme $X^3 - 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$ autre que 1.
   (d) p est congru à 1 modulo 3.
3. L'élément 3 est-il irréductible dans $\mathbb{Z}[j]$?
4. (a) Montrer que tout irréductible de $\mathbb{Z}[j]$ divise un unique nombre premier de $\mathbb{Z}$.
   (b) En déduire la liste des éléments irréductibles de $\mathbb{Z}[j]$
5. Déterminer quels entiers naturels n s'écrivent sous la forme $a^2 - ab + b^2$ avec $a, b \in \mathbb{Z}$.

Équations diophantiennes.

Exercice 3.

1. Soit $r \geq 2$. Soit a_1, …, a_k des éléments d'un anneau factoriel A qui sont premiers entre eux deux à deux. On suppose que $a_1 \dots a_k = b^r$ pour un certain $b \in A$. Montrer que chaque a_i s'écrit $\pm b_i^r$ avec $b_i \in A$.
2. Trouver toutes les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation :

$$y^2 + 4 = x^3.$$

Exercice 4. On considère l'anneau $A = \mathbb{Z}[i\sqrt{2}]$. Montrer que A est un anneau euclidien et en déduire les solutions entières de l'équation $y^2 + 2 = x^3$.

Exercice 5. Supposons qu'il existe des éléments non nuls x, y, z dans A tels que

$$x^3 + y^3 = z^3,$$

et posons $A = \mathbb{Z}[j]$. On note $N : w \mapsto w\overline{w}$ la norme usuelle. On pourra utiliser librement l'exercice 2.

1. Montrer que l'on peut supposer x, y, z premiers entre eux, ce que l'on suppose dans la suite.
2. Montrer que tout élément de A est congru à $0, 1$ ou -1 modulo $\theta := i\sqrt{3}$.
3. Soit ξ et η dans A non divisibles par θ. Montrer que

$$\begin{aligned} \xi \equiv 1 \mod \theta &\implies \xi^3 \equiv 1 \mod 9 \\ \xi \equiv -1 \mod \theta &\implies \xi^3 \equiv -1 \mod 9 \\ \xi^3 + \eta^3 \equiv 0 \mod \theta &\implies \xi^3 + \eta^3 \equiv 0 \mod 9 \\ \xi^3 - \eta^3 \equiv 0 \mod \theta &\implies \xi^3 + \eta^3 \equiv 0 \mod 9 \end{aligned}$$

4. Montrer que θ divise et et un seul des entiers x, y, z.
5. On suppose qu'il existe x, y, z dans A tels que θ ne divise pas xyz, des unités ϵ_1, ϵ_2 et un entier $r > 0$ tels que
$$x^3 + \epsilon_1 y^3 + \epsilon_2(\theta^r z)^3 = 0.$$
Montrer que $\epsilon_1 = \pm 1$ et $r \geq 2$.
6. Considérons x, y, z non nuls dans A vérifiant $x^3 + y^3 + \epsilon(\theta^r z)^3 = 0$, avec $r \geq 2$, ϵ une unité de A et θ ne divisant pas xyz. Supposons que $N(x^3y^3z^3\theta^{3r})$ soit minimale dans $\mathbb{Z}$. Obtenir une contradiction en construisant un autre triplet (x', y', z') de norme strictement plus petite et conclure.

Anneaux d'entiers algébriques.

Notations : Soit K un corps de nombres. Si $(x_1, \ldots, x_n) \in \mathcal{O}_K^n$ est une $\mathbb{Q}$-base de K, on note $d(x_1, \ldots, x_n)$ son discriminant. Si $(x_1, \ldots, x_n)$ est en fait une $\mathbb{Z}$-base de $\mathcal{O}_K$, l'entier $d(x_1, \ldots, x_n)$ est appelé discriminant de K et noté Δ_K.

Exercice 6. Parmi les nombres suivants, lesquels sont des entiers algébriques ?

$$\frac{8 + 2\sqrt{13}}{1 + \sqrt{13}}, \quad \frac{6 + 3\sqrt{7}}{5 + \sqrt{7}}, \quad \sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}, \quad \frac{-23 + 2\sqrt[3]{6} - 2\sqrt[3]{36}}{1 + 2\sqrt[3]{6}}, \quad \frac{1 + \sqrt[3]{5} + \sqrt[3]{25}}{2}.$$

Exercice 7. Soit z un nombre algébrique. Montrer qu'il existe un entier $n \geq 1$ tel que nz est un entier algébrique.

Exercice 8. Soit K un corps de nombres.

1. Montrer que :
$$\mathcal{O}_K^\times = \{x \in \mathcal{O}_K : N_{K/\mathbb{Q}}(x) = \pm 1\}.$$
2. Calculer $\mathcal{O}_K^\times$ lorsque $K = \mathbb{Q}(\sqrt{D})$ avec $D < 0$ entier sans facteurs carrés.

Exercice 9. Soit $D < 0$ un entier sans facteurs carrés. On rappelle qu'un anneau intègre A est euclidien s'il existe une application $\phi : A \setminus \{0\} \to \mathbb{N}$, telle que pour tout $a \in A$, $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\phi(r) < \phi(b)$.

1. Montrer que $\mathcal{O}_K$ est euclidien pour $D = -1, -2, -3, -7, -11$.

2. Montrer que si $\mathcal{O}_K$ est euclidien par rapport à ϕ, un élément b non inversible, tel que $\phi(b)$ soit minimal (parmi les non inversibles) vérifie l'assertion suivante : le quotient A/bA s'injecte (comme ensemble) dans $\mathcal{O}_K^\times \cup \{0\}$. Si $-D < -3$, en déduire que $N_{K/\mathbb{Q}}(b) = 2$ ou 3.
3. Pour quelles valeur de D existe-t-il $b \in \mathcal{O}_K$ tel que $N_{K/\mathbb{Q}}(b) = 2$ ou 3 ?
4. Conclure que les seuls anneaux d'entiers quadratiques imaginaires qui sont euclidiens sont ceux de la question 1.

Exercice 10.

1. Soit $z \in \mathbb{C}$ un entier algébrique de degré n. On pose $K = \mathbb{Q}(z)$ et on suppose que le discriminant de la base $(1, z, z^2, \ldots, z^{n-1})$ n'a pas de facteurs carrés. Montrer que $\mathcal{O}_K = \mathbb{Z}[z]$.
2. Soit $z \in \mathbb{C}$ tel que $z^3 - z + 1 = 0$. Soit $K := \mathbb{Q}(z)$. Montrer que $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}z \oplus \mathbb{Z}z^2$.
3. Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Montrer que $[K : \mathbb{Q}] = 4$ et que $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}, \frac{1+\sqrt{5}}{2}]$.

Exercice 11. Soit $z \in \mathbb{C}$ tel que $z^3 - z - 4 = 0$. Soit $K := \mathbb{Q}(z)$. Montrer que $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}z \oplus \mathbb{Z}\frac{z+z^2}{2}$.

Exercice 12. Soient $m, n \in \mathbb{Z} \setminus \{0, 1\}$ des entiers distincts, sans facteur carré, et tels que $m \equiv n \equiv 1 \mod 4$. On se propose de montrer que, si $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, alors $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\alpha\beta$ avec $\alpha = \frac{1+\sqrt{n}}{2}$ et $\beta = \frac{1+\sqrt{m}}{2}$.

1. Montrer que $[K : \mathbb{Q}] = 4$ et déterminer l'ensemble des plongements de K dans $\mathbb{C}$.
2. Vérifier que $d(1, \alpha, \beta, \alpha\beta) = m^2n^2$.
3. Montrer que :

$$\mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\alpha\beta \subset \mathcal{O}_K \subset \frac{1}{4}\left(\mathbb{Z} \oplus \mathbb{Z}\sqrt{n} \oplus \mathbb{Z}\sqrt{m} \oplus \mathbb{Z}\sqrt{mn}\right).$$

   On pourra utiliser les traces sur $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ et $\mathbb{Q}(\sqrt{mn})$.
4. Conclure.

Exercice 13. Soient $m, n \in \mathbb{Z} \setminus \{0, 1\}$ des entiers distincts, sans facteur carré, et tels que $m \equiv n \equiv 1 \mod 4$. On se propose de montrer que, si $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, alors il n'existe pas d'élément $x \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[x]$.

1. Exhiber un idéal I de $\mathbb{Z}[X, Y]$ tel que $\mathcal{O}_K \cong \mathbb{Z}[X, Y]/I$.
2. Faire la liste des idéaux $\mathfrak{m}$ de $\mathcal{O}_K$ tels que $\mathcal{O}_K/\mathfrak{m} \cong \mathbb{Z}/2\mathbb{Z}$.
3. Conclure.

Exercice 14. Soient $n \geq 3$ et $a, b \in \mathbb{Q}$ tels que $P := X^n + aX + b$ est irréductible dans $\mathbb{Q}[X]$. Soient $z \in \mathbb{C}$ une racine de P et $K = \mathbb{Q}(z)$. Calculer $d(1, z, z^2, \ldots, z^{n-1})$.

Exercice 15. Soit K un corps de nombres de degré n, et soit $u \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(u)$. Soit p un nombre premier tel que le polynôme minimal de u sur $\mathbb{Q}$ soit d'Eisenstein en p. L'objectif de l'exercice est de montrer que p ne divise pas l'indice de $\mathbb{Z}[u]$ dans $\mathcal{O}_K$.

1. Montrer que $\frac{u^n}{p} \in \mathcal{O}_K$ et que p^2 ne divise pas $N_{K/\mathbb{Q}}(u)$.
2. Supposons que $p | [\mathcal{O}_K : \mathbb{Z}[u]]$.
   (a) Montrer qu'il existe $x \in \mathcal{O}_K \setminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$. En déduire qu'il existe $b_0, ..., b_{n-1} \in \mathbb{Z}$ non tous divisibles par p tels que $x = \frac{b_0 + ... + b_{n-1}u^{n-1}}{p}$.
   (b) Notons r le plus petit entier tel que b_r n'est pas divisible par p. Montrer que $y = \frac{b_r u^r + ... + b_{n-1}u^{n-1}}{p}$ est dans $\mathcal{O}_K$.
   (c) Montrer que $z = \frac{b_r u^{n-1}}{p} \in \mathcal{O}_K$.

(d) Obtenir une contradiction en calculant la norme de z.

3. Soit q est une puissance de p.
   (a) Montrer que, si $K = \mathbb{Q}(\sqrt[q]{p})$, alors $\mathcal{O}_K = \mathbb{Z}[\sqrt[q]{p}]$.
   (b) Soit ζ une racine primitive q-ième de l'unité. Montrer que, si $K = \mathbb{Q}(\zeta)$, alors $\mathcal{O}_K = \mathbb{Z}[\zeta]$.
4. Montrer que, si $K = \mathbb{Q}(\sqrt[3]{2})$, alors $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

Exercice 16. Soient p un nombre premier et $k \geq 1$ un entier. Soit $\zeta \in \mathbb{C}$ une racine primitive p^k-ème de l'unité. Soit $\mathcal{O}_{p^k}$ l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$. Nous allons établir par une méthode différente de celle de l'exercice 15 que $\mathcal{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

1. Montrer l'identité $p = \prod_{\substack{r=1 \\ p \nmid r}}^{p^k} (1 - \zeta^r)$.
2. En déduire que $(\zeta - 1)\mathcal{O}_{p^k} \cap \mathbb{Z} = p\mathbb{Z}$.

Supposons $k = 1$.

3. En utilisant la trace, montrer que l'anneau $\mathcal{O}_p$ est égal à $\mathbb{Z}[\zeta]$.

Revenons au cas général $k \geq 1$.

4. Montrer que l'on a $\mathcal{O}_{p^k} = \mathbb{Z}[\zeta] + p^m \mathcal{O}_{p^k}$ pour tout $m \geq 0$.
5. Montrer que le discriminant de $(1, \zeta, \ldots, \zeta^{\varphi(p^k)-1})$ est, au signe près, une puissance de p (que l'on explicitera).
6. En déduire que l'anneau $\mathcal{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

Exercice 17. Soient K et L des extensions finies galoisiennes de $\mathbb{Q}$ de degrés respectifs m et n. On suppose que K et L sont linéairement disjointes, c'est-à-dire que $K \cap L = \mathbb{Q}$

1. Montrer que l'extension composée KL de $\mathbb{Q}$ est galoisienne finie.
2. Montrer que la restriction induit un isomorphisme de groupes $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/\mathbb{Q})$.
3. Montrer que l'application canonique $\mathrm{Gal}(KL/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ est un isomorphisme de groupes.

Soit maintenant $(x_1, \ldots, x_m)$ (resp. $(y_1, \ldots, y_n)$) une base de K (resp. L) telle que :

$$\mathcal{O}_K = \bigoplus_{i=1}^{m} \mathbb{Z}x_i \quad (\text{resp. } \mathcal{O}_L = \bigoplus_{i=1}^{n} \mathbb{Z}y_i).$$

On suppose que $\Delta_K \wedge \Delta_L = 1$.

4) Montrer que $\Delta_K \mathcal{O}_{KL} \subset \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathbb{Z}x_i y_j$.
5) Montrer que $\mathcal{O}_{KL} = \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{m} \mathbb{Z}x_i y_j$.
6) Calculer $d((x_i y_j)_{1 \leq i \leq m, 1 \leq j \leq n})$.
7) Soient $n \geq 3$ un entier et $\zeta \in \mathbb{C}$ une racine primitive n-ième de l'unité. Calculer l'anneau des entiers de $\mathbb{Q}(\zeta)$. On pourra pour cela utiliser le résultat de l'exercice 15 ou 16.

Exercice 18. Soit $d \in \mathbb{Z}$, $d > 1$ sans facteur cubique. Notons $\theta = \sqrt[3]{d}$ et $K = \mathbb{Q}(\theta)$. On cherche à déterminer l'anneau des entiers $\mathcal{O}_K$ de K.

1. Montrer que la base $(1, \theta, \theta^2)$ est de discriminant $\Delta = -27d^2$.
2. On écrit $d = ab^2$, avec $a, b \in \mathbb{N}$ sans facteur carré. On pose $\theta' = \sqrt[3]{a^2 b}$. Montrer que $K = \mathbb{Q}(\theta')$ et calculer le discriminant Δ' de la base $(1, \theta', \theta'^2)$.
3. Montrer que $(1, \theta, \theta')$ est une $\mathbb{Q}$-base de K et calculer son discriminant Δ''.

4. On note f, f' et f'' les indices respectifs de $\mathbb{Z}[\theta]$, $\mathbb{Z}[\theta']$ et $\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta'$ dans $\mathcal{O}_K$. On note Δ_K le discriminant de K.
   (a) Montrer que $f^2 = \frac{\Delta}{\Delta_K}$, $f'^2 = \frac{\Delta'}{\Delta_K}$ et $f''^2 = \frac{\Delta''}{\Delta_K}$.
   (b) Montrer que $a \wedge f = 1$ et que $b \wedge f' = 1$.
   (c) En déduire les assertions suivantes :
      i. $\Delta_K < 0$;
      (ii) $a^2b^2 | \Delta_K | 27a^2b^2$;
      (iii) si $3|a$, alors $27a^2 | \Delta_K$;
      (iv) si $3|b$, alors $27b^2 | \Delta_K$.
5. Montrer que si $3|d$, alors $\Delta_K = -27a^2b^2$ et $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta'$.
6. Supposons que 3 ne divise pas d et que $d \pm 1$ n'est pas multiple de 9. Montrer que le polynôme minimal de $\theta - d$ est 3-Eisenstein. En procédant comme dans les questions précédentes, en déduire que $\Delta_K = -27a^2b^2$ et $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta'$.
7. On suppose $d \equiv 1 \mod 9$. On pose $\alpha = \frac{1+\theta+\theta^2}{3}$.
   (a) Montrer que $\alpha \in \mathcal{O}_K$ et calculer son polynôme minimal.
   (b) En déduire que $3|f''$, puis que $\Delta_K = -3a^2b^2$.
   (c) Montrer que $\mathcal{O}_K = \mathbb{Z}\alpha \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta'$.
8. Supposons $d \equiv -1 \mod 9$. On pose $\alpha' = \frac{1-\theta+\theta^2}{3}$. Montrer que $\mathcal{O}_K = \mathbb{Z}\alpha' \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta'$.

Exercice 19. Pour $n \in \mathbb{N}$, on note $\mathbb{Q}_n[X]$ le $\mathbb{Q}$-espace vectoriel des polynômes de degré strictement plus petit que n. On appellera base canonique de $\mathbb{Q}_n[X]$ la base $(X^{n-1}, X^{n-2}, ..., 1)$. Pour $(P, Q) \in \mathbb{Q}[X] \times \mathbb{Q}[X]$ avec $\deg P = n$ et $\deg Q = m$, on note $\mathrm{Res}(P, Q)$ le déterminant dans les bases canoniques de l'application $\mathbb{Q}$-linéaire $\mathbb{Q}_m[X] \times \mathbb{Q}_n[X] \to \mathbb{Q}_{m+n}[X]$ qui envoie (U, V) sur $PU + QV$.

1. Écrire $\mathrm{Res}(P, Q)$ comme déterminant d'une matrice.
2. Comparer $\mathrm{Res}(P, Q)$ et $\mathrm{Res}(Q, P)$.
3. On suppose que P est un polynôme unitaire.
   (a) Montrer que $\mathrm{Res}(P, Q)$ est égal au déterminant de la multiplication par Q sur l'anneau $A[X]/(P)$ dans la base $(X^{n-1}, X^{n-2}, ..., 1)$.
   (b) Considérons $Q_1 \in A[X]$ et $Q_2 \in A[X]$ de degrés respectifs m_1 et m_2. Calculer $\mathrm{Res}(P, Q_1Q_2)$ en fonction de $\mathrm{Res}(P, Q_1)$ et $\mathrm{Res}(P, Q_2)$.
   (c) Exprimer $\mathrm{Res}(P, (X - \lambda_1)...(X - \lambda_m))$ en fonction de $P(\lambda_1)...P(\lambda_m)$.
   (d) Soit x un nombre algébrique de degré n. On pose $K = \mathbb{Q}(x)$. Exprimer $d(1, x, x^2, \ldots, x^{n-1})$ en fonction des coefficients du polynôme minimal μ_x de x.

Exercice 20. Soit K un corps de nombres. Soit Δ_K son discriminant. Les deux questions suivantes sont indépendantes.

1. Montrer le signe de Δ_K est $(-1)^s$ où s est le nombre d'éléments dans $\Sigma_{\mathbb{C}}$ (c'est-à-dire la moitié du nombre de plongements de K dans $\mathbb{C}$ dont l'image n'est pas contenue dans $\mathbb{R}$).
2. Montrer que Δ_K est congru à 0 ou 1 modulo 4.