

DM 17. un corrigé

Problème 1 : un anneau principal

Partie I

1°) a) Supposons que \sqrt{n} est un rationnel.

Il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $\sqrt{n} = \frac{p}{q}$ et $p \wedge q = 1$.

Ainsi, $q^2 n = p^2$, donc $q \mid p^2$, mais $q \wedge p^2 = 1$, donc d'après le théorème de Gauss, $q \mid 1$, or $q \in \mathbb{N}^*$, donc $q = 1$, puis $n = p^2$ ce qui contredit les hypothèses de l'énoncé. Ainsi, $\sqrt{n} \notin \mathbb{Q}$.

b) Soit $\alpha \in \mathbb{Q}[\sqrt{n}]$. Supposons qu'il existe $a, b, a', b' \in \mathbb{Q}$ tels que $a + b\sqrt{n} = \alpha = a' + b'\sqrt{n}$. Alors $(a' - a) + \sqrt{n}(b' - b) = 0$.

Si $b \neq b'$, alors $\sqrt{n} = \frac{a - a'}{b' - b} \in \mathbb{Q}$, ce qui est faux, donc $b = b'$, puis $a' - a = 0$, donc $a = a'$.

2°) a) Soit $\alpha, \beta \in \mathbb{Q}[\sqrt{n}]$. Il existe $a, b, a', b' \in \mathbb{Q}$ tels que $\alpha = a + b\sqrt{n}$ et $\beta = a' + b'\sqrt{n}$.

- $1 = 1 + 0\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$;
- $\alpha - \beta = (a - a') + (b - b')\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$;
- $\alpha\beta = (aa' + nbb') + \sqrt{n}(ba' + b'a) \in \mathbb{Q}[\sqrt{n}]$.

Ainsi, $\mathbb{Q}[\sqrt{n}]$ est un sous-anneau de \mathbb{R} .

Supposons que $\alpha \neq 0$. Si $a^2 - nb^2 = 0$, alors $|b|\sqrt{n} = |a|$, donc d'après l'unicité de la question précédente, $|a| = |b| = 0$, donc $\alpha = 0$ ce qui est faux. Ainsi, $a^2 - nb^2 \neq 0$ et

l'on peut écrire : $\frac{1}{\alpha} = \frac{a - b\sqrt{n}}{a^2 - nb^2} = \frac{a}{a^2 - nb^2} - \frac{b}{a^2 - nb^2}\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$.

Ainsi, $\mathbb{Q}[\sqrt{n}]$ est bien un sous-corps de \mathbb{R} .

b) Soit $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$. Il existe $a, b, a', b' \in \mathbb{Z}$ tels que $\alpha = a + b\sqrt{n}$ et $\beta = a' + b'\sqrt{n}$.

- $1 = 1 + 0\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$;
- $\alpha - \beta = (a - a') + (b - b')\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$;
- $\alpha\beta = (aa' + nbb') + \sqrt{n}(ba' + b'a) \in \mathbb{Z}[\sqrt{n}]$.

Or, $\mathbb{Z}[\sqrt{n}] \subset \mathbb{Q}[\sqrt{n}]$, donc $\mathbb{Z}[\sqrt{n}]$ est un sous-anneau de $\mathbb{Q}[\sqrt{n}]$.

3°) a) Posons $\varphi : \begin{array}{ccc} \mathbb{Q}[\sqrt{n}] & \longrightarrow & \mathbb{Q}[\sqrt{n}] \\ z & \longmapsto & \bar{z} \end{array}$.

Soit $\alpha, \beta \in \mathbb{Q}[\sqrt{n}]$. Il existe $a, b, a', b' \in \mathbb{Q}$ tels que $\alpha = a + b\sqrt{n}$ et $\beta = a' + b'\sqrt{n}$.

$\varphi(\alpha + \beta) = \varphi((a + a') + (b + b')\sqrt{n}) = (a + a') - (b + b')\sqrt{n}$

et $\varphi(\alpha) + \varphi(\beta) = a - b\sqrt{n} + a' - b'\sqrt{n}$, donc $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$. Ainsi φ est un morphisme de groupes. De plus,

- $\varphi(1) = 1$;
- $\varphi(\alpha\beta) = \varphi((aa' + nbb') + \sqrt{n}(ab' + ba')) = (aa' + nbb') - \sqrt{n}(ab' + ba')$
 et $\varphi(\alpha)\varphi(\beta) = (a - \sqrt{n}b)(a' - \sqrt{n}b') = (aa' + nbb') - \sqrt{n}(ab' + ba') = \varphi(\alpha\beta)$.

Ainsi φ est un morphisme d'anneaux.

De plus, pour tout $\alpha = a + \sqrt{n}b$, $\varphi(\varphi(\alpha)) = \varphi(a - \sqrt{n}b) = a + \sqrt{n}b = \alpha$, donc $\varphi \circ \varphi = Id_{\mathbb{Q}[\sqrt{n}]}$. Ainsi φ est une involution, donc en particulier une bijection.

On a bien montré que φ est un automorphisme involutif d'anneaux.

b) \diamond Soit $z \in \mathbb{Q}[\sqrt{n}]$. $N(z) = 0 \iff z\bar{z} = 0$, or \mathbb{R} est intègre, donc $N(z) = 0 \iff (z = 0) \vee (\bar{z} = 0)$.

Cependant $\bar{z} = 0 \implies \varphi(\bar{z}) = 0 \implies z = 0$, donc $N(z) = 0 \iff z = 0$.

\diamond Soit $z, z' \in \mathbb{Q}[\sqrt{n}]$. $N(zz') = (zz')\overline{(zz')} = zz'\bar{z}\bar{z}'$ car φ est un morphisme d'anneaux, donc $N(zz') = (z\bar{z})(z'\bar{z}') = N(z)N(z')$.

c) Soit $z \in \mathbb{Z}[\sqrt{n}]$.

Supposons que z est inversible dans $\mathbb{Z}[\sqrt{n}]$: il existe $z' \in \mathbb{Z}[\sqrt{n}]$ tel que $zz' = 1$. Alors $1 = N(1) = N(zz') = N(z)N(z')$, mais $N(z), N(z') \in \mathbb{Z}$, donc $N(z)$ est un entier relatif inversible dans l'anneau \mathbb{Z} . On sait alors que $|N(z)| = 1$.

Réciproquement, supposons que $N(z) = \varepsilon \in \{-1, 1\}$. On a vu que z est inversible dans $\mathbb{Q}[\sqrt{n}]$ avec $z^{-1} = \frac{\bar{z}}{N(z)} = \varepsilon\bar{z}$. Ainsi, $z^{-1} \in \mathbb{Z}[\sqrt{n}]$ et z est inversible dans $\mathbb{Z}[\sqrt{n}]$.

Partie II

4°) a) Soit $\alpha \in \mathbb{Q}$. Posons $a = \lfloor \alpha + \frac{1}{2} \rfloor \in \mathbb{Z}$.

On a $a \leq \alpha + \frac{1}{2} < a + 1$, donc $-\frac{1}{2} \leq \alpha - a \leq \frac{1}{2}$, donc $|\alpha - a| \leq \frac{1}{2}$.

b) Soit $z = \alpha + \sqrt{n}\beta \in \mathbb{Q}[\sqrt{n}]$. D'après la question précédente, il existe $a, b \in \mathbb{Z}$ tels que $|\alpha - a| \leq \frac{1}{2}$ et $|\beta - b| \leq \frac{1}{2}$. Posons $q = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.

$N(z - q) = N((\alpha - a) + \sqrt{n}(\beta - b)) = (\alpha - a)^2 - n(\beta - b)^2$. Or $0 \leq (\alpha - a)^2 \leq \frac{1}{4}$ et $-\frac{3}{4} \leq -\frac{n}{4} \leq -n(\beta - b)^2 \leq 0$, donc en sommant ces encadrements, $-\frac{3}{4} \leq N(z - q) \leq \frac{1}{4}$. Ainsi, $|N(z - q)| < 1$.

5°) a) Soit $x, y \in \mathbb{Z}[\sqrt{n}]$ avec $y \neq 0$. Posons $z = \frac{x}{y} \in \mathbb{Q}[\sqrt{n}]$. D'après la question précédente, il existe $q \in \mathbb{Z}[\sqrt{n}]$ tel que $N(\frac{x}{y} - q) < 1$.

Posons $r = x - qy \in \mathbb{Z}[\sqrt{n}]$. $|N(r)| = |N(y(\frac{x}{y} - q))| = |N(y)| |N(\frac{x}{y} - q)| < N(y)$, car y étant non nul, $N(y) \neq 0$.

On a bien montré qu'il existe $q, r \in \mathbb{Z}[\sqrt{n}]$ tels que $x = qy + r$ et $|N(r)| < |N(y)|$.

b) Le couple (q, r) n'est pas unique, comme le montre le contre-exemple suivant : prenons $x = 1$ et $y = 2$. On peut écrire $x = 0.y + 1$ et $1 = |N(1)| < |N(y)| = 2$, mais aussi $x = 1.y - 1$ et $1 = |N(-1)| < |N(y)|$.

6°) \diamond Posons $I = a_0A$ et montrons que I est un idéal.

$0 = a_0 \times 0 \in I$, donc $I \neq \emptyset$.

Soit $x, y \in I$. Il existe $a, b \in A$ tels que $x = a_0a$ et $y = a_0b$. Alors $x - y = a_0(a - b) \in I$.

Ainsi I est un sous-groupe de A .

Soit $a \in A$ et $x \in I$. Il existe $b \in A$ tel que $x = a_0b$. Alors $ax = a_0(ab)$, car l'anneau est commutatif, donc $ax \in I$.

Ainsi I est un idéal de A , qui contient a_0 .

◊ Si J est un second idéal contenant a_0 , alors pour tout $x \in A$, J étant un idéal, $a_0x \in J$. Ainsi J contient a_0A .

On a bien prouvé que a_0A est le plus petit idéal de A contenant a_0 .

7°) a) I contient $\{0\}$ en tant que sous-groupe, mais $I \neq \{0\}$, donc il existe $z_0 \in I \setminus \{0\}$. Alors $|N(z_0)| \in \{|N(z)|/z \in I \setminus \{0\}\}$, donc cet ensemble est une partie non vide de \mathbb{N} et à ce titre il possède un minimum.

b) $y \in I$, donc d'après la question précédente, $yA \subset I$, où $A = \mathbb{Z}[\sqrt{n}]$.

Réciproquement, soit $x \in I$. $y \neq 0$, donc d'après la question 5.a, il existe $q, r \in \mathbb{Z}[\sqrt{n}]$ tels que $x = qy + r$ et $|N(r)| < |N(y)|$.

$r = x - qy$, or $x, y \in I$ et I est un idéal donc $r \in I$.

Si $r \neq 0$, $|N(r)| \in \{|N(z)|/z \in I \setminus \{0\}\}$ mais ce n'est pas compatible avec le fait que $|N(r)| < |N(y)| = k_0$.

Ainsi, $r = 0$ puis $x = qy \in yA$. Ceci montre que $I \subset yA$.

En conclusion, $I = yA$.

c) Soit A un sous-anneau de $\mathbb{Z}[\sqrt{n}]$. L'application $p : \begin{array}{ccc} \mathbb{Z}[\sqrt{n}] & \longrightarrow & \mathbb{Z} \\ a + \sqrt{n}b & \longmapsto & b \end{array}$ est un morphisme de groupes, bien défini d'après la question 1.b, donc $p(A)$ est un sous-groupe de \mathbb{Z} . D'après le cours, il existe $k \in \mathbb{N}$ tel que $p(A) = k\mathbb{Z}$.

$1 \in A$ car A est un sous-anneau.

$k \in p(A)$, donc il existe $\alpha \in A$ tel que $k = p(\alpha)$. Ainsi, il existe $a \in \mathbb{Z}$ tels que $\alpha = a + k\sqrt{n}$. Alors, $k\sqrt{n} = (a + k\sqrt{n}) - a \in A$.

Ainsi, $\{1, k\sqrt{n}\} \subset A$, donc A contient le sous-groupe engendré par $\{1, k\sqrt{n}\}$, c'est-à-dire $B = \mathbb{Z} + k\sqrt{n}\mathbb{Z} = \{a + kb\sqrt{n}/a, b \in \mathbb{Z}\}$.

Réciproquement, si $\alpha \in A$, $p(\alpha) \in p(A) = k\mathbb{Z}$, donc il existe $a, b \in \mathbb{Z}$ tels que $\alpha = a + kb\sqrt{n}$, donc $\alpha \in B$.

On a ainsi montré que si A est un sous-anneau de $\mathbb{Z}[\sqrt{n}]$, alors il existe $k \in \mathbb{N}$ tel que $A = \mathbb{Z} + k\sqrt{n}\mathbb{Z}$.

Réciproquement, si $k \in \mathbb{N}$, posons $A = \mathbb{Z} + k\sqrt{n}\mathbb{Z}$. $1 \in A$ et si $\alpha, \beta \in A$, on vérifie que $\alpha - \beta \in A$ et que $\alpha\beta \in A$: en effet, lorsque $\alpha = a + kb\sqrt{n}$ et $\beta = a' + kb'\sqrt{n}$, $\alpha\beta = (aa' + k^2bb'n) + k\sqrt{n}(ab' + ba')$.

Ainsi, $\mathbb{Z} + k\sqrt{n}\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[\sqrt{n}]$.

En conclusion, les sous-anneaux de $\mathbb{Z}[\sqrt{n}]$ sont exactement les $\mathbb{Z} + k\sqrt{n}\mathbb{Z}$, où $k \in \mathbb{N}$.

Problème 2 : une intégrale dépendant d'un paramètre

1°) a) Soit $x, y \in \mathbb{R}_+^*$ tels que $x \leq y$.

Pour tout $t \in [0, 1]$, $\frac{1}{t^3 + t + y} \leq \frac{1}{t^3 + t + x}$, donc par croissance de l'intégrale,

$$F(y) = \int_0^1 \frac{dy}{t^3 + t + y} \leq \int_0^1 \frac{dx}{t^3 + t + x}, \text{ ce qui montre que } F \text{ est décroissante.}$$

b) Pour tout $t \in [0, 1]$, $t^3 + t + x \geq x$, donc $0 \leq \frac{1}{t^3 + t + x} \leq \frac{1}{x}$, puis

$$0 \leq F(x) \leq \frac{1}{x} \xrightarrow{x \rightarrow +\infty} 0, \text{ donc d'après le principe des gendarmes, } F(x) \xrightarrow{x \rightarrow +\infty} 0.$$

c) De plus, pour tout $t \in [0, 1]$, $t^3 + t + x \leq 2 + x$,

donc $\frac{1}{2 + x} \leq \frac{1}{t^3 + t + x} \leq \frac{1}{x}$, puis $\frac{x}{2 + x} \leq xF(x) \leq 1$, or $\frac{x}{2 + x} \xrightarrow{x \rightarrow +\infty} 1$, donc d'après le principe des gendarmes, $xF(x) \xrightarrow{x \rightarrow +\infty} 1$.

2°) a) Soit $a, x \in \mathbb{R}_+^*$. $F_a(x) = \int_0^1 \frac{dt}{at + x} = \left[\frac{1}{a} \ln(at + x) \right]_0^1 = \frac{1}{a} \ln\left(\frac{a + x}{x}\right)$.

b) Soit $x \in \mathbb{R}_+^*$.

Pour tout $t \in [0, 1]$, $t^2 \leq 1$, donc $t^3 \leq t$. Ainsi $t + x \leq t^3 + t + x \leq 2t + x$, puis $\frac{1}{2t + x} \leq \frac{1}{t^3 + t + x} \leq \frac{1}{t + x}$, donc en intégrant entre 0 et 1, $F_2(x) \leq F(x) \leq F_1(x)$.

c) $F_2(x) = \frac{1}{2} \ln\left(\frac{2}{x} + 1\right) \xrightarrow{x \rightarrow 0} +\infty$, donc $F(x) \xrightarrow{x \rightarrow 0} +\infty$.

d) Soit $x \in \mathbb{R}_+^*$.

$$0 \leq F_1(x) - F(x) = \int_0^1 \left(\frac{1}{t + x} - \frac{1}{t^3 + t + x} \right) dt = \int_0^1 \frac{t^3 dt}{(t + x)(t^3 + t + x)}.$$

Or, pour tout $t \in [0, 1]$, $(t + x)(t^3 + t + x) \geq (t + x)(t + x) = (t + x)^2 \geq t^2$, donc

$$0 \leq F_1(x) - F(x) \leq \int_0^1 t dt = \frac{1}{2}, \text{ puis } 0 \leq \frac{F_1(x) - F(x)}{-\ln x} \leq \frac{1}{-2 \ln x} \xrightarrow{x \rightarrow 0} 0.$$

$$\text{Ainsi, } \frac{F(x)}{-\ln x} = -\frac{F_1(x) - F(x)}{-\ln x} + \frac{\ln(1 + x) - \ln x}{-\ln x} \xrightarrow{x \rightarrow 0} 1.$$

3°) a) Soit $n \in \mathbb{N}^*$. En intégrant par parties,

$$I_n = \int_0^1 (3t^2 + 1)(t^3 + t)^n \frac{1}{3t^2 + 1} dt = \left[\frac{(t^3 + t)^{n+1}}{n + 1} \frac{1}{3t^2 + 1} \right]_0^1 + \int_0^1 \frac{(t^3 + t)^{n+1}}{n + 1} \frac{6t}{(3t^2 + 1)^2} dt,$$

Donc $I_n = \frac{2^{n+1}}{n + 1} \frac{1}{4} + \frac{6}{n + 1} \int_0^1 \frac{t(t^3 + t)^{n+1}}{(3t^2 + 1)^2} dt$, ce qu'il fallait démontrer.

b) Pour tout $t \in [0, 1]$, $t^3 + t \leq 2t$, donc

$$\left| \frac{1}{2^n} \int_0^1 \frac{t(t^3 + t)^{n+1}}{(3t^2 + 1)^2} dt \right| \leq \frac{1}{2^n} \int_0^1 \frac{t(2t)^{n+1}}{1^2} dt = 2 \int_0^1 t^{n+2} dt = \frac{2}{n + 3} \xrightarrow{n \rightarrow +\infty} 0.$$

c) $I_n \times \frac{n}{2^{n-1}} = \frac{n}{n + 1} + \frac{n}{n + 1} \frac{12}{2^n} \int_0^1 \frac{t(t^3 + t)^{n+1}}{(3t^2 + 1)^2} dt \xrightarrow{n \rightarrow +\infty} 1$, donc $I_n \sim \frac{2^{n-1}}{n}$.

4°) a) Soit $u \in \mathbb{R}_+$ et $n \in \mathbb{N}^*$.

$-u \neq 1$, donc d'après le cours, $\sum_{k=0}^{n-1} (-u)^k = \frac{1 - (-u)^n}{1 + u}$,

donc $\frac{1}{1+u} - \sum_{k=0}^{n-1} (-1)^k u^k = \frac{(-1)^n u^n}{1+u}$, puis $\left| \frac{1}{1+u} - \sum_{k=0}^{n-1} (-1)^k u^k \right| \leq \frac{u^n}{1+u} \leq u^n$.

b) Soit $t \in [0, 1]$, $x \in \mathbb{R}_+^*$ et $n \in \mathbb{N}^*$. Appliquons l'inégalité précédente avec $u = \frac{t^3 + t}{x}$:

$$\left| \frac{1}{1 + \frac{t^3+t}{x}} - \sum_{k=0}^{n-1} (-1)^k \frac{(t^3+t)^k}{x^k} \right| \leq \frac{(t^3+t)^n}{x^n}.$$

On divise cette inégalité par x : $\left| \frac{1}{x + t^3 + t} - \sum_{k=0}^{n-1} (-1)^k \frac{(t^3+t)^k}{x^{k+1}} \right| \leq \frac{(t^3+t)^n}{x^{n+1}} \leq \frac{2^n}{x^{n+1}}$.

c) D'après l'inégalité triangulaire relative aux intégrales,

$$\begin{aligned} \left| \int_0^1 \frac{dt}{x + t^3 + t} - \sum_{k=0}^{n-1} (-1)^k \int_0^1 \frac{(t^3+t)^k}{x^{k+1}} dt \right| &= \left| \int_0^1 \left(\frac{1}{x + t^3 + t} - \sum_{k=0}^{n-1} (-1)^k \frac{(t^3+t)^k}{x^{k+1}} \right) dt \right| \\ &\leq \int_0^1 \left| \frac{1}{x + t^3 + t} - \sum_{k=0}^{n-1} (-1)^k \frac{(t^3+t)^k}{x^{k+1}} \right| dt \\ &\leq \int_0^1 \frac{2^n}{x^{n+1}} dt = \frac{2^n}{x^{n+1}}. \end{aligned}$$

Pour tout $k \in \{1, \dots, n\}$, posons $a_k = (-1)^{k-1} I_{k-1}$, puis notons, pour tout $x \in \mathbb{R}_+^*$,

$\varepsilon(x) = x^n \left(F(x) - \sum_{k=1}^n \frac{a_k}{x^k} \right)$. D'après ce qui précède, $|\varepsilon(x)| \leq \frac{2^n}{x} \xrightarrow{x \rightarrow +\infty} 0$,

donc $F(x) = \frac{a_1}{x} + \frac{a_2}{x^2} + \dots + \frac{a_n}{x^n} + \frac{\varepsilon(x)}{x^n}$, où ε est une fonction telle que $\varepsilon(x) \xrightarrow{x \rightarrow +\infty} 0$.