CHAPITRE 23 - ANNEAUX, ARITHMÉTIQUE

Exercice 23.1

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 23.4

→ Les éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont les classes $\bar{p}$ avec p premier avec 8, c'est-à-dire $\bar{1}, \bar{3}, \bar{5}$ et $\bar{7}$.

→ On cherche l'ordre de chaque élément (donc le cardinal du groupe engendré par un élément). L'ordre de $\bar{1}$ est 1, celui de $\bar{7} = -\bar{1}$ est 2. On a $\bar{3}^2 = \bar{5}^2 = \bar{1}$, donc les éléments différents de 1 sont d'ordre 2. Le groupe n'est donc pas cyclique (*remarque* : on peut montrer que ce groupe des inversibles est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

Exercice 23.5

1. D'après le théorème de Lagrange, l'ordre d'un sous-groupe divise l'ordre du groupe. Si n est premier et H un sous-groupe de $G = \mathbb{Z}/n\mathbb{Z}$ alors card H vaut 1 ou n donc H est $\{0\}$ ou G. Si n n'est pas premier, il existe p et q supérieurs ou égaux à 2 tels que $n = pq$. Le groupe engendré par $\bar{p}$ dans $\mathbb{Z}/n\mathbb{Z}$ est d'ordre q où $1 < q < n$. Finalement $\mathbb{Z}/n\mathbb{Z}$ est simple si et seulement si n est premier (ou $n = 1$?)
2. Si G est simple, tout élément différent du neutre engendre un sous-groupe à au moins 2 éléments donc engendre G : G est donc cyclique et donc de cardinal premier d'après la première question. Si G est cyclique d'ordre p premier alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et est donc simple.

Exercice 23.6

1. On a $\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k!}$ mais factoriser par p n'est pas très éclairant car on ne sait pas si l'autre facteur est un entier.

   Écrivons plutôt $k!\binom{p}{k} = p(p-1)\cdots(p-k+1)$. Par conséquent, $p \mid k!\binom{p}{k}$, or p est premier et $k \in [\![1\,;p-1]\!]$, donc p et $k!$ sont premiers entre eux.

   On déduit par le théorème de Gauss que p divise $\binom{p}{k}$.
2. D'après la formule du binôme de Newton : $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$. D'après 1), pour $k \in [\![1\,;p-1]\!]$, $\binom{p}{k} \equiv 0 \pmod{p}$ donc, modulo p, seuls restent dans le développement le premier et le dernier terme :
$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$
3. → Si $p = 2$, $a^2 - a = a(a-1)$ est un nombre pair, donc $a^2 \equiv a \pmod{2}$.

   → Supposons à présent $p \geqslant 3$. Démontrons par récurrence sur $a \in \mathbb{N}$ la propriété $\mathscr{P}_a$ suivante : $a^p \equiv a \pmod{p}$.
   Initialisation : $a = 0$. On a bien $0^p = 0 \equiv 0 \pmod{p}$, donc $\mathcal{P}_0$ est vraie.
   Hérédité : soit $a \in \mathbb{N}$. Supposons $\mathcal{P}_a$ vraie et montrons $\mathcal{P}_{a+1}$. $(a+1)^p \equiv a^p + 1^p \pmod{p}$ d'après la première question avec $b = 1$. On en déduit avec $\mathscr{P}_a$ que $(a+1)^p \equiv a+1 \pmod{p}$. En conclusion, $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbb{N}$. Si $a \in \mathbb{Z}_-$, d'après ce qui précède $(-a)^p \equiv -a \pmod{p}$. Comme p est impair, on conclut que $a^p \equiv a \pmod{p}$. En résumé, $\forall a \in \mathbb{Z},\ a^p \equiv a \pmod{p}$.

   → On déduit de ce qui précède que : $a\left(a^{p-1} - 1\right) \equiv 0 \pmod{p}$, donc si p ne divise pas a alors, comme p est premier, il est premier avec a et par théorème de Gauss, p divise $a^{p-1} - 1$. Ainsi, on a bien $a^{p-1} \equiv 1 \pmod{p}$.

Exercice 23.7

1. 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 polynôme unitaires qui engendre 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.
2. 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 $\deg R \leqslant d-1$ et $P(\alpha) = R(\alpha)$.
3. Tout d'abord $\mathbb{Q}[\alpha]$ est un anneau (facile à vérifier). On vérifie que tous ses éléments non nuls sont inversibles : si $P \in Q_{d-1}[X]$ 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 $Q_{d-1}[\alpha]$.

Exercice 23.8

→ 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 $\mathbb{R}$, $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}$, ce qui donne que $(a+b\sqrt{2})\left(\dfrac{a}{a^2-2b^2}-\dfrac{b}{a^2-2b^2}\sqrt{2}\right)=1$ 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 $\varphi(p.\frac{1}{p})=1$ soit $\varphi(\frac{1}{p})=\frac{1}{p}$. Finalement, $\varphi\left(\frac{p}{q}\right)=\frac{p}{q}$ 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 $\varphi(\sqrt{2}.\sqrt{2})=2=\varphi(\sqrt{2})^2$, 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 23.10

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 23.11

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 $1.37-4.9=1$, donc l'inverse de $\bar{9}$ est $-\bar{4}$. On a alors $x=-12=25$. On a alors $7y=-72$. On écrit une relation $16.7-3.37=1$ pour avoir l'inverse de 7 qui est 16. Ainsi $y=-16.72=32$.

Exercice 23.12

1. Soit H un sous-groupe de G, distinct de $\{e\}$. On note m le plus petit entier naturel non nul tel que $a^m\in H$. Comme H est un sous-groupe, le sous-groupe engendré par a^m est inclus dans H. Soit $x\in H$. Il existe un entier naturel k tel que $x=a^k$. Par division euclidienne de k par m, il existe deux entiers naturels j et r tels que $k=mj+r$ et $r\leqslant m-1$. Comme H est un groupe et que $x\in H$, $x(a^m)^{-j}\in H$, c'est-à-dire $a^r\in H$, d'où $r=0$ par minimalité de m, d'où $x=a^m j$ et $x\in H$. On a montré que H est cyclique engendré par a^m. Par division euclidienne de n par m, il existe deux entiers naturels q et s tels que $n=mq+s$ et $s\leqslant m-1$. Comme $a^n=e$, on obtient $a^s=(a^m)^{-q}$, donc $a^s\in H$, d'où $s=0$ par minimalité de m, donc m divise n.
2. Comme d divise n, il existe $m\in\mathbb{N}$ tel que $n=dm$. Montrons que le sous-groupe engendré par a^m est d'ordre d. On a $(a^m)^d=e$. S'il existe deux entiers k et j tels que $0\leq j<k<d$ et $a^{km}=a^{jm}$, alors $(k-j)m\geqslant n$, ce qui est absurde car $k-j\leqslant d-1$. Le sous-groupe engendré par a^m est donc formé des d éléments distincts a^{km} pour $0\leqslant k\leqslant d-1$. Inversement, si H est un sous-groupe de G de cardinal d, l'étude menée à la première question montre que H est engendré par $a^{n/d}$.
3. Nous sommes ici en notation additive. Soit $x\in[\![0;n-1]\!]$, l'élément $\overline{x}$ est d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si $\overline{dx}=\overline{0}$ et $\forall k\in[\![1;d-1]\!]$, $\overline{kx}\neq\overline{0}$. Cela équivaut à l'existence de $u\in[\![1;d-1]\!]$ premier avec d tel que $x=\frac{n}{d}u$. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d. En partitionnant les éléments de $\mathbb{Z}/n\mathbb{Z}$ suivant leur ordre (qui doit diviser n), on en déduit que $n=\sum_{d|n}\varphi(d)$.

Exercice 23.13

1. 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 $a^{\varphi(n)}\equiv 1\,[n]$.
2. 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 $a^p\equiv a\,[p]$.
3. On a $798=6\times 7\times 19$. On veut montrer que $m^19n-n^19m\equiv 0[798]$. 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 inférieurs 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 23.14

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 $k \in [\![0\,;p-1]\!]$, on a $p+q-1-k \geqslant q$, 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 $k \in [\![p\,;p+q-1]\!]$, 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 $p \geqslant 1$ 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 $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
   → Soit $x \in \sqrt{n\mathbb{Z}}$. Il existe $k \in \mathbb{N}^*$ tel que n divise x^k, donc pour tout $i \in [\![1\,;r]\!]$, 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 $k = \max(\alpha_1, \ldots, \alpha_r)$, 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 23.15

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 sécrit $\frac{a}{b}$ 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 23.16

1. Supposons I maximal. Soit $a \in A \setminus I$. On constate que $I + aA$ est un idéal de A contenant I strictement (car $a \notin I$), donc $I + aA = A$. Supposons que $\forall a \in A \setminus I,\ I + aA = A$. Soit J un idéal de A contenant strictement I, et soit $a \in J \setminus I$. Par hypothèse, $I + aA = A$, or $I \subset J$ et $aA \subset J$, donc leur somme est incluse dans J, d'où $J = A$ et I est maximal. L'équivalence est démontrée.
2. Soient $(a,b) \in (A \setminus I)^2$. On suppose que $ab \in I$. D'après 1), $A = I + aA$, donc il existe $x \in I$ et $y \in A$ tels que $1 = x + ay$, d'où $b = bx + aby$. Comme I est un idéal, $aby \in I$ et $bx \in I$, donc $b \in I$, ce qui est absurde, d'où finalement $ab \notin I$, et I est un idéal premier.
3. Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. Un tel idéal est maximal si, et seulement si n est premier, c'est-à-dire si, et seulement si l'idéal est premier. Le résultat est le même dans $K[X]$.
4. Soit I un idéal premier, et J un idéal tel que $I \subsetneq J$. Comme A étant principal, il existe a et $b \in A$ tels que $I = aA$ et $J = bA$. Comme I est inclus dans J, il existe $c \in A$ tel que $a = bc$, et $I \neq J$, donc $b \notin I$. Puisque I est premier, $c \in I$, donc il existe $d \in A$ tel que c= ad, d'où $a(1-bd) = 0$. Or A est intègre, donc $bd = 1$, d'où $1 \in J$, ce qui implique $J = A$. On a montré que I est maximal.
5. → On va démontrer que si $f \in I$, alors il existe $g \in A$ telle que, pour tout $x \in \mathbb{R}$, $f(x) = x.g(x)$. En effet, puisque $f(0) = 0$, on a, pour tout $x \in \mathbb{R}$,
$$f(x) - f(0) = f(x) = \int_0^x f'(t)\mathrm{d}t = x\int_0^1 f'(ux)\mathrm{d}u$$
le résultat étant vrai pour $x \neq 0$ par changement de variable linéaire, et immédiatement vrai si $x = 0$. On définit alors la fonction g sur $\mathbb{R}$ par $g(x) = \int_0^1 f'(ux)\mathrm{d}u$. Puisque $(u,x) \in [0,1] \times \mathbb{R} \mapsto f'(ux)$ est de classe $\mathscr{C}^\infty$ (et que l'intégrale est bien sur le segment $[0,1]$, la fonction g est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ (chaque dérivée d'ordre k par rapport à x est continue sur $[0,1] \times [c,d]$ donc majorée par une constante, ce qui permet d'avoir des hypothèses de domination locale sur les segments à tout ordre). Ceci se traduit par l'égalité $I = \mathrm{Id}_{\mathbb{R}}.A$, donc I est principal.
   → L'idéal I est premier car si $(fg)(0) = 0$, alors $f(0) = 0$ ou $g(0) = 0$.
   → Soit J un idéal de A contenant strictement I. Soit $f_0 \in J \setminus I$. Tout élément $f \in A$ peut s'écrire sous la forme $f - \frac{f(0)}{f_0(0)}f_0 + \frac{f(0)}{f_0(0)}f_0$, avec $f - \frac{f(0)}{f_0(0)}f_0 \in I \subset J$, d'où $f \in J$ et $J = A$, donc I est maximal (on retrouve ainsi qu'il est premier).
6. → Par linéarité de la dérivation, J est un sous-groupe additif. Si $f \in J$ et $g \in A$, alors fg a toutes ses dérivées nulles en 0 par la formule de Leibniz, donc $fg \in J$ et J est un idéal de A.

→ On suppose que $f_1 f_2 \in J$ et que $f_2 \notin J$. Soit k le plus petit entier tel que $f_2^{(k)}(0) \neq 0$. En écrivant que $(f_1 f_2)^{(k)}(0) = 0$, on obtient par formule de Leibniz $f_1(0) f_2^{(k)}(0) + \sum_{1 \leqslant j \leqslant k} \binom{k}{j} f_1^{(j)}(0) f_2^{(k-j)}(0) = 0$, d'où $f_1(0) = 0$, puis en écrivant que $(f_1 f_2)^{(k+1)}(0) = 0$, on obtient de même $f_1'(0) = 0$ et ainsi de suite pour finalement obtenir par récurrence que toutes les dérivées de f_1 s'annulent en 0, donc $f_1 \in J$, ce qui prouve que J est premier.

→ L'idéal J n'est pas maximal car il est inclus strictement dans I. Par la même méthode qu'à la question 4), on en déduit que J n'est pas principal.

Exercice 23.17

1. les idéaux $p\mathbb{Z}$ où p est premier
2. Soit $f : A \to K$ 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 $x \in J \backslash K$ 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 $x.x = x^2 \in (x^2)$ donc $x \in (x^2)$ et finalement $(x) = (x^2)$. Il existe alors $y \in A$ tel que $x = y.x^2 = (yx)x$. Puisque A est intègre, on a $yx = 1$ et x est inversible.

Exercice 23.19

On note $G = \mathbb{Z}/p\mathbb{Z}$.

1. On considère f l'application de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ dans lui même qui à x associe x^2 (le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ comporte $p-1$ éléments). C'est un morphisme de groupes. On a $x^2 = 1$ si et seulement si $(x-1)(x+1) = 0$ donc si et seulement si $x = 1$ ou $x = -1$. On a donc $\ker f$ qui comporte deux éléments. On a alors $|\mathrm{Im}\, f| = \dfrac{p-1}{2}$. On ajoute alors 0 comme dernier carré. Il y a donc $\dfrac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.
2. si x est un carré, il existe $y \in G$ tel que $x = y^2$ et alors $x^{(p+1)/2} == y^{p+1} = y^{p-1}y^2$ or $y^{p-1} = 1$ car $p-1 = \varphi(p)$ et l'ordre de y divise $\varphi(p)$. Ainsi $x^{(p+1)/2} = x$. Puisque G est un corps, il est intègre et un polynôme de degré k admet au maximum k racines (si x_0 est racine, on peut factoriser par $(x - x_0)$). Le polynôme admet pour racines tous les carrés. Il sont au nombre de $\dfrac{p+1}{2}$ donc toutes les racines de ce polynôme sont exactement les carrés de G.
3. -1 est un carré si et seulement si $(-1)^{(p+1)/2)} = -1$. On note $p = 2q+1$, alors $\dfrac{p+1}{2} = q+1$ et -1 est un carré si et seulement si q est pair. Finalement, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p est un nombre premier de la forme $4q+1$.
4. Si $p = 4k+1$, il y a $p-1$ solutions. Si $p = 4k+3$, il y a $p+1$ solutions...

Exercice 23.20

1. On a $\nu(z) = z\overline{z}$. On en déduit alors facilement le résultat.
2. Si z est inversible d'inverse z' alors $zz' = 1$ et $\nu(zz') = \nu(z)\nu(z') = 1$. Puisque $\nu(z)$ 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 : $(1+i)(1-i) = 2$.
4. Cela implique de trouver $q \in \mathbb{Z}[i]$ tel que $\left|\frac{z}{w} - q\right| < 1$. 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.
5. Même principe que dans le cours, maintenant qu'on a une division euclidienne.

Exercice 23.21

1. voir exercices du chapitre « groupes ».
2. voir chapitre groupes : si x et y sont d'ordre respectif p et q alors il existe un élément d'ordre $\mathrm{ppcm}(p, q)$. On peut alors considérer le 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 $k = e(G)$.
3. théorème de Lagrange.
4. Si G est cyclique alors il admet un élément d'ordre $o(G)$ 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.
5. 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 $p \geqslant e(G)$ et finalement l'égalité.
6. 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 $k \leqslant p-2$ 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 $(\overline{0}, \overline{1})$ est d'ordre 4.

7. On note $n = o(G)$. On a, pour tout $z \in G$, $z^n = 1$ donc $G \subset \mathbb{U}_n$. Par cardinal, $G = \mathbb{U}_n$ et $(G, \times)$ est cyclique.

Exercice 23.23

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

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 $\displaystyle\sum_{q|n} \varphi(q) = n$, 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 23.24

On a

$$U_n = \sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n}\left(\sum_{q|k} q\right) = \sum_{(p,q)\in\mathbb{N}^{*2}, pq\leqslant n} q.$$

Alors

$$U_n = \sum_{p=1}^{n}\left(\sum_{q\leqslant \frac{n}{p}} q\right) = \sum_{p=1}^{n}\left(\sum_{q=1}^{\left\lfloor \frac{n}{p}\right\rfloor} q\right) = \frac{1}{2}\sum_{p=1}^{n} \left\lfloor \frac{n}{p}\right\rfloor \left(\left\lfloor \frac{n}{p}\right\rfloor + 1\right)$$

Or, pour tout $x \in \mathbb{R}, x - 1 < \lfloor x \rfloor \leqslant x$, donc

$$\frac{1}{2}\sum_{p=1}^{n}\left(\frac{n}{p} - 1\right)\frac{n}{p} \leqslant U_n \leqslant \frac{1}{2}\sum_{p=1}^{n}\left(\frac{n}{p} + 1\right)\frac{n}{p},$$

$$\frac{n^2}{2}\left(\sum_{p=1}^{n}\frac{1}{p^2}\right) - \frac{n}{2}\left(\sum_{p=1}^{n}\frac{1}{p}\right) \leqslant U_n \leqslant \frac{n^2}{2}\left(\sum_{p=1}^{n}\frac{1}{p^2}\right) + \frac{n}{2}\left(\sum_{p=1}^{n}\frac{1}{p}\right)$$

Or, $\displaystyle\sum_{p=1}^{n}\frac{1}{p} = O(\ln n)$, $\displaystyle\sum_{p=1}^{+\infty}\frac{1}{p^2} = \zeta(2) = \frac{\pi^2}{6}$ et $\displaystyle\frac{\pi^2}{6} - \frac{1}{n} \leqslant \sum_{p=1}^{n}\frac{1}{p^2} \leqslant \frac{\pi^2}{6}$, ce qui assure que $U_n = \dfrac{\pi^2 n^2}{12} + O(n\ln n)$, donc $U_n \underset{n\to+\infty}{\sim} \dfrac{\pi^2 n^2}{12}$.

Exercice 23.25

Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k$ 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 $Q = \displaystyle\sum_{k=0}^{n}\overline{a_{n-k}}X^k$. 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 23.26

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 $(x, x^2, x^4, \dots, x^{2^n} \dots$ 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 sont de modules 1 est sur la droite d'équation $x = -\frac{1}{2}$. Il n'y a donc que deux racines possible j et $j^2 = \overline{j}$.
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 $P = ((X-k)(X-\overline{j}))^m = (X^2+X+1)^m$. On regarde si réciproquement un tel polynôme convient. On a
$$P(X)P(X-1) = \Big((X^2+X+1)((X-1)^2+(X-1)+1)\Big)^m = ((X^2+X+1)(X^2-X+1))^m = ((X^2+1)^2-X^2)^m = (X^4+X^2+1)^m$$
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 23.27

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 $x \in \mathbb{R}$, $P''(x)P(x) - P'(x)^2 \leqslant 0$.
2.

Exercice 23.29

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 $|x| \geqslant A$, 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 $Q(x_0) = P(x_0) \geqslant 0$.