

CHAPITRE 19 - ANNEAUX, ARITHMÉTIQUE

Exercice 19.1

Soit I un idéal de K non réduit à $\{0\}$. Soit a un élément non nul de I . Soit $x \in K$, comme K est un corps, a est inversible dans K , donc $x = xa^{-1}a$. Or $a \in I$ et I est un idéal, donc $x \in I$, d'où finalement $I = K$.

Exercice 19.4

- L'anneau $\mathbb{Q}[X]$ est principal puisque \mathbb{Q} est un corps (on a une division euclidienne et on retrouve ainsi le fait que tout idéal est principal). L'ensemble I_α des polynômes $P \in \mathbb{Q}[X]$ tels que $P(\alpha) = 0$ est un idéal et est donc engendré par un polynôme de degré minimal parmi tous les polynômes non nuls qui ont α comme racine.
 - on peut diviser ce polynôme par son coefficient dominant pour le rendre unitaire
 - si on a deux polynômes unitaires qui engendrent l'idéal I_α alors ces polynômes sont multiples l'un de l'autre donc sont égaux à une constante multiplicative près. Puisqu'ils sont unitaires, cette constante vaut 1 et les polynômes sont égaux. Cela donne l'unicité. On note Π ce polynôme.
 - si Π n'était pas irréductible, il existerait une factorisation $\Pi = \Pi_1 \Pi_2$ avec des polynômes de $\mathbb{Q}[X]$ de degré strictement inférieurs à celui de Π tous les deux (et non constants). Le réel α est racine de l'un des deux polynômes au moins, ce qui contredit la minimalité de Π .
- On a l'inclusion $\mathbb{Q}_{d-1}[\alpha] \subset \mathbb{Q}[\alpha]$. L'autre s'obtient par division euclidienne par Π : si $P \in \mathbb{Q}[X]$, on a $P = \Pi.Q + R$ avec $\deg R \leq d-1$ et $P(\alpha) = R(\alpha)$.
- Tout d'abord $\mathbb{Q}[\alpha]$ est un anneau (facile à vérifier). On vérifie que tous ses éléments non nuls sont inversibles : si $P \in \mathbb{Q}_{d-1}[X]$ avec $P \neq 0$, alors P est premier avec Π puisque Π est irréductible de degré d (si on avait un pgcd non constant, ce serait un diviseur de Π). Il existe donc des polynômes U et V de $\mathbb{Q}[X]$ tels que $UP + V\Pi = 1$. En évaluant en α , on obtient $P(\alpha)U(\alpha) = 1$ et ainsi $P(\alpha)$ est inversible avec son inverse dans $\mathbb{Q}[\alpha]$, donc dans $\mathbb{Q}_{d-1}[\alpha]$.

Exercice 19.5

- On vérifie facilement que K est un anneau. Puisque $\sqrt{2}$ est irrationnel, on a $a + b\sqrt{2} = 0$ si et seulement si $a = b = 0$. Si ce n'est pas le cas, on a, dans \mathbb{R} , $\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$, ce qui donne que $(a + b\sqrt{2}) \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2} \right) = 1$ et on obtient ainsi un inverse de $a + b\sqrt{2}$ dans K .
- Soit φ un morphisme d'anneau de K dans K . On a $\varphi(1) = 1$, $\varphi(p) = p$ par récurrence si $p \in \mathbb{N}$, puis $\varphi(p) = p$ si $p \in \mathbb{Z}$ par symétrie. Plus généralement, pour tout $x \in K$ et $p \in \mathbb{Z}$, $\varphi(px) = p\varphi(x)$ et notamment $\varphi(p \cdot \frac{1}{p}) = 1$ soit $\varphi(\frac{1}{p}) = \frac{1}{p}$. Finalement, $\varphi(\frac{p}{q}) = \frac{p}{q}$ si $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$. On a alors, si $a, b \in \mathbb{Q}$,

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(\sqrt{2})\varphi(b) = a + b\varphi(\sqrt{2}).$$

Or $\varphi(\sqrt{2} \cdot \sqrt{2}) = 2 = \varphi(\sqrt{2})^2$, ce qui ne laisse que deux possibilités pour $\varphi(\sqrt{2})$, à savoir $\pm\sqrt{2}$. Il n'y a donc que deux morphismes d'anneaux possibles : identité et la conjugaison. Réciproquement les deux conviennent.

Exercice 19.7

On note $n = 3^{7^5}$.

- On pourrait raisonner modulo 10 mais le théorème chinois dit qu'on peut le faire modulo 2 et 5.
- On a $3 \equiv 1[2]$ donc $3^{7^5} \equiv 1[2]$.
- Puisque 3 est premier avec 5, $\bar{3}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$. On a alors $\bar{3}^{\varphi(5)} = \bar{1}$. De plus $\varphi(5) = 5 - 1 = 4$. Il reste donc à connaître le reste de la division euclidienne de 7^5 par 4.
- On a $7 \equiv -1[4]$ donc $7^5 \equiv (-1)^5 \equiv -1 \equiv 3[4]$.
- Finalement $3^{7^5} \equiv 3^3 \equiv 3 \times 9 \equiv -3 \equiv 2[5]$.
- Ainsi $n \equiv 2[5]$. On a n congru à 2 ou 7 modulo 5 et $n \equiv 1[2]$ donne $n \equiv 7[5]$.

Exercice 19.8

Par différence, le système est équivalent à $9x = 3$ et $6x = 7y$.

- dans $\mathbb{Z}/36\mathbb{Z}$: soit $p \in \mathbb{Z}$ tel que $x = \bar{p}$. On doit avoir $9p = 3 + 36k$, soit $3x = 1 + 12k$ ce qui est impossible car $3x - 12k = 1$ est divisible par 3.
- dans $\mathbb{Z}/37\mathbb{Z}$: on cherche l'inverse de 9, ce qu'on peut faire en écrivant une relation de Bezout entre 9 et 37. On remarque que $1 \cdot 37 - 4 \cdot 9 = 1$, donc l'inverse de $\bar{9}$ est $-\bar{4}$. On a alors $x = -12 = 25$. On a alors $7y = -72$. On écrit une relation $16 \cdot 7 - 3 \cdot 37 = 1$ pour avoir l'inverse de 7 qui est 16. Ainsi $y = -16 \cdot 72 = 32$.

Exercice 19.9

- cours : \bar{a} est un élément du groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ qui est de cardinal $\varphi(n)$. L'ordre de \bar{a} divise $\varphi(n)$ et $a^{\varphi(n)} \equiv 1[n]$.
- on a $\varphi(p) = p - 1$. Si $\bar{a} \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$ alors a est inversible et $a^{p-1} \equiv 1[p]$, puis $a^p \equiv a[p]$. Si $a \equiv 0[p]$, alors $a^p \equiv a[p]$.
- On a $798 = 6 \times 7 \times 19$. On veut montrer que $m^{19}n - n^{19}m \equiv 0[798]$. D'après le théorème chinois, il suffit de prouver que c'est vrai modulo 6, 7 et 19.

- puisque 19 est premier, on a $m^{19}n \equiv mn[19]$ et de même $n^{19}m \equiv mn[19]$, donc $m^{19}n \equiv n^{19}m[19]$.
 → On a $\varphi(7) = 6$. Si a est premier avec 7 alors $a^6 \equiv 1[7]$, sinon $a^6 \equiv 0[7]$. Ainsi $m^{19} \equiv m[7]$ que m soit ou non un multiple de 7. On trouve alors comme précédemment $m^{19}n \equiv n^{19}m[7]$.
 → $6 = 2 \times 3$, donc $\varphi(6) = 1 * 2 = 2$ le raisonnement précédent fonctionne encore car $19 = 2.8 + 1$.
4. Les deux propriétés donnent d'une part que $n - 1$ est un multiple de $\varphi(n)$ mais également que $\varphi(n)$ n'est pas inférieur à $n - 1$. On a donc $\varphi(n) = n - 1$. Les seuls entiers pour lesquels on a cette égalité sont les nombres premiers (on sait que $\varphi(n)$ est toujours inférieur à $n - 1$ par définition et il y a égalité si et seulement si n est premier avec tous les entiers de 1 à $n - 1$ donc si et seulement si n est premier).

Exercice 19.10

1. On observe déjà que $I \subset \sqrt{I}$. Soient x et $y \in \sqrt{I}$. Il existe p et q appartenant à \mathbb{N}^* tels que $x^p \in I$ et $y^q \in I$. Par la formule du binôme,

$$(x + y)^{p+q-1} = \sum_{k=0}^{p+q-1} \binom{p+q-1}{k} x^k y^{p+q-1-k}.$$

Pour $k \in \llbracket 0; p-1 \rrbracket$, on a $p+q-1-k \geq q$, d'où $y^{p+q-1-k} = y^{p-1-k} y^q \in I$ (car I est un idéal), donc $\binom{p+q-1}{k} x^k y^{p+q-1-k} \in I$ (toujours car I est un idéal). Pour $k \in \llbracket p; p+q-1 \rrbracket$, on a $x^k = x^{k-p} x^p \in I$, donc $\binom{p+q-1}{k} x^k y^{p+q-1-k} \in I$. Tous les termes de la somme appartiennent à I qui est stable par +, donc $(x + y)^{p+q-1} \in I$, d'où $x + y \in \sqrt{I}$, et clairement $-x \in I$. Soient $x \in I$ et $a \in A$. Il existe $p \geq 1$ tel que $x^p \in I$, donc $(ax)^p = a^p x^p \in I$ (car I est un idéal). Ceci achève de prouver que \sqrt{I} est un idéal de A .

2. Soit $n\mathbb{Z}$ un idéal de \mathbb{Z} . On décompose n en facteurs premiers sous la forme $p_1^{\alpha_1} \dots p_r^{\alpha_r}$.
 → Soit $x \in \sqrt{n\mathbb{Z}}$. Il existe $k \in \mathbb{N}^*$ tel que n divise x^k , donc pour tout $i \in \llbracket 1; r \rrbracket$, p_i divise x^k . Or p_i est premier, donc p_i divise x pour tout i , d'où finalement $\prod_{i=1}^r p_i$ divise x .
 → Inversement, si $\prod_{i=1}^r p_i$ divise x , alors en notant $k = \max(\alpha_1, \dots, \alpha_r)$, n divise $\prod_{i=1}^r p_i^k$, donc n divise x^k .
 Nous avons finalement montré que $\sqrt{n\mathbb{Z}} = \left(\prod_{i=1}^r p_i \right) \mathbb{Z}$.

Exercice 19.11

1. On a $0 \in Z_p$. Soient $x = \frac{a}{b}$ et $y = \frac{c}{d}$ deux éléments de Z_p . On a $x - y = \frac{ad - bc}{bd}$ et $xy = \frac{ac}{bd}$. Comme p est premier et qu'il ne divise ni b ni d , il ne divise pas bd , donc $x - y$ et xy appartiennent à Z_p . On en déduit que Z_p est un sous-anneau de \mathbb{Q} .
2. Montrer que J_p est un idéal de Z_p se fait facilement. Soit J un idéal de Z_p . On suppose qu'il existe un élément de J qui n'est pas dans J_p . Cet élément s'écrit $\frac{a}{b}$ avec a non divisible par p . Alors $\frac{b}{a}$ est dans Z_p et $1 = \frac{a}{b} \frac{b}{a}$ est dans l'idéal J . Un tel idéal qui contient l'élément unité est Z_p tout entier. En conclusion si J est un idéal strict de Z_p , il est contenu dans J_p .
3. On remarque que $J_p = pZ_p$. On va montrer que les idéaux non nuls de Z_p sont les ensembles $p^\alpha Z_p$, où $\alpha \in \mathbb{N}$. Soit I un idéal non nul de Z_p . On note α le plus grand entier naturel tel que p^α divise les numérateurs de tous les éléments de I (écrits sous forme irréductible). Tout élément de I s'écrit donc sous la forme $p^\alpha \frac{u}{v}$, avec $\frac{u}{v} \in Z_p$, donc $I \subset p^\alpha Z_p$. De plus, par maximalité de α , il existe un élément x de I s'écrivant $p^\alpha \frac{a}{b}$, avec a et b premiers avec p . Mais alors $\frac{b}{a} \in Z_p$, et I est un idéal, donc $p^\alpha = \frac{b}{a} x \in I$, et comme I est un idéal, $p^\alpha Z_p \subset I$. Finalement, on a bien $I = p^\alpha Z_p$.

Exercice 19.12

1. les idéaux $p\mathbb{Z}$ où p est premier
2. Soit $f : A \rightarrow K$ un morphisme d'anneaux et $B = \ker f$. Pour $x, y \in A$, on a $xy \in B$ si et seulement si $f(xy) = f(x)f(y) = 0$ donc si et seulement si $f(x) = 0$ ou $f(y) = 0$, donc si et seulement si x ou y est dans B .
3. Soit $I = J \cap K$ ou J et K sont des idéaux premiers. Soient $x, y \in A$. On a $xy \in J$ donc $x \in J$ ou $y \in J$, puis $xy \in K$ donc $x \in K$ ou $y \in K$. On pourrait avoir $x \in J \setminus K$ et le contraire pour y . Comme contre-exemple : si p et q sont deux nombres premiers alors $J = p\mathbb{Z}$ et $K = q\mathbb{Z}$ sont premiers et $J \cap K = (pq)\mathbb{Z}$ ne l'est pas (p et q ne sont pas dans $pq\mathbb{Z}$ alors que $pq \in pq\mathbb{Z}$).
4. Soit x, y tels que $xy = 0$. On a $x, y \in (0)$ (où (0) est l'idéal engendré par 0 donc $\{0\}$). Ainsi x ou y est dans (0) donc est nul. L'anneau est intègre. Soit $x \in A$ non nul. On a $(x^2) \subset (x)$. Réciproquement $x \cdot x = x^2 \in (x^2)$ donc $x \in (x^2)$ et finalement $(x) = (x^2)$. Il existe alors $y \in A$ tel que $x = y \cdot x^2 = (yx)x$. Puisque A est intègre, on a $yx = 1$ et x est inversible.

Exercice 19.14

1. On a $v(z) = z\bar{z}$. On en déduit alors facilement le résultat.
2. Si z est inversible d'inverse z' alors $zz' = 1$ et $v(zz') = v(z)v(z') = 1$. Puisque $v(z)$ est un entier naturel, il vaut 1. On donc z parmi 1, -1 , i , $-i$ et ces quatre éléments sont bien inversibles.
3. ça semble plutôt le contraire : $(1 + i)(1 - i) = 2$.

- Cela implique de trouver $q \in \mathbb{Z}[i]$ tel que $|\frac{z}{w} - q| < 1$. Réciproquement, si on trouve un tel $q \in \mathbb{Z}[i]$ et si on pose $r' = \frac{z}{w} - q$, alors $z - qw = r'w \in \mathbb{Z}[i]$ et on aura bien $r = r'w$ qui est dans $\mathbb{Z}[i]$, $|r| < |w|$ et $z = qw + r$. On note alors $\frac{z}{w} = a + ib \in \mathbb{C}$. Si on note p et q les parties entières de a et b , alors $a + ib$ se trouve dans le carré délimité par les éléments $p + iq, (p + 1) + iq, p + i(q + 1)$ et $(p + 1) + i(q + 1)$ de $\mathbb{Z}[i]$. Il y a toujours au moins un de ces quatre coins qui est à une distance strictement inférieure à 1 de $a + ib$ (mais pas forcément un seul - par exemple si $a = b = \frac{1}{2}$, les quatre conviennent). On en choisit un et il donne l'entier de Gauss q recherché.
- Même principe que dans le cours, maintenant qu'on a une division euclidienne.

Exercice 19.15

- voir exercices du chapitre « groupes ».
- voir chapitre groupes : si x et y sont d'ordre respectif p et q alors il existe un élément d'ordre $\text{ppcm}(p, q)$. On peut alors considérer le $\text{ppcm } k$ des ordres des éléments de G : tout ordre d'un élément de G divise k et k est bien l'ordre d'un élément de G . On a donc $k = e(G)$.
- théorème de Lagrange.
- Si G est cyclique alors il admet un élément d'ordre $e(G)$ et tous les éléments sont d'ordre inférieur donc $e(G) = |G|$. Si $e(G) = |G|$ alors G admet un sous-groupe cyclique qui comporte autant d'éléments que G donc ce sous-groupe est G . On a bien l'équivalence.
- On note p le minimum considéré. Puisque $e(G)$ est le ppcm des ordres des éléments, l'ordre de n'importe quel $x \in G$ divise $e(G)$ et donc $x^{e(G)} = 1$. On a donc $e(G)$ dans l'ensemble des entiers considérés. De plus, G admet un élément d'ordre $e(G)$. Pour cet élément qu'on note x , on a $x^k \neq 1$ si $k \in [1; e(G) - 1]$. On a donc $p \geq e(G)$ et finalement l'égalité.
- Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})^*$ est de cardinal $p - 1$. On a donc, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^{p-1} = 1$. Supposons que $e(G)$ soit strictement inférieur à $p - 1$. On aurait un entier $k \leq p - 2$ tel que, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^k = 1$. Or $\mathbb{Z}/p\mathbb{Z}$ étant un corps, le polynôme $X^k - 1$ admet au maximum k racines dans $\mathbb{Z}/p\mathbb{Z}$. On obtient une contradiction et ainsi $e(\mathbb{Z}/p\mathbb{Z}^*) = p - 1$ et, au passage, on a montré que $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique. Pour $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, on vérifie que tout élément est d'ordre au plus 4 et que $(\bar{0}, \bar{1})$ est d'ordre 4.
- On note $n = o(G)$. On a, pour tout $z \in G$, $z^n = 1$ donc $G \subset \cup_n$. Par cardinal, $G = \cup_n$ et (G, \times) est cyclique.

Exercice 19.17

- Toutes les sommes étant à termes positifs, on peut effectuer toutes les sommations par paquets voulues. On a alors

$$\zeta(s)^2 = \sum_{p=1}^{+\infty} \sum_{q=1}^{+\infty} \frac{1}{(pq)^s} = \sum_{n=1}^{+\infty} \sum_{(p,q) \in I_n} \frac{1}{(pq)^s}$$

où I_n est l'ensemble des couples (p, q) tels que $pq = n$. Il y a exactement $d(n)$ couples de la sorte (on prend les $d(n)$ diviseurs de n possibles pour p et $q = n/p$). On a alors

$$\sum_{(p,q) \in I_n} \frac{1}{(pq)^s} = \sum_{(p,q) \in I_n} \frac{1}{n^s} = \frac{d(n)}{n^s}$$

et enfin $\sum_{n=1}^{+\infty} \frac{d(n)}{n^s} = \zeta(s)^2$

- On calcule cette fois le produit

$$\zeta(s) \sum_{q=1}^{+\infty} \frac{\varphi(q)}{q^s} = \sum_{q=1}^{+\infty} \sum_{p=1}^{+\infty} \frac{\varphi(q)}{p^s q^s} = \sum_{n=1}^{+\infty} \left(\sum_{(p,q) \in I_n} \frac{\varphi(q)}{p^s q^s} \right) = \sum_{n=1}^{+\infty} \left(\sum_{(p,q) \in I_n} \frac{\varphi(q)}{n^s} \right) = \sum_{n=1}^{+\infty} \left(\sum_{q|n} \frac{\varphi(q)}{n^s} \right) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \left(\sum_{q|n} \varphi(q) \right)$$

En utilisant la relation $\sum_{q|n} \varphi(q) = n$, on obtient bien

$$\zeta(s) \sum_{q=1}^{+\infty} \frac{\varphi(q)}{q^s} = \sum_{n=1}^{+\infty} \frac{n}{n^s} = \zeta(s-1).$$

Exercice 19.18

Soit $P = \sum_{k=0}^n a_k X^k$ un tel polynôme. Pour tout $\theta \in \mathbb{R}$, $P(e^{i\theta}) \overline{P(e^{i\theta})} = 1$. On a

$$\overline{P(e^{i\theta})} = \sum_{k=0}^n \overline{a_k} \frac{1}{e^{ik\theta}} = \frac{1}{e^{in\theta}} \sum_{k=0}^n \overline{a_k} e^{i(n-k)\theta} = \frac{1}{e^{in\theta}} \sum_{k=0}^n \overline{a_{n-k}} e^{ik\theta} = \frac{1}{e^{in\theta}} Q(e^{i\theta})$$

où $Q = \sum_{k=0}^n \overline{a_{n-k}} X^k$. On a donc pour tout $\theta \in \mathbb{R}$, $P(e^{i\theta})Q(e^{i\theta}) = e^{in\theta}$, ce qui donne $PQ = X^n$. Par degré, Q est constant et ainsi $P = \alpha X^n$. Réciproquement, ces polynômes conviennent.

Exercice 19.19

1. Si x est racine de P alors x^2 également. Si x est une racine non nulle de module différent de 1, on construit alors une infinité de racines deux à deux distinctes $(x, x^2, x^4, \dots, x^{2^m} \dots)$ de modules strictement monotones. Si 0 est racine alors 1 est racine, puis $P(4) = P(2)P(1) = 0$ ce qui est donc impossible. Les racines sont de module 1 (et différentes de 1).
2. Si x est racine alors $(x+1)^2$ aussi puisque $P((x+1)^2) = P(x+1)P(x) = 0$. On a donc $|x+1|^2 = 1$ donc $|x+1| = 1$. On a donc $|x| = |x+1| = 1$. Les racines de modules 1 est sur la droite d'équation $x = -\frac{1}{2}$. Il n'y a donc que deux racines possible j et \bar{j} .
3. Puisque $P \in \mathbb{R}[X]$ les racines sont de même multiplicité. Le coefficient dominant de P vérifie $a = a^2$ donc $a = 1$ (si P est non nul). On a donc P sous la forme $P = ((X-k)(X-\bar{j}))^m = (X^2 + X + 1)^m$. On regarde si réciproquement un tel polynôme convient. On a

$$P(X)P(X-1) = \left((X^2 + X + 1)((X-1)^2 + (X-1) + 1) \right)^m = ((X^2 + X + 1)(X^2 - X + 1))^m = ((X^2 + 1)^2 - X^2)^m = (X^4 + X^2 + 1)^m$$

et c'est bien $P(X^2)$. Les solutions sont donc les polynômes $(X^2 + X + 1)^m$ avec $m \in \mathbb{N}$.

remarque : on peut aussi utiliser la forme factorisée de P et factoriser $P(X^2)$ et $P(X)P(X-1)$ séparément.

Exercice 19.20

1. On remarque que la quantité à étudier correspond au numérateur de $\left(\frac{P'}{P}\right)'$. Lorsque $P(x) = 0$, le résultat est immédiat puisque $P'(x) \neq 0$ (racine simple). On note z_1, \dots, z_n les racines de P (réelles et distinctes). On a $P = a_n \prod_{k=1}^n (X - z_k)$ et $\frac{P'}{P} = \sum_{k=1}^n \frac{1}{X - z_k}$ (on dérive P et on effectue le quotient). On a alors, en dérivant

$$\frac{P''P - P'^2}{P^2} = - \sum_{k=1}^n \frac{1}{(X - z_k)^2}$$

Si x n'est pas une racine de P , on obtient bien que $P''(x)P(x) - P'(x)^2 < 0$.

remarque : si on ne suppose pas que les racines sont simples mais seulement que P est scindé sur \mathbb{R} , on a alors, pour tout $x \in \mathbb{R}$, $P''(x)P(x) - P'(x)^2 \leq 0$.

2. Par application du théorème de Rolle, on vérifie que si P est scindé à racines simples sur \mathbb{R} alors P' l'est également et plus généralement les dérivées d'ordre quelconque de P sont toujours scindées à racines simples sur \mathbb{R} (on peut même le justifier simplement avec le caractère scindé en considérant les multiplicités). En appliquant la première question à $P^{(k-1)}$ et en évaluant en 0, on obtient $P^{(k+1)}(0)P^{(k-1)}(0) \leq P^{(k)}(0)$. Cela donne

$$(k+1)!(k-1)!a_{k+1}a_{k-1} \leq k!a_k^2 \text{ c'est-à-dire } a_{k+1}a_{k-1} \leq \frac{k}{k+1}a_k^2 \leq a_k^2.$$

Exercice 19.22

On commence par remarquer que $Q - Q' = P$. Pour des raisons de limites en $\pm\infty$, le degré de Q est pair (c'est aussi celui de P) et son coefficient dominant est strictement positif. Ce polynôme admet un minimum global sur \mathbb{R} : on note $M = |Q(0)|$. Il existe $A > 0$ tel que, pour tout $x \in \mathbb{R}$, avec $|x| \geq A$, on a $Q(x) > M + 1$. Le polynôme admet un minimum atteint sur $[-A, A]$ en un point x_0 , et ce minimum est inférieur ou égal à $Q(0)$ donc à M . En ce minimum, Q' s'annule et ainsi $Q(x_0) = P(x_0) \geq 0$.