Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 4, 13 Mars 2020

Notations et conventions.

- Pour chaque $n > 1$, μ_n, respectivement μ_n', note l'ensemble des racines de l'unité en $\mathbb{C}$, respectivement les racines primitives.
- Si K est un corps de nombres, $\mathfrak{O}_K$ désigne son anneau d'entiers.
- Si K est un corps de nombres, Δ_K note *le* discriminant de K. Il s'agit d'un entier.
- Si K est un corps de nombres, un idéal premier de K est un idéal premier de $\mathfrak{O}_K$. Son corps résiduel $\mathfrak{O}_K/\mathfrak{p}$ sera noté $\mathbb{F}_\mathfrak{p}$.

Détermination des anneaux d'entiers

Exercice 1. Soient p un nombre premier, $q = p^m$ et K le corps de nombres $\mathbb{Q}(\theta)$ où $\theta = \sqrt[q]{p}$. Montrer que $\mathfrak{O}_K = \mathbb{Z}[\theta]$.

Exercice 2. Soit $K = \mathbb{Q}(\mathrm{i}, \sqrt{2})$. En utilisant un corps cyclotomique et l'exercice 3, déterminer le discriminant de K. Ensuite, montrer que $\mathscr{B} = \left\{1, \mathrm{i}, \sqrt{2}, \dfrac{\sqrt{2} + \mathrm{i}\sqrt{2}}{2}\right\}$ est base entière de $\mathfrak{O}_K$.

Exercice 3. Soient p un nombre premier, $q > 1$ une puissance de p, ζ une racine primitive q-ème de l'unité et K le corps de nombres $\mathbb{Q}(\zeta)$. Montrer que $\mathscr{B} = \{1, \zeta, \ldots, \zeta^{\varphi(q)-1}\}$ est une base entière de $\mathfrak{O}_K$ et calculer ensuite, à signe près, Δ_K.

Exercice 4 (Extensions monogènes cubiques)**.** Soient $m > 0$ un entier qui n'est pas un cube, $\theta = \sqrt[3]{m}$ et $K = \mathbb{Q}(\theta)$.

1/ Soit $\mathscr{B} = \{1, \theta, \theta^2\}$. Calculer $\Delta_K(\mathscr{B})$.

2/ On suppose désormais que m *n'a pas de facteur carré et* $m \not\equiv \pm 1 \mod 9$. Montrer que $\mathscr{B}$ est une base entière de $\mathfrak{O}_K$ et en particulier $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Indication : Si $3 \nmid m$, on considère $\mathbb{Z}[\sigma]$, où $\sigma = \theta - m$.

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 5, 17 Mars 2020

Notations et conventions.

- Pour chaque $n > 1$, $\boldsymbol{\mu}_n$, respectivement $\boldsymbol{\mu}'_n$, note l'ensemble des racines de l'unité en $\mathbb{C}$, respectivement les racines primitives.
- Si K est un corps de nombres, $\mathfrak{O}_K$ désigne son anneau d'entiers.
- Si K est un corps de nombres, Δ_K note *le* discriminant de K. Il s'agit d'un entier.
- Si K est un corps de nombres, un idéal premier de K est un idéal premier de $\mathfrak{O}_K$. Son corps résiduel $\mathfrak{O}_K/\mathfrak{p}$ sera noté $\mathbb{F}_\mathfrak{p}$.

Calcul d'anneaux d'entiers

Exercice 1 (Une extension non-monogène)**.** Soient $0 < m < n$ des nombres naturels sans facteur carré, $x = \sqrt[3]{m^2 n}$ et $K = \mathbb{Q}(x)$.

1/ Montrer que $y = \sqrt[3]{mn^2} \in \mathfrak{O}_K$ et que $\mathscr{B} = \{1, x, y\}$ est une base de K. Ensuite calculer $\Delta_K(\mathscr{B})$.

2/ Pour chaque $\alpha = a + bx + cy \in K$, calculer $\mathrm{N}_K(\alpha)$ et $\mathrm{Tr}_K(\alpha)$.

On suppose maintenant que mn n'a pas de facteur carré et n'est pas divisible par 3.

3/ Soit G le groupe quotient $\mathfrak{O}_K/\mathbb{Z} + \mathbb{Z}x + \mathbb{Z}y$. Montrer que son ordre est une puissance de 3.

4/ En supposant $m = 5$ et $n = 7$, montrer que $\mathscr{B}$ est une base entière. (Il est possible de traiter des cas plus généraux que ceci.)

5/ Soit $\theta = bx + cy$ avec $b, c \in \mathbb{Z}$. Calculer le quotient $\lambda := \dfrac{\Delta_K(1, \theta, \theta^2)}{\Delta_K(1, x, y)}$. En étudiant λ modulo 7, montrer que $\{1, \theta, \theta^2\}$ ne peut pas être une base entière de $\mathfrak{O}_K$.

6/ Soit $\theta = a + bx + cy$ avec $a, b, c \in \mathbb{Z}$. Montrer que si $\{1, \theta, \theta^2\}$ est base entière de $\mathfrak{O}_K$ et $\sigma = \theta - a$, alors $\{1, \sigma, \sigma^2\}$ est aussi base entière de $\mathfrak{O}_K$. Déduire que l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{175})$ n'est pas de la forme $\mathbb{Z}[\theta]$.

Premiers décomposés, inertes et ramifiés

Exercice 2 (Vocabulaire)**.** Soit p un nombre premier et soient $K \subset L$ des corps de nombres. Montrer les implications suivantes :

1/ Si p ramifie en K alors il ramifie en L.

2/ Si p se décompose totalement en L, alors il se décompose totalement en K.

3/ Si p est inerte en L alors il est inerte en K aussi.

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 6, 20 mars 2020

Premiers inertes, ramifies et totalement décomposés

- Pour chaque $n > 1$, μ_n, resp. μ_n', note l'ensemble des racines de l'unité en $\mathbb{C}$, resp. les racines primitives.
- Si K est un corps de nombres, Δ_K note *le* discriminant de K. Il s'agit d'un entier.
- Si K est un corps de nombres, un idéal premier de K est un idéal premier de $\mathfrak{O}_K$. Son corps résiduel $\mathfrak{O}_K/\mathfrak{p}$ sera noté $\mathbb{F}_\mathfrak{p}$.

Exercice 1. Soit $m \in \mathbb{Z} \smallsetminus \{0, 1\}$ un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{m})$. Le discriminant de K sera noté par d dans la suite.

1/ Rappeler le lien entre d et m. En déduire que d détermine K uniquement.

2/ L'entier d est soit $\equiv 0$, soit $\equiv 1$ modulo 4. Justifier.

3/ En écrivant $\delta = \dfrac{d + \sqrt{d}}{2}$, montrer que $\{1, \delta\}$ est toujours une base entière de $\mathfrak{O}_K$.

4/ Soit p un nombre premier. Exprimer $\mathfrak{O}_K/(p)$ comme $\mathbb{F}_p[X]/(f(X))$, où f est un polynôme unitaire.

On fixe $p > 2$ un nombre premier.

5/ Soit $F = X^2 + bX + c \in \mathbb{F}_p[X]$ et $\Delta = b^2 - 4c$. Montrer que si $\Delta = 0$ si et seulement si F est le carré d'un polynôme de degré 1. Montrer que $\Delta \neq 0$ et est un carré de $\mathbb{F}_p^*$ si et seulement si F est le produit de deux polynômes linéaires distincts. Montrer que si Δ n'est pas un carré si et seulement si F est irréductible. (Dit autrement, sur $\mathbb{F}_p[X]$ la théorie "marche" comme sur $\mathbb{R}[X]$.)

6/ Montrer que p ramifie en K si et seulement si $p \mid d$.

7/ Montrer que p se décompose en K si et seulement si d est un carré modulo p.

8/ Montrer que p est inerte dans K si et seulement si d n'est pas un carré modulo p.

9/ Montrer que 2 ramifie si et seulement si $d \equiv 0 \mod 4$.

10/ Montrer que 2 se décompose si et seulement si $d \equiv 1 \mod 8$.

11/ Montrer que 2 est inerte si et seulement si $d \equiv 5 \mod 8$.

Exercice 2. Soient $\alpha = \sqrt[3]{2}$ et $K = \mathbb{Q}(\alpha)$. Décomposer 5, 7 et 11 en premiers dans $\mathfrak{O}_K$ en déterminant le degré de chaque premier dans la décomposition.

Exercice 3. Soit p un nombre premier, $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme p-Eisenstein et α une racine de f. Montrer que p est totalement ramifié en $K = \mathbb{Q}(\alpha)$, i.e. $p\mathfrak{O}_K = \mathfrak{p}^n$. Indication : On regardera la puissance maximale d'un $\mathfrak{p} \mid p$ dans la factorisation de $-a_0 = \alpha^n + \cdots + a_1\alpha$.

Exercice 4. On souhaite étudier la décomposition des nombres premiers dans une extension cyclotomique. On fixe ainsi p un nombre premier et $n > 1$ un entier qui n'est pas divisible par p.

1/ Soient $E/\mathbb{F}_p$ une extension finie et $\zeta \in E$ une racine primitive n-ème de l'unité. Montrer que $f = [\mathbb{F}_p(\zeta) : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n)^*$.

2/ Soit $K = \mathbb{Q}(\mu_n)$ et $\mathfrak{p}$ un idéal premier de K au-dessus p, c'est-à-dire, $p \in \mathfrak{p}$. Montrer que si $\zeta \in \mathfrak{O}_K$ est une racine m-ème *primitive* de l'unité, alors la classe $\zeta + \mathfrak{p}$ est aussi une racine primitive m-ème de l'unité de $\mathbb{F}_\mathfrak{p}$. Indication : On regardera les racines du polynôme $X^n - 1$ en $\mathbb{F}_\mathfrak{p}$.

À partir de maintenant, n est une puissance d'un premier ℓ.

3/ ⋆ Soit $K = \mathbb{Q}(\mu_n)$. Montrer que $p\mathfrak{O}_K$ n'est pas ramifié, c'est-à-dire, il existe des premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ deux-à-deux distincts de K tels que

$$p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

4/ ⋆ On garde les notations de la question précédente. Prouver que le degré de chaque $\mathfrak{p}_i$ (qui vaut $[\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p]$), est l'ordre de p dans $(\mathbb{Z}/n)^*$. Indication : Faire appel à la question 2. En déduire que si $p \equiv 1 \mod n$, alors p est totalement décomposé en K.

5/ ⋆ On suppose $n = 8$ et $p = 3$. Décomposer l'idéal $p\mathfrak{O}_K$ en premiers.

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 7, 24 mars 2020

— Un premier de K est un idéal premier de $\mathfrak{O}_K$.
— On dit qu'un premier $\mathfrak{p}$ de K divise un $a \in \mathfrak{O}_K$ si $a \in \mathfrak{p}$.
— Le groupe des classes de $\mathfrak{O}_K$ est noté Cl_K. La classe d'un idéal fractionnaire $\mathfrak{a}$ dans Cl_K sera désignée par $[\mathfrak{a}]$.

Autour des théorèmes de Minkowski

Exercice 1. Déterminer deux vecteurs $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^2$ qui sont $\mathbb{Q}$-linéairement indépendants, mais qui ne sont pas $\mathbb{R}$-linéairement indépendants. Le sous-groupe $A = \mathbb{Z}\boldsymbol{u} + \mathbb{Z}\boldsymbol{v}$ est-il discret ?

Exercice 2. Soit $\alpha = \sqrt[3]{3}$ et soit $K = \mathbb{Q}(\alpha)$.

1/ Décrire explicitement le plongement canonique ι de K.

2/ Vérifiez directement que $\{\iota(1), \iota(\alpha), \iota(\alpha^2)\}$ est une $\mathbb{R}$-base du $\mathbb{R}$-espace vectoriel $\mathbb{R} \times \mathbb{C}$ et que

$$\big[\det(\iota(1), \iota(\alpha), \iota(\alpha^2))\big]^2 = \frac{|\Delta_K(1, \alpha, \alpha^2)|}{4}$$

Exercice 3. Quels sont les corps de nombres où chaque nombre premier est non-ramifié ?

Exercice 4. On fixe K un corps de nombres de degré n, signature (r, s) et constante de Minkowski $M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta_K|}$. (Attention : La terminologie n'est pas universellement acceptée.)

1/ Montrer que Cl_K est engendré par (les classes des) idéaux premiers dont la norme est au plus M_K. (Note : On dira que l'ensemble $\varnothing$ engendre un groupe si et seulement si le groupe est trivial.)

2/ Pour chaque nombre premier p, on écrit

$$\mathscr{D}_p = \{\mathfrak{p} \text{ premier de } \mathfrak{O}_K \,:\, \mathfrak{p} \mid p\}\,.$$

Montrer que les (classes des) éléments de $\mathscr{M} = \bigcup_{p \leqslant M_K} \mathscr{D}_p$ engendrent Cl_K.

3/ Soit K un corps de nombres parmi $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{13})$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ et $\mathbb{Q}(\sqrt{-7})$. Montrer que l'ensemble $\mathscr{M}$ de la question précédente est vide et en déduire que $\mathfrak{O}_K$ est principal.

4/ Pour chaque $d \in \{11, 19, 43, 67, 163\}$, soit $K = \mathbb{Q}(\sqrt{-d})$. Exprimer $\mathfrak{O}_K$ comme $\mathbb{Z}[\alpha]$; ensuite déterminer le polynôme minimal f de α ainsi que $\mathrm{disc}(f)$. Indication : Dans tous les cas, $d \equiv 3\ (4)$.

5/ Montrer que les anneaux d'entiers des corps K de la question précédente sont tous principaux. (Gauss avait déjà conjecturé que $\mathfrak{O}_{\mathbb{Q}(\sqrt{-d})}$ était principal *seulement si*,

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Cette conjecture a été vérifiée au siècle XX.) Indication : Faire appel à une calculatrice et à $\frac{2}{\pi} < 0,637$.

Exercice 5. Déterminer la structure du groupe de classes des corps de nombres suivantes : $\mathbb{Q}(\sqrt{-6})$ et $\mathbb{Q}(\sqrt{-10})$ et $\mathbb{Q}(\sqrt{-13})$.

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 8, 27 mars 2020

— Un premier de K est un idéal premier de $\mathfrak{O}_K$.
— On dit qu'un premier $\mathfrak{p}$ de K divise un $a \in \mathfrak{O}_K$ si $a \in \mathfrak{p}$. O désigne par $\mathscr{D}_a$ (les diviseurs) l'ensemble des premiers de K qui contiennent a.
— Le groupe des classes de $\mathfrak{O}_K$ est noté Cl_K. La classe d'un idéal fractionnaire $\mathfrak{a}$ dans Cl_K sera désignée par $[\mathfrak{a}]$.
— Si K est un corps de nombres de degré n et signature (r, s), la constante de Minkowski de K est $M_K = \dfrac{4^s}{\pi^s}\dfrac{n!}{n^n}\sqrt{|\Delta_K|}$. (Cette terminologie n'est pas universelle.)

Groupes de classes

Exercice 1. Soient $m > 0$ un entier qui n'est pas un cube, α la racine $\sqrt[3]{m}$ et K le corps de nombres $\mathbb{Q}(\alpha)$. On étudie, dans des cas spécifiques, le groupe de classes de l'anneau d'entiers $\mathfrak{O}_K$. (Une technique utile qui est présentée dans la suite est une méthode pour *trouver des générateurs d'un idéal*.)

1/ Justifier brièvement pourquoi $\{1, \alpha, \alpha^2\}$ est une $\mathbb{Q}$-base de K. Ensuite, exprimer $\mathrm{N}_K(x + y\alpha + z\alpha^2)$ en fonction de x, y et z.

2/ En supposant que m n'a pas de facteur carré et que $m \not\equiv \pm 1$ (9), déterminer une base entière de $\mathfrak{O}_K$ et le discriminant Δ_K. (Vous pouvez consulter les Exercices de la séance du 13 mars 2020.)

3/ Montrer que si $m = 2$, alors $\mathfrak{O}_K$ est principal.

4/ On se concentre sur le cas $m = 3$.

a/ Montrer que

$$2\mathfrak{O}_K = \mathfrak{p}\mathfrak{q},$$

où $\mathfrak{p} = (2, f(\alpha))$ et $\mathfrak{q} = (2, g(\alpha))$ avec f et g dans $\mathbb{Z}[X]$ tels que $f \equiv X + 1$ (2) et $g \equiv X^2 + X + 1$ (2). Par un choix judicieux de f et g, déduire que $\mathfrak{p}$ et $\mathfrak{q}$ sont principaux. Indication : Considérer $\mathrm{N}(f(\alpha)\mathfrak{O}_K)$ et $\mathrm{N}(g(\alpha)\mathfrak{O}_K)$.

b/ En déduire que $\mathfrak{O}_K$ est principal.

5/ On se concentre sur le cas $m = 5$.

a/ Montrer que chaque premier de $\mathscr{D}_5$ et de $\mathscr{D}_7$ est principal.

b/ Montrer que $\mathscr{D}_3$ possède un unique élément et que cet élément, $\mathfrak{p}$ disons, est de la forme $(3, f(\alpha))$, où $f \in \mathbb{Z}[X]$ est tel que $f \equiv X+1$ (3). Prouver que $\mathfrak{p}$ est principal en choisissant judicieusement f.

c/ Montrer que $(2) = \mathfrak{p}\mathfrak{q}$ avec $\mathfrak{p} = (2, \alpha+1)$ et $\mathfrak{q} = (2, \alpha^2+\alpha+1)$. Montrer que $\mathfrak{p}$ et $\mathfrak{q}$ sont principaux. Indication : Pour trouver un générateur de $\mathfrak{p}$, on montrera que *l'unique* idéal de $\mathscr{D}_3$ (trouvé dans la question précédente) divise $(\alpha+1)$, et pour $\mathfrak{q}$ on remplacera $\alpha^2+\alpha+1$ par $\varepsilon_2\alpha^2+\varepsilon_1\alpha+\varepsilon_0$ où ε_i est pair.

d/ En déduire que $\mathfrak{O}_K$ est principal.

Exercice 2. Montrer que le groupe de classes de $\mathbb{Q}(\sqrt{-14})$ est $\mathbb{Z}_{/4}$. Indications : (a) On considère un diviseur $\mathfrak{p}_2$ de 2 et un diviseur $\mathfrak{p}_3$ de 3 et on montre que $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$. (b) Pour déterminer des générateurs d'un idéal $\mathfrak{a}$, on travaillera avec l'isomorphisme $\mathfrak{O}_{\mathbb{Q}(\sqrt{-14})} \simeq \mathbb{Z}[X]/(X^2+14)$.

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 9, 31 mars 2020

— Un idéal de K est, par abus de terminologie, un idéal de $\mathfrak{O}_K$.
— On dira qu'un idéal $\mathfrak{a}$ de K divise un $x \in \mathfrak{O}_K$ quand $x \in \mathfrak{a}$.
— On dira que deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de K sont premiers entre eux quand aucun idéal premier de K divise simultanément $\mathfrak{a}$ et $\mathfrak{b}$.
— Si $\mathfrak{a}$ est un idéal fractionnaire de K, sa classe dans Cl_K sera notée $[\mathfrak{a}]$.

Exercice 1 (Des groupes de classe très grands)**.** Soit $m > 1$ un entier $\equiv 5\ (12)$ et sans facteur carré, α la racine $\sqrt{-m}$, et $K = \mathbb{Q}(\alpha)$.

1/ Prouver que $3\mathfrak{O}_K = \mathfrak{p}\mathfrak{p}'$ où $\mathfrak{p} \neq \mathfrak{p}'$ sont des premiers de K. De plus, montrer que $\mathfrak{p}'$ est l'image de $\mathfrak{p}$ par l'automorphisme $\sigma : K \to K$ définit par $\sigma(\alpha) = -\alpha$.

2/ Si $d = \mathrm{ord}([\mathfrak{p}])$, soit $x + y\alpha$ un générateur de $\mathfrak{p}^d$. Justifier l'égalité $3^d = x^2 + my^2$.

3/ En déduire que $d > \log_3 m$. Indication : Supposer le contraire pour montrer que d est pair et que $(3^{d/2})$ s'écrit de deux façons différentes comme produit d'idéaux premiers.

Exercice 2. Soit $m \geqslant 2$ un entier. On souhaite étudier l'équation de Bachet–Fermat

$$Y^3 = X^2 + m \tag{BF}$$

en faisant des hypothèses suivantes sur m :

P1. il ne possède pas de facteurs carrés,

P2. il est $\equiv 1\ (4)$ ou $\equiv 2\ (4)$,

P3. Si $\varrho = \sqrt{-m}$, alors le nombre de classes du corps $K = \mathbb{Q}(\varrho)$ n'est pas divisible par 3.

Dans la suite, on *admet l'existence* d'une solution $(x, y) \in \mathbb{Z}^2$ de (BF).

1/ Montrer que y est impair et que $x \wedge y = 1$.

2/ Montrer que les idéaux $(x - \varrho)$ et $(x + \varrho)$ sont premiers entre eux.

3/ En employant l'hypothèse sur le nombre de classes, déduire l'existence d'un couple d'entiers (u, v) et d'une unité $\varepsilon \in \mathfrak{O}_K^\times$ tels que

$$x + \varrho = \varepsilon(u + v\varrho)^3.$$

4/ Montrer $\mathfrak{O}_K^\times = \{\pm 1\}$ et en déduire que $x + \varrho$ est le cube d'un *unique* élément de $\mathfrak{O}_K$.

5/ En déduire que *uniquement* un des cas suivants a lieu :

Cas 1 : Le réel $U = \sqrt{(m+1)/3}$ est entier et les *seules* solutions de (BF) sont (X, Y) et $(-X, Y)$, où

$$X = \pm U \cdot \left(U^2 - 3m\right) \quad \text{et} \quad Y = U^2 + m.$$

Cas 2 : Le réel $U = \sqrt{(m-1)/3}$ est entier et les *seules* solutions de (BF) sont (X, Y) et $(-X, Y)$, où

$$X = \pm U \cdot \left(U^2 - 3m\right) \quad \text{et} \quad Y = U^2 + m.$$

Cas 3 : L'équation (BF) ne possède aucune solution en entiers.

6/ Quels sont les solutions en entiers des équations $Y^3 = X^2+2$, $Y^3 = X^2+5$, $Y^3 = X^2+6$, $Y^3 = X^2+10$, $Y^3 = X^2+13$ et $Y^3 = X^2+14$? (Pour rappel, si $h(-m)$ note le nombre de classes du corps $\mathbb{Q}(\sqrt{-m})$, alors $h(-2) = 1$, $h(-5) = h(-6) = h(-10) = h(-13) = 2$ et $h(-14) = 4$. Le calcul de $h(-6)$, $h(-10)$ et $h(-13)$ a été fait lors de la séances du 24 mars 2020 et celui de $h(-14)$ lors de la séance du 27 mars 2020.)

Remarque historique : Voici comment Fermat exprima son intérêt pour cette équation : "Peut-on trouver en nombres entiers un carré autre que 25 qui, augmenté de 2, fasse un cube ? A la première vue cela paraît d'une recherche difficile ; en fractions une infinité de nombres se déduisent de la méthode de Bachet ; mais la doctrine des nombres entiers, qui est assurément très belle et très subtile, n'a été cultivée ni par Bachet, ni par aucun autre dans les écrits venus jusqu'à moi." Le fait que (BF) possède, dans le cas $m = 2$, une infinité de solutions rationnelles a été observé par Bachet en employant, dit en langage moderne !, la structure de groupe de la courbe elliptique $y^3 = x^2 + 2$.

Exercice 3. Soit $p \geqslant 5$ un nombre premier, ζ une racine primitive p-ème de l'unité et K le corps de nombres $\mathbb{Q}(\zeta)$. On suppose que p ne divise pas $|\mathrm{Cl}_K|$ (des tels premiers sont dits "réguliers"). Dans cet exercice, on souhaite montrer le théorème suivant, connu comme le premier cas du "Théorème de Fermat pour exposant régulier", dû à Kummer :

Théorème. *Soient $x, y, z \in \mathbb{Z}$ tels que $z^p + y^p = z^p$. Alors $p \mid xyz$.*

La preuve est découpé en plusieurs exercices. Certains sont moins instructifs que d'autres : le plus importants pour l'éducation en théorie des nombres à notre niveau sont les items 3 et 4 et 5.

Pour ne pas exténuer l'étudiant, on se gardera de prouver le resultat suivant (qui n'est pas hors portée) :

Lemme A. *Soit $u \in \mathfrak{O}_K^\times$. Alors $\zeta^s u$ est réel pour un certain $s \in \{0, 1 \ldots, p-1\}$.*

1/ Il est possible de trouver des entiers x', y' et z', deux-à-deux premiers entre eux tels que $x' \mid x$, $y' \mid y$ et $z' \mid z$, et $x'^p + y'^p = z'^p$.

Dans la suite, on change les notations et on suppose que x, y, z sont deux-à-deux premiers entre eux et que $x^p + y^p = z^p$. Ceci suffit pour établir le théorème.

2/ Prouver l'identité de $\mathfrak{O}_K[X, Y]$:

$$X^p + Y^p = \prod_{i=0}^{p-1} (X + \zeta^i Y).$$

3/ ⋆ Soient $i < j$ des entiers de $\{0, \ldots, p-1\}$. Montrer que *si* les idéaux $\mathfrak{A}_i = (x + \zeta^i y)$ et $\mathfrak{A}_j = (x + \zeta^j y)$ *ne sont pas* premiers entre eux, alors $p \mid z$. Indication : Prouver que $(\zeta^i - \zeta^j) = (1 - \zeta)$ et que $(1 - \zeta)$ est un premier de K qui divise p.

Dans la suite, on suppose que les idéaux $\{\mathfrak{A}_i : i = 0, \ldots, p-1\}$ de la question précédente sont deux-à-deux premiers entre eux. Ceci suffit pour établir le théorème.

4/ ⋆ En utilisant que p ne divise pas $|\mathrm{Cl}_K|$, prouver que $x + \zeta y = u\alpha^p$, où $u \in \mathfrak{O}_K^\times$ et $\alpha \in \mathfrak{O}_K$.

5/ ⋆ Utiliser le Lemme A pour prouver que $x + \zeta y \equiv \zeta^s v a \mod p\mathfrak{O}_K$, où $v \in \mathfrak{O}_K^\times$ est *réel* et a est un *nombre entier*. En déduire que

$$\boxed{x + \overline{\zeta} y \equiv \zeta^{-2s}(x + \zeta y) \mod p\mathfrak{O}_K,}$$

et que l'entier algébrique

$$A := x + \zeta y - \zeta^{2s} x - \zeta^{2s-1} y$$

est divisible par p en $\mathfrak{O}_K$.

6/ Soient $a_0, \ldots, a_{p-2}$ des entiers tels que $a_0 + \cdots + a_{p-2}\zeta^{p-2} \equiv 0 \mod p\mathfrak{O}_K$. Prouver que $p \mid a_i$ pour tout i. Conclure que soit $p \mid xy$, soit $p \mid x - y$. Indication : Étudier les cas $2s \equiv -1, 0, 1\ (p)$. (C'est ici que l'hypothèse $p \geqslant 5$ rentre.)

7/ Appliquer les conclusions précédentes à l'équation $x^p + (-z)^p = (-y)^p$ pour conclure.

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 10, 3 avril 2020

— Si a et b sont des entiers, $(a \mid b)$ désigne le symbole de Kronecker associé à eux.
— Si A est un groupe abstrait, $\mathbb{X}(A)$ note le groupe des caractères linéaires de A, c'est à dire, de morphismes de groupe $A \to \mathbb{C}^\times$.
— Une fonction $f : \mathbb{Z} \to \mathbb{C}$ est complètement multiplicative si $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{Z}$.

Caractères de Dirichlet

Exercice 1. Soit $t > 0$ un entier.

1/ On écrit

$$X_t = \left\{ \chi : \mathbb{Z} \to \mathbb{C} \;\; : \;\; \begin{array}{l} \chi \text{ est } t\text{-périodique,} \\ \chi(mn) = \chi(m)\chi(n) \text{ pour tous } m, n \in \mathbb{Z} \text{ et} \\ \chi(m) \text{ s'annule uniquement si } m \wedge t \neq 1. \end{array} \right\}.$$

Quel est le lien entre X_t est les caractères de Dirichlet modulo t ?

2/ Déterminer explicitement X_2, X_4 et X_8.

Exercice 2. 1/ Exprimer les symboles de Kronecker suivants à l'aides des caractères de Dirichlet décrits à l'Exercice 1.

$$(* \mid 2), \quad (2 \mid *), \quad (4 \mid *), \quad (-4 \mid *), \quad (8 \mid *), \quad (-8 \mid *).$$

2/ On souhaite étudier $(3 \mid *)$.

a/ Calculer $(3 \mid n)$ pour $n \in \{1, \ldots, 7\}$ en utilisant la réciprocité quadratique pour le symbole de Jacobi. Constater que $(3 \mid *)$ n'est pas un caractère de Dirichlet modulo 3.

b/ Montrer que $(3 \mid 6k+1) = (-1)^k$. Utiliser ce fait pour prouver que si $q > 0$ est une période de $(3 \mid *)$, alors $6 \mid q$. Puis, à partir de $(3 \mid 2^l) = (3 \mid 2^l + q)$, déduire que

$$2^l \cdot 6 \mid q \quad \Rightarrow \quad 2^{l+1} \cdot 6 \mid q.$$

Conclure que $(3 \mid *)$ n'est pas périodique. (Un résultat de Allouche et Goldmakher montre que $(d \mid *)$ n'est jamais périodique si $d \equiv 3 \; (4)$.)

Exercice 3. On étudie la périodicité du symbole de Kronecker $(d \mid *)$.

1/ Soit p un nombre premier $\equiv 1\ (4)$. Montrer que $(p \mid n) = (n \mid p)$ pour tout $n \in \mathbb{Z}$. En déduire que $(p \mid *)$ est un caractère de Dirichlet modulo p.

2/ Soit p un nombre premier $\equiv 3\ (4)$. Montrer que $(-p \mid n) = (n \mid p)$; en déduire que $(-p \mid *)$ est un caractère de Dirichlet modulo p.

3/ Soient d et e des entiers tels que $(d \mid *)$ et $(e \mid *)$ sont des caractères de Dirichlet modulo $|d|$ et $|e|$ respectivement. Prouver que $(de \mid *) = (d \mid *)(e \mid *)$. En déduire que $(de \mid *)$ est un caractère de Dirichlet modulo $|de|$.

4/ Soit d un entier qui est $\equiv 1\ (4)$ et qui n'a pas de facteurs carrés. Montrer que $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$. Indication : Faire une récurrence sur le nombre de facteur premiers de $|d|$.

5/ Soit $d = 4m$ avec $m \equiv 3\ (4)$ sans facteurs carrés. Montrer que $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$. Indication : Faire une récurrence sur le nombre de facteur premiers de $|m|$.

6/ Soit $d = 8m$ avec m un entier impair sans facteur carré. Montrer que $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$.

7/ En déduire que si d est le discriminant d'un corps quadratique, alors $(d \mid *)$ est un caractère de Dirichlet modulo $|d|$.

Exercice 4. Soient m un entier sans facteur carré, K le corps de nombres $\mathbb{Q}(\sqrt{m})$ et d le discriminant de K. Le résultat suivant a été vu lors de la séance 6, 20 mars 2020.

$$p \text{ premier impair } \Longrightarrow \begin{cases} (d \mid p) = 0 & \Leftrightarrow \ p \text{ ramifie en } K \\ (d \mid p) = 1 & \Leftrightarrow \ p \text{ se décompose en } K. \\ (d \mid p) = -1 & \Leftrightarrow \ p \text{ est inerte en } K. \end{cases}$$

De même, on a vu que

$$\begin{aligned} d \equiv 0\ (4) &\Leftrightarrow \ 2 \text{ ramifie en } K \\ d \equiv 1\ (8) &\Leftrightarrow \ 2 \text{ se décompose en } K. \\ d \equiv 5\ (8) &\Leftrightarrow \ 2 \text{ est inerte en } K. \end{aligned}$$

Montrer que pour un nombre premier quelconque p, les implications suivantes sont vraies :

$$\begin{aligned} (d \mid p) = 0 &\Leftrightarrow \ p \text{ ramifie en } K \\ (d \mid p) = 1 &\Leftrightarrow \ p \text{ se décompose en } K. \\ (d \mid p) = -1 &\Leftrightarrow \ p \text{ est inerte en } K. \end{aligned}$$

Produits d'Euler

Exercice 5. On étudie quelques propriétés autour des produits d'Euler.

1/ Pour chaque entier $x \geqslant 2$, soit

$$\mathscr{N}_x = \{1\} \cup \{n \in \mathbb{N}^* \text{ : si } p \text{ est facteur premier de } n, \text{ alors } p \leqslant x\}.$$

Montrer que

$$\prod_{p \leqslant x} (1 - p^{-1})^{-1} = \sum_{n \in \mathscr{N}_x} n^{-1}.$$

2/ ⋆ En déduire que

$$\prod_{p \leqslant x} (1 - p^{-1})^{-1} \geqslant \log(x + 1).$$

3/ ⋆ Utiliser la minoration précédente et l'égalité $\displaystyle\sum_{m=2}^{\infty} \frac{1}{m(m-1)} = 1$ pour montrer que

$$\sum_{p \leqslant x} \frac{1}{p} \geqslant \log\log(x + 1) - \frac{1}{2}.$$

Remarque : La somme de $\sum_{m \geqslant 2} \frac{1}{m(m-1)}$ se fait à l'aide d'une décomposition en éléments simples. Cette série est connue comme la série de Mengoli.

4/ ⋆ Soit E le sous-ensemble de $[0, 1]$ définit par les quotients $\varphi(n)/n$, où φ est l'indicatrice d'Euler et n est entier strictement positif. Possède-t-il des points adhérents ? Est-il dense ?

Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 11, 21 Avril 2020

— Si A est un groupe abélien, $\mathbb{X}(A)$ note le groupe des caractères linéaires, c'est-à-dire, les morphismes de groupe $A \to \mathbb{C}^\times$. Si m est un entier positif, X_m désigne les caractères de Dirichlet modulo m.
— $\mathbb{1}_m : \mathbb{Z} \to \mathbb{C}$ est le caractère trivial modulo m, c'est-à-dire, le caractère de Dirichlet induit par le caractère linéaire trivial $(\mathbb{Z}/m)^\times \to \mathbb{C}^\times$.
— $(a \mid b)$ est le symbole de Kronecker.
— $D(a,r)$ désigne le disque ouvert du plan complexe centré en a et de rayon r. De même, $\overline{D}(a,r)$ désigne son adhérence.

Exercice 1 (L'équation fonctionnelle de ζ)**.** On souhaite suivre une méthode de Riemann pour montrer que la fonction ζ se prolonge en une fonction méromorphe sur $\mathbb{C}$. La preuve est basée sur une identité remarquable d'une "fonction θ de Jacobi" (voir l'exercice 4) et la fonction Γ (voir exercices 6 à 9).

1/ Soit $\Re s > 0$. Montrer que pour chaque $n \in \mathbb{N}^*$ l'équation suivant est vérifiée :

$$\pi^{-s/2}\frac{\Gamma(s/2)}{n^s} = \int_0^\infty x^{s/2-1}e^{-n^2\pi x}\,dx.$$

2/ Soit $\omega(x) = \sum_{n\geqslant 1} e^{-\pi n^2 x}$, pour $x > 0$. Justifier brièvement pourquoi ω est une fonction de classe C^1 sur $]0,\infty[$.

3/ En déduire de la question 1, que si $\Re s > 1$, alors

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty x^{s/2-1}\omega(x)\,dx,$$

où $\omega(x) = \sum_{n\geqslant 1} e^{-n^2\pi x}$. (Attention : tout le travail consiste à bien justifier l'inversion dans l'intégration.)

4/ Soit s un complexe dont la partie réelle est > 1. En employant l'équation, valable pour $x > 0$,

$$\omega(1/x) = -\frac{1}{2} + \frac{1}{2}x^{1/2} + x^{1/2}\omega(x),$$

montrer que

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{s(s-1)} + I(s),$$

où

$$I(s) = \int_1^\infty (x^{s/2-1} + x^{-s/2-1/2})\omega(x)\,dx.$$

5/ ⋆ Pour chaque s tel que $\Re s > 1$, on définit

$$\xi(s) := s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Prouver que ξ possède un prolongement à une fonction entière, notée encore ξ, telle que, si $\alpha : \mathbb{C} \to \mathbb{C}$ désigne la symétrie centrale par rapport à $\frac{1}{2}$ (à savoir $s \mapsto 1-s$), alors

$$\xi(\alpha(s)) = \xi(s).$$

6/ ⋆ En déduire que

$$Z(s) = \frac{\pi^{s/2}\xi(s)}{s(s-1)\Gamma(s/2)}$$

définit un prolongement de ζ à une fonction méromorphe ayant un unique pôle simple en $s = 1$.

Indication : On devra faire appel aux propriétés de Γ définies plus bas.

7/ ⋆ Déterminer $\zeta(0)$. Utiliser le fait que $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ et $\zeta(2) = \frac{\pi^2}{6}$ pour calculer $\zeta(-1)$.

Exercice 2. Soient ω une racine primitive 8-ème de l'unité, K le corps de nombres $\mathbb{Q}(\omega)$ et χ_d le caractère de Dirichlet défini par le symbole de Kronecker : $\chi_d(n) = (d \mid n)$. Montrer que si $\Re s > 1$, alors

$$\zeta_K(s) = \zeta(s)L(\chi_{-4}; s)L(\chi_8; s)L(\chi_{-8}; s).$$

Exercice 3. Soient ℓ un nombre premier, $n > 1$ une puissance de ℓ, ω une racine primitive n-ème de l'unité et K le corps de nombres $\mathbb{Q}(\omega)$. On souhaite arriver à la formule générale

$$\zeta_K(s) = \zeta(s) \prod_{\substack{\chi \in X_n \\ \chi \neq \mathbb{1}_n}} L(\chi, s), \qquad s > 1.$$

1/ Si $f > 0$ est un entier justifier légalité en $\mathbb{C}[T]$:

$$1 - T^f = \prod_{\xi \in \mathbb{U}_f} (1 - \xi T).$$

En déduire que si A est un groupe cyclique d'ordre f et a un générateur, alors

$$1 - T^f = \prod_{\chi \in \mathbb{X}(A)} (1 - \chi(a)T).$$

2/ Soit $p \nmid \ell$ un nombre premier ; on désigne par f_p l'ordre de $p + n\mathbb{Z}$ dans le groupe $(\mathbb{Z}/n)^\times$. Déduire l'identité polynomiale

$$\prod_{\chi \in X_n} (1 - \chi(p)T) = \left(1 - T^{f_p}\right)^{\frac{\varphi(n)}{f_p}} .$$

Indication : Si A note le sous-groupe de $(\mathbb{Z}/n)^\times$ engendré par la classe de p, et $\pi : \mathbb{X}((\mathbb{Z}/n)^\times) \to \mathbb{X}(A)$ l'homomorphisme naturel, on dénombrera $\mathbb{X}((\mathbb{Z}/n)^\times)$ suivant les images réciproques et on appliquera la question précédente.

3/ Montrer que, pour tout $s > 1$, on a

$$\zeta_K(s) = (1 - \ell^{-s})^{-1} \prod_{p \nmid \ell} \left(1 - p^{-f_p s}\right)^{-\frac{\varphi(n)}{f_p}} .$$

En déduire la formule

$$\zeta_K(s) = (1 - \ell^{-s})^{-1} \prod_{p \nmid \ell} \prod_{\chi \in X_n} \left(1 - \chi(p) p^{-s}\right)^{-1} .$$

4/ Déduire que

$$\zeta_K(s) = \zeta(s) \prod_{\substack{\chi \in X_n \\ \chi \neq \mathbb{1}_n}} L(\chi, s), \qquad s > 1.$$

Compléments analytiques

Propos. Dans ces compléments, j'ai réuni plusieurs exercices et théorèmes (transformés en exercices) qui ont fait partie de mes enseignements. L'objectif étant de montrer à l'étudiant comment obtenir les bases pour bien comprendre la brève partie sur la théorie analytique de nombres étudiée dans ce cours sans avoir besoin de faire des détours inutiles et couteaux. (Plusieurs textes contemporains d'analyse complexe se contentent que la fonction Γ soit son produit de Weierstrass (exercice 8), ce qui est gênant pour l'étude de ζ. La raison pour cela est probablement le fait que les théorèmes sur les fonctions holomorphes définies par les intégrales (exercice 5) y reçoivent peu d'attention et que les critère de "dérivation sous le signe d'intégrale" ne sont pas rapprochés des critères pour les séries.)

Littérature

B07 T. J. I. Bromwich, Introduction to the theory of infinite series, MacMilland and Co. 1908. Disponible sur `https://archive.org`.

G25 E. Goursat, Cours d'Analyse Mathématique. Tomme I et II. Troisième Édition. 1925. Disponible sur `https://archive.org`.

Cours19 Mon cours "Séries de fonctions et intégrales à un paramètre". Disbonible sur `https://webusers.imj-prg.fr/~joao-pedro.dos-santos/2M261_Notes_Cours_2019.pdf`

Formule sommatoire de Poisson

Exercice 4. Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe C^1 telle que $x \mapsto x^2 f(x)$ et $x \mapsto x^2 f'(x)$ sont bornées.

1/ Soit $x \in \mathbb{R}$, montrer que $F(x) = \sum_{k\in\mathbb{Z}} f(x + 2\pi k)$ converge absolument et définit une fonction 2π-périodique de classe C^1.

2/ Si $\widehat{f}(\xi) = \displaystyle\int_{\mathbb{R}} f(x)e^{-\mathrm{i}x\xi}\,dx$ désigne la transformée de Fourier de f (sur $\mathbb{R}$) et $\widehat{F}(n) = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} F(x)e^{-\mathrm{i}nx}\,dx$ celle de F (sur le cercle) prouver que

$$2\pi\widehat{F}(n) = \widehat{f}(n).$$

3/ En déduire la formule sommatoire de Poisson :

$$2\pi \sum_{k=-\infty}^{\infty} f(2\pi k) = \sum_{n=-\infty}^{\infty} \widehat{f}(n).$$

4/ On définit $\gamma(x) = \dfrac{1}{\sqrt{2\pi}} e^{-x^2/2}$. Montrer que $\widehat{\gamma}'(\xi) = -\xi\widehat{\gamma}(\xi)$. En utilisant que $1 = \int_{\mathbb{R}} \gamma(x)\,dx$, en déduire que $\widehat{\gamma} = \sqrt{2\pi}\cdot\gamma$.

5/ Pour chaque $\lambda > 0$ on pose

$$\theta(\lambda) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2\lambda^2}.$$

Prouver que $\theta(1/\lambda) = \lambda\theta(\lambda)$. Indication : Si $\gamma_\lambda(x) = \gamma(\lambda x)$, alors $\widehat{\gamma}_\lambda(\xi) = \lambda^{-1}\widehat{\gamma}(\xi/\lambda) = \sqrt{2\pi}\cdot\lambda^{-1}\cdot\gamma(\xi/\lambda)$.

Fonctions holomorphes définies par des intégrales

Exercice 5. Soient $I \subset \mathbb{R}$ un intervalle, $U \subset \mathbb{C}$ un ouvert, $f : I \times U \to \mathbb{C}$ une fonction continue. On suppose que pour chaque $t \in I$, la fonction $z \mapsto f(t,z)$ soit holomorphe et, si $f'(t,z)$ désigne la dérivée de $w \mapsto f(t,w)$ en z, alors $(t,z) \mapsto f'(t,z)$ est continue. De plus, on introduit l'hypothèse que pour chaque $z \in U$, l'intégrale

$$F(z) := \int_I f(t,z)\,dt$$

converge.

1/ On suppose que $I = [a,b]$. Soit $x \in U$ tel que $\overline{D}(x,r) \subset U$.

a/ Soit $t \in I$ fixé. Rappeler la formule

$$\frac{f(t,x+h) - f(t,x)}{h} - f'(t,x) = \frac{h}{2\pi i}\int_{\partial D} \frac{f(t,z)}{(z-x)^2(z-x-h)}\,dz.$$

b/ En déduire

$$F'(x) = \frac{1}{2\pi i}\int_I f'(t,x)\,dt.$$

2/ On suppose désormais que $I = [a,b[$. On dira que F converge uniformément si pour tout $\varepsilon > 0$, il existe un $P \in [a,b[$ tel que si $p \geqslant P$, alors

$$\left| F(z) - \int_a^p f(t,z)\,dt \right| \leqslant \varepsilon$$

pour tout $z \in U$.

a/ Montrer que le "test M de Weierstrass" ou "convergence normale $\Rightarrow$ uniforme" est vérifié dans ce contexte : l'intégrale F converge uniformément s'il existe une fonction continue $M : I \to \mathbb{R}_+$ telle que $|f(t,z)| \leqslant M(t)$ pour tout $z \in U$ et $\int_I M(t)\,dt$ converge.

b/ Montrer que si F converge uniformément alors, pour toute suite $(b_n) \subset [a, b[$ ayant b pour limite, la suite de fonctions

$$F_n(z) := \int_a^{b_n} f(t, z)\, dt$$

converge uniformément vers F.

c/ En déduire que si F converge uniformément, alors F est holomorphe et

$$F'(z) = \int_I f'(t, z)\, dz.$$

La fonction Γ

Exercice 6 (Premières propriétés)**.** Pour chaque complexe s tel que $\Re s > 0$, on écrit

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt.$$

1/ Montrer, dans la terminologie de l'exercice 5, que Γ converge uniformément sur chaque bande $\{a \leqslant \Re s \leqslant A\}$, où $a > 0$. En déduire que Γ est une fonction holomorphe. Indication : On pourra écrire $\Gamma = \Gamma_0 + \Gamma_\infty$, où Γ_0 correspond à l'intégrale $\int_0^1$ et Γ_∞ à $\int_1^\infty$.

2/ Soit s tel que $\Re s > 0$. En faisant une intégration par parties, montrer que $\Gamma(s+1) = s\Gamma(s)$. En déduire que $\Gamma(n) = (n-1)!$ pour tout $n \geqslant 1$ entier.

3/ Si $n \in \mathbb{N}^*$, on définit

$$\Gamma_n(s) = \frac{\Gamma(s+n)}{s(s+1)\cdots(s+n-1)}, \qquad \Re s > -n.$$

Montrer que

$$\Gamma_n(s) = \Gamma(s), \qquad \Re s > 0$$

et en déduire que Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$, toujours notée Γ, n'ayant que des *pôles simples* sur $\{0, -1, \ldots\}$.

4/ $\star$ Soit $n \in \mathbb{N}$. Quel est le résidu de Γ en $-n$?

Exercice 7 (La formule d'Euler pour Γ)**.** On souhaite montrer la formule d'Euler

$$\Gamma(s) = \lim_{n \to +\infty} \frac{n!\, n^s}{s(s+1)\ldots(s+n)}, \qquad \Re s > 0.$$

[Cette formule était la définition initiale de la fonction Γ. Ici je suis l'exposition du classique [Br08]. Il arrive à contourner l'emploi de la convergence dominée par une remarque assez simple.]

1/ On commence par des remarques simples.

a/ Montrer que les inégalités suivantes sont vraies :

$$\begin{aligned} e^{\theta} &> 1+\theta \quad \text{si } \theta > 0, \\ e^{-\theta} &> 1-\theta, \quad \text{si } \theta > 0, \\ (1-\theta)^n &> 1-n\theta \quad \text{si } n \in \mathbb{N}^* \text{ et } 0 < \theta < 1. \end{aligned}$$

Indication : Utiliser le théorème des accroissements finis.

b/ Soit $n \in \mathbb{N}^*$. En déduire que si $0 < t < n$, alors

$$0 < e^{-t} - \left(1 - \frac{t}{n}\right)^n < e^{-t}\frac{t^2}{n}.$$

2/ On fixe s un complexe tel que $\Re s > 0$. Utiliser l'encadrement

$$0 \leqslant e^{-t} - \left(1 - \frac{t}{n}\right)^n \leqslant e^{-t}\frac{t^2}{n}, \qquad \text{pour tout } 0 < t < n,$$

pour prouver

$$\Gamma(s) = \lim_{n\to\infty} \int_0^n \left(1 - \frac{t}{n}\right)^n \cdot t^{s-1}\, dt.$$

3/ Montrer que

$$\Gamma(s) = \lim_{n\to+\infty} n^s \int_0^1 (1-u)^n u^{s-1}\, du.$$

4/ En integrant successivement par parties, démontrer la formule d'Euler.

Exercice 8 (Le produit de Weierstrass pour la fonction Γ)**.** On souhaite montrer que pour chaque s tel que $\Re s > 0$, la fonction Γ possède un expression comme un produit infini :

$$\Gamma(s) = \frac{1}{se^{\gamma s}} \prod_{k=1}^{\infty} e^{s/k} \left(1 + \frac{s}{k}\right)^{-1},$$

où γ est la constante d'Euler-Mascheroni (définie dans la suite).

1/ En étudiant la série $\sum_{k\geqslant 1} \delta_k$, où $\delta_k = \frac{1}{k} - \int_k^{k+1} \frac{dt}{t}$, montrer que la suite

$$\gamma_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n} - \log n$$

converge. La limite, notée γ, est connue comme la constante d'Euler-Mascheroni.

2/ À l'aide de la formule d'Euler pour Γ, en déduire la formule de Weierstrass pour Γ.

Exercice 9 (Propriétés du produit de Weierstrass)**.** On souhaite montrer que la formule du produit de Weierstrass pour Γ est valable sur $\mathbb{C}$ et ainsi déduire que Γ ne s'annule jamais. Pour chaque $s \in \mathbb{C}$, on écrit

$$P_n(s) = \prod_{k=1}^{n} e^{-s/k} \left(1 + \frac{s}{k}\right).$$

1/ Soit $\log : D(1,1) \to \mathbb{C}$ la branche principale du logarithme. Soit $R > 0$ un réel. Montrer que, pour chaque entier N tel que $2R \leqslant N$, la série de fonctions

$$\sum_{n \geqslant N} \log\left(1 + \frac{s}{n}\right) - \frac{s}{n}$$

converge normalement sur le disque $\overline{D}(0,R) = \{s \in \mathbb{C} \ : \ |s| \leqslant R\}$.

2/ Pour chaque $s \in \mathbb{C}$, montrer que

$$P(s) := \lim_{n \to \infty} P_n(s)$$

existe et que la fonction P ainsi déduite est holomorphe sur $\mathbb{C}$. Puis, prouver que P s'annule exclusivement sur $\{-1, -2, \ldots\}$.

3/ En déduire que pour chaque $s \in \mathbb{C} \backslash \{0, -1, \ldots\}$, on a

$$\Gamma(s) = \frac{1}{s e^{\gamma s}} \prod_{k=1}^{\infty} e^{s/k} \left(1 + \frac{s}{k}\right)^{-1},$$

et que Γ ne s'annule jamais.