Anneaux

1 Anneaux

Exercice 1. ♡* On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.

1. Démontrer que, pour tout $x \in A$, $x = -x$.
2. Montrer que A est commutatif.

Exercice 2. ♡* On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.
4. ** Soit $x = a + b\sqrt{2}$ un élément inversible de $\mathbb{Z}\left[\sqrt{2}\right]$, tel que $x > 1$. Montrer que $a \geq 1$ et $b \geq 1$. En déduire que le plus petit élément inversible de $\mathbb{Z}\left[\sqrt{2}\right]$ vérifiant $x > 1$ est $1 + \sqrt{2}$.
5. Soit $x = a + b\sqrt{2}$ un élément inversible de $\mathbb{Z}\left[\sqrt{2}\right]$ vérifiant $x > 1$. Montrer qu'il existe un unique entier positif n tel que
$$\left(1 + \sqrt{2}\right)^n \leq x < \left(1 + \sqrt{2}\right)^{n+1}.$$
Montrer ensuite que $x = \left(1 + \sqrt{2}\right)^n$.
6. **En déduire les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$. (On pourra distinguer les cas $x \geq 1$, $x \in]0, 1[$ et $x < 0$).

2 Idéaux

Exercice 3. ♡** Soit $(A, +, \times)$ un anneau commutatif. Si I et J sont deux idéaux de A, on note

$$\begin{aligned} I + J &= \{i + j;\ i \in I, ; j \in J\} \\ I.J &= \{i_1 j_1 + \cdots + i_n j_n;\ n \geq 1,\ i_k \in I,\ j_k \in J\} \end{aligned}$$

On dit que deux idéaux I et J sont étrangers si $I + J = A$.

1. Montrer que $I + J$ et IJ sont encore des idéaux de A.
2. Montrer que $I.J \subset I \cap J$.
3. Montrer que $(I + J).(I \cap J) \subset I.J$.
4. Montrer que si I et J sont étrangers, alors $I.J = I \cap J$.

Exercice 4. ** Soit A un anneau commutatif (unitaire). Si I est un idéal de A, on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A;\ \exists n \geq 1,\ x^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Soient I, J deux idéaux de A et $p \geq 1$. Montrer que
$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J},\ \sqrt{\sqrt{I}} = \sqrt{I} \text{ et } \sqrt{I^p} = \sqrt{I}.$$
3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$, $k \geq 1$, déterminer le radical de I.

Exercice 5. ** Soit A un anneau commutatif. On dit qu'un idéal I est premier si $xy \in I \implies x \in I$ ou $y \in I$. On dit que I est maximal si, pour tout idéal J de A tel que $I \subset J$, on a $J = I$ ou $J = A$.

1. Déterminer les idéaux premiers de $\mathbb{Z}$.
2. Soit I un idéal et $x \in A \backslash I$. Soit J l'idéal engendré par I et x. Montrer que
$$J = \{a \in A;\ \exists i \in I,\ \exists k \in A,\ a = i + kx\}\,.$$
3. En déduire que tout idéal maximal est premier.
4. Montrer que si tous les idéaux de A sont premiers, alors A est un corps.
5. Montrer que si A est principal, tout idéal premier est maximal.

Exercice 6. ** Soit A un anneau commutatif. On dit que $p \in A$ est premier si l'déal pA engendre p est premier (cf exercice précédent).

1. Montrer que si p est premier, alors p est irréductible.
2. Dans l'anneau $\mathbb{Z}[i\sqrt{5}]$ montrer que 3 est irréductible, mais n'est pas premier.

Exercice 7. ** Soit A un anneau principal tel que tout suite décroissante d'idéaux est stationnaire. Montrer que A est un corps.

Exercice 8. ** Soit E un ensemble fini et non vide. On rappelle que la différence symétrique de deux parties A et B de E est le sous-ensemble de E défini par :
$$A \Delta B = (A \cap \overline{B}) \cup (B \cap \overline{A})$$
(En notant $\overline{C}$ le complémentaire dans E de toute partie C de E.

1. Démontrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif unitaire. Hint. Utiliser l'application $\chi_A : E \to \mathbb{Z}/2\mathbb{Z}$, avec $\chi_A(a) = 1$ si $a \in A$ et 0 sinon.
2. Soit $a \in E$ fixé. On pose $J_a = \{A \in \mathcal{P}(E) \,/\, a \notin A\}$
   (a) Démontrer que J_a est un idéal de $(\mathcal{P}(E), \Delta, \cap)$.
   (b) Démontrer que cet idéal est maximal, c'est à dire que si J est un idéal de $(\mathcal{P}(E), \Delta, \cap)$ contenant strictement J_a alors $J = \mathcal{P}(E)$

3 Arithmétique

Exercice 9. ♡* Résoudre

1. $x^2 + x + \overline{7} = \overline{0}$ dans $\mathbb{Z}/13\mathbb{Z}$.
2. $x^2 - \overline{4}x + \overline{3} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 10. **

1. Montrer qu'il existe un nombre infini de nombres premiers de la forme $4k + 3$.
2. Montrer que la différence entre deux nombres premiers consécutifs peut être arbitrairement grande.

Exercice 11. ** Démontrer que, pour tout entier $n \geq 0$, $(3 - \sqrt{5})^n + (3 + \sqrt{5})^n$ est divisible par 2^n.

Exercice 12. ♡♡** Le but de cet exercice est de montrer qu'il n'existe pas d'entier $n \geq 2$ tel que n divise $2^n - 1$.
On raisonne par l'absurde : supposons qu'un tel entier n existe. On note p le plus petit diviseur premier de n.

1. Montrer que $p > 2$.
2. On note m l'ordre de la classe de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   (a) Montrer que $m|p - 1$.
   (b) Montrer que $m|n$.

(c) Conclure.

Exercice 13. ♡♡** Le but de cet exercice est de démontrer le théorème de Wilson : un entier $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1\ [n]$.

1. Soit $p \geq 2$ premier. Combien de solutions l'équation $x^2 = 1$ admet-elle de solutions dans $\mathbb{Z}/p\mathbb{Z}$?
2. Soit $p \geq 2$ premier. Montrer que $(p-1)! = -1\ [p]$.
3. Soit $n \geq 2$ un entier tel que n divise $(n-1)! + 1$. Montrer que pour tout $a \in \{1, \ldots, n-1\}$, a est inversible dans $(\mathbb{Z}/n\mathbb{Z}, \times)$. En déduire que n est premier.

Exercice 14. ** Pour $n \geq 1$ un entier, on note $\varphi(n)$ l'indicateur d'Euler de n.

1. Soit d un diviseur de n. On pose

$$A_d = \{1 \leq k \leq n;\ k \wedge n = d\}\,.$$

   Quel est le cardinal de A_d ?
2. En déduire que $n = \sum_{d|n} \varphi(d)$.

Exercice 15. *(De l'utilité des mathématiques)* Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces.
Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces.
Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.

Le cuisinier se demande combien de pièces d'or il recevrait au minimum s'il empoisonnait le reste des pirates. D'après vous ?

Exercice 16. *** Soit p un nombre premier supérieur ou égal à 5. On écrit

$$\sum_{i=1}^{p-1} \frac{1}{i} = \frac{m}{(p-1)!},$$

avec $m \in \mathbb{N}$.

1. Montrer que l'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, $x \mapsto \dfrac{1}{x}$ est une bijection (est-ce un isomorphisme de groupes ?)
2. En déuire que $p^2 | m$. On pourra utiliser l'égalité

$$2 \times \sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=1}^{p-1} \frac{p}{i(p-i)}.$$

4 Polynômes

Exercice 17. ♡* Déterminer les polynômes de $\mathbb{R}[X]$ tels que P' divise P.

Exercice 18. ♡**

1. Soit $P \in \mathbb{R}[X]$ vérifiant $P(X^2) = P(X-1)P(X+1)$.
   (a) Démontrer que si z est racine de P, il existe une racine de P de module supérieur strict à z.
   (b) En déduire les polynômes $P \in \mathbb{R}[X]$ solutions.
2. Soit $P \in \mathbb{R}[X] \backslash \{0\}$ vérifiant $P(X^2) = P(X)P(X-1)$.
   (a) Démontrer que si z est racine de P, alors $z = j$ ou $z = j^2$.
   (b) En déduire les polynômes $P \in \mathbb{R}[X]$ solution.

Exercice 19. ♡** Soit $n, m \geq 1$. Déterminer le pgcd de $X^n - 1$ et $X^m - 1$.

Exercice 20. ♡**

1. En s'inspirant de la formule pour tous complexes z et z', $|zz'|^2 = |z|^2|z'|^2$, montrer que tout polynôme P de $\mathbb{R}[X]$ tel que $P(x) \geq 0$ pour $x \in \mathbb{R}$ peut s'écrire $P = Q^2 + R^2$ avec Q et R deux polynômes de $\mathbb{R}[X]$.
2. Montrer que tout polynôme P de $\mathbb{R}[X]$ tel que $P(x) \geq 0$ pour $x \in \mathbb{R}^+$ peut s'écrire $P = Q^2 + XR^2$ avec Q et R deux polynômes de $\mathbb{R}[X]$.

Exercice 21. ***

1. Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{U}) \subset \mathbb{U}$.
2. Déterminer les fonctions rationnelles $F \in \mathbb{C}(X)$ tels que $F(\mathbb{U}) \subset \mathbb{U}$.

Exercice 22. *** Soit a_1, ..., $a_n \in \mathbb{Z}$ deux à deux distincts.

1. Montrer que $P = (X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.
2. De même, traiter le cas $Q = (X - a_1) \cdots (X - a_n) + 1$ (on distinguera $n > 4$ de $n \leq 4$.

Exercice 23. ♡* Soient A et B dans $\mathcal{M}_n(\mathbf{Z})$ telles que $\det(A) \wedge \det(B) = 1$. Montrer qu'il existe U, $V \in \mathcal{M}_n(\mathbf{Z})$ telles que $AU + BV = I_n$.

Exercice 24. ♡** (Critère d'irrédutibilité d'Eisentein) Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe p premier tel que $\forall k \in [\![0, n-1]\!]$, $p|a_k$ et $p^2 \not| a_0$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.
Par exemple $P = X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 25. *** Soit $P = \sum_{k=0}^{m} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ des polynômes de $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps.

1. Montrer qu'il existe un couple $(R, S) \in \mathbb{K}_{n-1}[X] \times \mathbb{K}_{m-1}[X]$ tel que $PR + QS = P \wedge Q$ et que ce couple est unique si $P \wedge Q = 1$.
2. Soit $\varphi : \mathbb{K}_{n-1}[X] \times \mathbb{K}_{m-1}[X] \to \mathbb{K}_{m+n-1}[X]$, $(T, U) \mapsto PT + QU$.
   Soit $S(P, Q)$, la matrice de passage de φ où $\mathbb{K}_{n-1}[X] \times \mathbb{K}_{m-1}[X]$ est rapporté à la base
   $$\big((X^{n-1}, 0), \cdots, (1, 0), (0, X^{m-1}), \cdots, (0, 1)\big)$$
   et $\mathbb{K}_{m+n-1}[X]$ à la base $(X^{m+n-1}, \cdots, 1)$.
   Vérfier que
   $$S(P,Q) = \begin{pmatrix} a_m & & & & b_n & & & \\ a_{m-1} & a_m & & & b_{n-1} & b_n & & \\ & a_{m-1} & \ddots & & & \ddots & & \\ \vdots & & \ddots & a_m & \vdots & & & b_n \\ & \vdots & & a_{m-1} & b_1 & & & b_{n-1} \\ a_0 & & & & b_0 & & & \\ & a_0 & & & & & & \vdots \\ & & \ddots & \vdots & & \ddots & & \\ & & & a_0 & & & & b_0 \end{pmatrix} \in \mathbb{K}_{m+n}[X]$$
   S s'appelle la matrice de Sylvester de P et Q et $R(P, Q) = \det S(P, Q)$ le résultant de P et Q.
3. Montrer que $\det S(P, Q) = Res(P, Q) \neq 0$ si et seulement si $P \wedge Q = 1$.
4. En déduire que si $\mathbb{K} = \mathbb{C}$, l'ensemble des polynômes scindés à racines simples est un ouvert.

Anneaux

(Solutions)

Solution 1.

1. On applique la propriété à l'élément $x+x$. Il vient
$$x+x=(x+x)^2=x^2+x^2+x^2+x^2=x+x+x+x.$$
Après simplification, on trouve $x+x=0$, soit $x=-x$.
2. Soient $x,y\in A$. On doit prouver $xy=yx$. Appliquons la propriété à l'élément $x+y$. On a
$$(x+y)=(x+y)^2=x^2+y^2+xy+yx=x+y+xy+yx.$$
Après simplification, on trouve $xy+yx=0$ soit $xy=-yx$, soit $xy=yx$ en appliquant le résultat de la question précédente.

Solution 2.

1. Il suffit de prouver que c'est un sous-anneau de $(\mathbb{R},+,\times)$. Mais $\mathbb{Z}[\sqrt{2}]$ est
— stable par la loi $+$: $(a+b\sqrt{2})+(a'+b'\sqrt{2})=(a+a')+(b+b')\sqrt{2}$.
— stable par la loi $\times$:
$$(a+b\sqrt{2})\times(a'+b'\sqrt{2})=(aa'+2bb')+(ab'+a'b)\sqrt{2}$$
.
— stable par passage à l'opposé $-(a+b\sqrt{2})=-a+(-b)\sqrt{2}$.
De plus, $1\in\mathbb{Z}[\sqrt{2}]$, ce qui achève la preuve du fait que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.
2. Posons $x=a+b\sqrt{2}$ et $y=a'+b'\sqrt{2}$. En tenant compte de la formule pour le produit obtenue à la question précédente, on a
$$\begin{aligned}N(xy) &= (aa'+2bb')^2-2(ab'+a'b)^2\\ &= (aa')^2-2(ab')^2-2(a'b)^2+(4bb')^2.\end{aligned}$$
D'autre part,
$$\begin{aligned}N(x)\times N(y) &= (a^2-2b^2)(a'^2-2b'^2)\\ &= (aa')^2-2(ab')^2-2(a'b)^2+(4bb')^2.\end{aligned}$$
3. Soit $x=a+b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y. Alors $N(xy)=N(1)=1$, et donc $N(x)N(y)=1$. Puisque $N(x)$ et $N(y)$ sont tous les deux des entiers, on a nécessairement $N(x)=\pm1$. Réciproquement, si $N(x)=\pm1$, alors, en utilisant la quantité conjuguée :
$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\pm(a-b\sqrt{2})$$
ce qui montre que $a+b\sqrt{2}$ est inversible, d'inverse $\pm(a-b\sqrt{2})$.
4. Soit x un élément inversible de $\mathbb{Z}[\sqrt{2}]$, tel que $x>1$. Dans ce cas $\frac{1}{x}\in\left]0,1\right[$.
Posons $x=a+b\sqrt{2}$, alors $\frac{1}{x}=\pm(a-b\sqrt{2})$.
Si $\frac{1}{x}=a-b\sqrt{2}, 2a>0$ car $x+\frac{1}{x}>0$, d'où $a\in\mathbb{N}^*$. Si b était négatif ou nul, on aurait $x\leq\frac{1}{x}$, ce qui est impossible. Donc b est un entier strictement positif. $b\geq1$.
Si $\frac{1}{x}=-(a-b\sqrt{2}), x+\frac{1}{x}=2b\sqrt{2}$ d'où $b\in\mathbb{N}^*$. D'autre part, $x-\frac{1}{x}=2a$ est strictement positif, d'où $a\in\mathbb{N}^*$.
Si $x=a+b\sqrt{2}$ est un élément inversible de $\mathbb{Z}[\sqrt{2}]$, tel que $x>1, a\geq1$ et $b\geq1$.
Or $1+\sqrt{2}$ est inversible dans $\mathbb{Z}[\sqrt{2}]$.
Le plus petit élément inversible de $\mathbb{Z}[\sqrt{2}]$ strictement supérieur à 1 est $1+\sqrt{2}$.

5. On utilise la fonction partie entière : $n = \left[\frac{\ln x}{\ln(1+\sqrt{2})}\right]$ est le seul entier positif qui convient.
   L'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ est stable par le produit.
   De même si x est un élément inversible de $\mathbb{Z}[\sqrt{2}]$, $\frac{1}{x}$ est également un élément inversible de $\mathbb{Z}[\sqrt{2}]$.
   Donc si x est un élément inversible de $\mathbb{Z}[\sqrt{2}]$ vérifiant $(1+\sqrt{2})^n \leq x < (1+\sqrt{2})^{n+1}$, $\frac{x}{(1+\sqrt{2})^n}$ est inversible et vérifie $1 \leq \frac{x}{(1+\sqrt{2})^n} < 1+\sqrt{2}$, d'où $\frac{x}{(1+\sqrt{2})^n} = 1$.
   Les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ vérifiant $x > 1$ sont de la forme $(1+\sqrt{2})^n$ avec $n \in \mathbb{N}^*$.
6. Si $x \geq 1, x = (1+\sqrt{2})^n$ avec $n \in \mathbb{N}$.
   Si $x \in]0, 1\,[, \frac{1}{x} > 1$, donc $x = (1+\sqrt{2})^{-n} = (\sqrt{2}-1)^n$.
   Si $x < 0, x = -(1+\sqrt{2})^n$ avec $n \in \mathbb{Z}$.

Solution 3.

1. Commençons par $I+J$. Il faut d'abord démontrer que c'est un sous-groupe de $(A,+)$. Mais $0 = 0+0 \in I+J$. D'autre part, si x et y sont éléments de $I+J$, on les écrit $x = i+j$, $y = i'+j'$, et on a
$$x - y = (i-i') + (j-j') \in I+J$$
puisque $i-i' \in I$ et $j-j' \in J$. D'autre part, pour $a \in A$, on a, par distributivité de $\times$ par rapport à $+$:
$$ax = ai + aj \in I+J$$
puisque, I et J étant deux idéaux, $ai \in I$ et $aj \in J$. Ceci prouve que $I+J$ est un idéal. Passons maintenant à $I.J$: $0 \times 0 = 0$ est élément de $I.J$. De plus, si $x = \sum_{k=1}^{n} i_k j_k$ et $y = \sum_{l=1}^{m} i'_l j'_l$, en posant $i_k = -i'_{k-n}$ et $j'_k = -j'_{k-n}$ pour k allant de $n+1$ à $n+m$, on a
$$x - y = \sum_{k=1}^{n+m} i_k j_k$$
ce qui prouve que $I.J$ est un sous-groupe de $(A,+)$. Enfin, pour tout a dans A, on a
$$ax = \sum_{k=1}^{n} (ai_k)(bj_k) \in I.J$$
puisque chaque ai_k (resp. aj_k) est élément de I (resp. de J).
2. Soit $x = \sum_{k=1}^{n} i_k j_k$ un élément de $I.J$. Pour chaque k, $i_k j_k$ est un élément de I puisque I est un idéal. Comme I est de plus stable par la somme, $I.J$ est bien contenu dans I. Par symétrie du rôle joué par I et J, $I.J$ est aussi contenu dans J et donc $I.J$ est contenu dans $I \cap J$.
3. Soit $x \in (I+J).(I \cap J)$. On écrit $x = \sum_{k=1}^{n} a_k b_k$ avec $a_k \in I+J$ et $b_k \in I \cap J$. Puisque $I.J$ est un idéal, il suffit de prouver que $a_k b_k \in I.J$. On écrit $a_k = i_k + j_k$, de sorte que
$$a_k b_k = i_k b_k + b_k j_k.$$
C'est un élément de $I.J$, car $i_k \in I$, $b_k \in J$ et $b_k \in I$, $j_k \in J$.
4. Il suffit de prouver que $I \cap J \subset I.J$. Prenons $x \in I \cap J$. Le problème est de faire apparaitre des produits de deux éléments de A à partir de x. La possibilité la plus simple est d'écrire $x = 1.x$. Puisque I et J sont étrangers, alors $1 = i+j$ avec $i \in I$ et $j \in J$. Ainsi,
$$x = 1 \times x = (i+j) \times x = ix + xj$$
avec $ix \in I.J$ et $xj \in I.J$. Et donc $x \in I.J$.

Solution 4. 1. On commence par remarquer que si $x^n \in I$, alors pour tout $k \geq n$, $x^k = x^{k-n}x^n \in I$ (qui est un idéal). Montrons d'abord que $(\sqrt{I},+)$ est un sous-groupe de $(A,+)$. En effet, $0 \in \sqrt{I}$ puisque $\sqrt{I} \subset I$. De plus, si x est dans $\sqrt{I}$ alors $(-x)^n = (-1)^n x^n \in I$ puisque $x^n \in I$ et que I est

un idéal. Prenons maintenant x, $y \in I$ et $n, m \in \mathbb{N}$ tels que $x^n \in I$, $y^m \in I$. Alors, par la formule du binôme que l'on peut appliquer dans l'anneau **commutatif** A, on a

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Or, si $k \leq n$, alors $n+m-k \geq m$ et donc $y^{n+m-k} \in I$, ce qui entraine $x^k y^{n+m-k} \in I$. Si $k \geq n$, cette fois $x^k \in I$ et donc $x^k y^{n+m-k} \in I$. $(I,+)$ étant un sous-groupe de $(A,+)$, on en déduit que $(x+y)^{n+m} \in I$, c'est-à-dire $x+y \in \sqrt{I}$.
Finalement, prouvons que pour $a \in A$ et $x \in \sqrt{I}$, alors $ax \in \sqrt{I}$. Soit $n \geq 0$ tel que $x^n \in I$. Alors $(ax)^n = a^n x^n \in I$, ce qui prouve le résultat.

2. — Soit $x \in \sqrt{I.J}$. Il existe $n \geq 1$ tel que $x^n \in I.J$, c'est-à-dire $x^n = \sum_k a_k b_k$ avec $a_k \in I$ et $b_k \in J$. Alors $x^n \in I$ puisque I est un idéal et $x^n = ab$, $a \in I$, et de même $x^n \in J$ (on utilise en fait que $I.J \subset I \cap J$). Ainsi, $x \in \sqrt{I \cap J}$.
Soit maintenant $x \in \sqrt{I \cap J}$. Alors il existe $n \geq 1$ tel que $x^n \in I$ et $x^n \in J$. Donc $x \in \sqrt{I}$ et $x \in \sqrt{J}$, soit $x \in \sqrt{I} \cap \sqrt{J}$.
Finalement, soit $x \in \sqrt{I} \cap \sqrt{J}$. Alors il existe $n, m \geq 1$ tels que $x^n \in I$ et $x^m \in J$. Alors $x^{n+m} = x^n x^m \in I.J$, et donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I.J}$.

   — On a $I \subset \sqrt{I}$ et donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Réciproquement, prenons $x \in \sqrt{\sqrt{I}}$. Il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$. Posons $y = x^n \in \sqrt{I}$. Il existe $m \geq 1$ tel que $y^m \in I$. Alors, $x^{nm} = y^m \in I$ et donc $x \in \sqrt{I}$.

   — La dernière égalité se prouve de façon tout à fait identique !

3. Soit $x \in \mathbb{Z}$. x est dans $\sqrt{n\mathbb{Z}}$ si et seulement si il existe $n \geq 1$ tel que $x^n \in k\mathbb{Z}$. Autrement dit, $k | x^n$. Décomposons k en produits de facteurs premiers : $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. On obtient que $p_i | x^n \implies p_i | x$ pour tout $i = 1, \dots, r$ et donc $p_1 \dots p_r | x$, ce qui peut encore s'écrire $x \in (p_1 \dots p_r)\mathbb{Z}$. Réciproquement, si $x \in (p_1 \dots p_r)\mathbb{Z}$, alors, x s'écrit $x = p_1 \dots p_r m$. Notant $n = \max_{i \in \{1,\dots,r\}}(\alpha_i)$, on a $k | x^n$. Ainsi, on a prouvé que $\sqrt{I} = (p_1 \dots p_r)\mathbb{Z}$.

Solution 5.

1. Soit $I = n\mathbb{Z}$ un idéal de $\mathbb{Z}$. Si n n'est pas premier, alors n se factorise en ab avec $1 < a, b < n$. Mais, ou bien $a \in I$, ou bien $b \in I$ et donc a ou b est un multiple de n ce qui est une contradiction. Réciproquement, si n est premier et $xy \in I$, ie $n | xy$, alors, par le théorème de Gauss, $n | x$ ou $n | y$, ce qui prouve $x \in I$ ou $y \in I$. En résumé, $n\mathbb{Z}$ est un idéal premier si et seulement si n est premier.
2. On pose $K = \{a \in A;\ \exists i \in I,\ \exists k \in \mathbb{Z},\ a = i + kx\}$. On vérifie d'abord que K est un idéal et qu'il contient I et x. D'autre part, soit J' un idéal de A contenant I et x, et soit $a = i + kx$ un élément de K. Puisque $I \subset J'$, on a $i \in J'$ et puisque $x \in J'$, on a $kx \in J'$. Ainsi, $K \subset J'$: K est bien l'idéal engendré par I et x.
3. Soit I un idéal maximal et $x, y \in A$ tel que $x \notin I$. On doit prouver que $y \in I$. Pour cela, on considère J l'idéal engendré par I et x. Puisque I est maximal et que J est contient strictement I, on sait que $J = A$. Or, d'après la question précédente, tout élément de J s'écrit $i + kx$, $i \in I$ et $k \in \mathbb{Z}$. Ainsi, $1 = i + kx$. On multiplie par y et on obtient

$$y = yi + k(xy).$$

Mais $yi \in I$ car I est un idéal, $k(xy)$ aussi et donc y est aussi élément de I ce qui termine la démonstration.

4. On commence par démontrer que A est intègre. En effet, l'idéal engendré par 0 est premier. Donc, si $xy \in (0) = \{0\}$, alors $x = 0$ ou $y = 0$ et donc A est intègre. Soit ensuite $x \in A$ non nul. Il s'agit de démontrer que x est inversible. On considère I l'idéal engendré par x^2. Alors $x \times x \in I$ et donc il existe $b \in A$ tel que $x = bx^2$ puisque I est premier (d'où $x \in I$). On regroupe et on factorise en $x(1 - bx) = 0$. Puisque A est intègre et x est non-nul, on obtient $1 = bx$ et donc x est inversible d'inverse b.

5. Soit $I = (a)$ un idéal premier de A et soit J un idéal avec $I \subset J$. Puisque A est principal, $J = (b)$. Puisque $I \subset J$, $a = bc$ pour $c \in A$. Puisque I est premier, on a
   — ou bien $b \in I$, mais alors $(b) \subset I$ et donc $J = I$.
   — ou bien $c \in I$, donc c s'écrit xa et on a $a = bxa$. Puisque A est principal, donc intègre, ceci entraine $bx = 1$, c'est-à-dire que b est inversible et $J = A$.

   Ceci prouve que I est maximal.

Solution 6. L'application norme $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}, N(x + i\sqrt{5}y) = x^2 + 5y^2$ est multiplicative : $N(ab) = N(a)N(b)$.
Si $3 = ab$, alors $9 = N(a)N(b)$, dont on déduit $N(a) = 1$ ou $N(b) = 1$. Ce qui montre que soit a, soit b est inversible. Par contre, l'idéal (3) n'est pas premier car 3 divise le produit $(2 + i\sqrt{5})(2 - i\sqrt{5})$ mais aucun de ses facteurs (utilisez la norme).

Solution 7. Soit a un élément non-nul de A, et I_n l'idéal engendré par a^n. Alors $I_{n+1} \subset I_n$. En effet, si $x \in I_{n+1}$, x s'écrit $a^{n+1}u$, soit encore $a^n(au)$. Ainsi, la suite (I_n) est décroissante et donc stationnaire. Soit p un entier tel que $I_p = I_{p+1}$. En particulier, a^p est élément de I_{p+1}, c'est-à-dire que $a^p = a^{p+1}u$, $u \in A$. On peut réécrire ceci en $a^p(1 - au) = 0$ ce qui implique, car A est intègre et a, donc a^n, sont non-nuls, $1 - au = 0 \iff au = 1$. Ainsi, a est inversible. Comme a est arbitraire dans $A\backslash\{0\}$, A est un corps.

Solution 8. 1. Il est facile de montrer que $(\mathcal{P}(E), \Delta)$ est un groupe commutatif dont l'élément neutre est $\emptyset$, tout élément étant son propre symétrique. On démontre l'associativité de Δ à l'aide des fonctions caractéristiques des sous-ensembles de Elégèrement modifiées : χ_A est l'application de E dans $\mathbb{Z}/2\mathbb{Z}$ qui à tout $a \in E$ associe $\overline{1}$ si $a \in A$ et $\overline{0}$ sinon. ($\chi_{A\Delta B} = \chi_A + \chi_B$ et $\chi_{A\cap B} = \chi_A \cdot \chi_B$) ; de même pour la distributivité de $\cap$ sur Δ. L'élément neutre pour $\cap$ étant E.

2. (a) On note que $\emptyset \in J_a$, donc $J_a \neq \emptyset$. Si $A \in J_a$ et $B \in J_a$ alors $a \notin A$ et $a \notin B$ donc $a \notin A \cup B$ donc $a \notin A\Delta B$; donc $A\Delta B \in J_a$. D'autre part, Si $A \in J_a$ et $B \in \mathcal{P}(E)$ alors $a \notin A$ donc $a \notin A \cap B$ donc $A \cap B \in J_a$.

   (b) soit J un idéal de $(\mathcal{P}(E), \Delta, \cap)$ contenant strictement J_a. Il existe $C \in \mathcal{P}(E)$ tel que $C \in J$ et $C \notin J_a$, et donc $a \in C$ et $C \setminus \{a\} \in J_a$ d'où $C \setminus \{a\} \in J$. J étant un idéal de $\mathcal{P}(E)$, on en déduit que $C\Delta(C \setminus \{a\}) \in J$ c'est à dire $\{a\} \in J$. D'autre part, pour toute partie $P \in \mathcal{P}(E), P \setminus \{a\} \in J_a$, donc $P \setminus \{a\} \in J$ donc $(P \setminus \{a\})\Delta\{a\} \in J$, c'est à dire $P \in J$; ainsi $J = \mathcal{P}(E)$ et J_a est bien maximal.

Solution 9. L'idée est de procéder comme pour la résolution habituelle d'une équation du second degré. On applique donc la méthode qui conduit au discriminant, c'est-à-dire que l'on met le trinome sous forme canonique.

1. On peut remarque pour cette question que $\overline{14} = \overline{1}$. Ainsi,

$$x^2 + x + \overline{7} = \overline{0} \iff x^2 + \overline{14}x + \overline{7} = 0 \iff (x + \overline{7})^2 - \overline{42} = \overline{0}$$

   soit encore $(x + \overline{7})^2 = \overline{3}$. On remarque alors que $\overline{4}^2 = \overline{3}$. Ainsi, l'équation est équivalente à

$$(x + \overline{7})^2 - \overline{4}^2 = 0 \iff (x + \overline{7} + \overline{4})(x + \overline{7} - \overline{4}) = 0.$$

   Puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, et donc en particulier est intègre, ceci est encore équivalent à $x + \overline{11} = \overline{0}$ ou $x + \overline{3} = \overline{0}$. L'ensemble des solutions est donc $\{\overline{2}, \overline{10}\}$.

2. On procède de la même façon. L'équation est équivalente à

$$(x - \overline{2})^2 - \overline{1} = 0.$$

   On peut bien sûr factoriser encore et obtenir que l'équation est équivalente à

$$(x - \overline{2} - \overline{1})(x - \overline{2} + \overline{1}) = 0.$$

Mais cette fois, **on ne peut pas aller plus loin** car $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. Il faut plutôt écrire $(x-\overline{2})^2 = \overline{1}$ et chercher les t dans $\mathbb{Z}/12\mathbb{Z}$ avec $t^2 = \overline{1}$. Pour cela on dresse le tableau :

t	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
t^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$-\overline{3}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

(on a bien sûr $(-t)^2 = t^2$). Ainsi, l'équation est équivalente $x - \overline{2} \in \{-\overline{5}, -\overline{1}, \overline{1}, \overline{5}\}$. L'ensemble des solutions est donc $\{-\overline{5}, -\overline{3}, \overline{1}, \overline{5}\}$.

Solution 10.

1. Supposons qu'il en existe simplement un nombre fini, notés $p_1, \ldots, p_k$ et considérons n le produit de tous ces nombres :
$$n = p_1 \times \cdots \times p_k = 3 \times 7 \times 11 \times 19 \times \ldots.$$
Considérons alors $m = 4n - 1$, qui est un nombre impair. Alors m est congru à 3 modulo 4. D'autre part, aucun des p_i ne divise m sinon, puisqu'il divise n, il diviserait aussi 1 ce qui est impossible. Donc m est le produit de facteurs premiers $q_1 \ldots q_p$ qui sont tous congrus à 1 modulo 4 (ils sont impairs). Donc m est congru à 1 modulo 4, une contradiction.
2. Il n'existe pas de nombre premiers entre $n! + 2$ et $n! + n$.

Solution 11. Posons $u_n = (3 - \sqrt{5})^n + (3 + \sqrt{5})^n$. L'idée est de prouver que la suite (u_n) vérifie une relation de récurrence d'ordre 2. En effet, elle est de la forme $u_n = r_1^n + r_2^n$. D'après la théorie des suites récurrentes linéaires, (u_n) vérifie l'équation de récurrence linéaire dont l'équation caractéristique associée est
$$X^2 - (r_1 + r_2)X + r_1 r_2 = 0 \iff X^3 - 6X + 4 = 0.$$
Autrement dit, on a $u_{n+2} = 6u_{n+1} - 4u_n$. Bien sûr, on peut vérifier directement que la suite (u_n) satisfait cette condition de récurrence.
On prouve alors par récurrence sur n que 2^n divise u_n. C'est vrai pour $n = 0$, car $u_0 = 2$ et pour $n = 1$, car $u_1 = 6$. Supposons que $2^n | u_n$ et $2^{n+1} | u_{n+1}$. Alors, écrivant $u_n = k2^n$ et $u_{n+1} = l2^{n+1}$, on a
$$u_{n+2} = 2 \times 3 \times l2^{n+1} - 2^2 \times k2^n = 2^{n+2}(3l - k).$$
Ceci prouve le résultat demandé.

Solution 12.

1. Si $2|n$, alors $2|2^n - 1$ et donc $2^n - 1$ est pair, ce qui n'est pas le cas.
2. (a) Puisque p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe de cardinal $p - 1$. D'après le théorème de Lagrange, l'ordre de tout élément divise $p - 1$. Donc $m|p - 1$.
   (b) Par hypothèse, $2^n \equiv 1\ [n]$ ce qui entraîne $2^n \equiv 1\ [p]$, ou encore $2^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. n est donc un multiple de l'ordre de 2, ou encore $m|n$.
   (c) Puisque p est le plus petit facteur premier de n, on a $n \wedge (p-1) = 1$. Ainsi, $m|\text{pgcd}(p-1, n) = 1$, et donc $m = 1$. C'est absurde puisque $2 \neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$, $p \geq 3$. Il est donc impossible que n divise $2^n - 1$.

Solution 13.

1. L'équation $x^2 = 1$ est équivalente à $(x - 1)(x + 1) = 0$, ce qui est équivalent à dire, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, $x = 1$ ou $x = -1$.
2. Travaillons dans $\mathbb{Z}/p\mathbb{Z}$. Tout élément de $\{\overline{1}, \ldots, \overline{p-1}\}$ est inversible et son inverse est différent de lui-même, sauf pour $\overline{1}$ et $\overline{-1}$ d'après la question précédente. Dans le produit $\overline{2} \times \cdots \times \overline{p-2}$, on peut donc regrouper chaque élément avec son inverse, et on trouve que
$$\overline{1} \times \cdots \times \overline{p-1} = \overline{1} \times \overline{p-1} = \overline{-1}$$
ce qui est le resultat attendu.
3. Soit $a \in \{1, \ldots, n-1\}$. Alors a est un facteur de $(n-1)!$ et donc il existe k tel que $(n-1)! = ak$. On en déduit $a \times (-k) \equiv 1\ [n]$, et donc a est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Par le théorème de Bézout, ceci signifie que a est premier avec n, et ceci est vrai pour tout a de $\{1, \ldots, n-1\}$. Autrement dit, n est premier.

Solution 14. 1. Soit $k \in A_d$. Alors k s'écrit $d \times l$, avec $l \wedge \dfrac{n}{d} = 1$ et $1 \leq ld \leq n$ ce qui entraîne $1 \leq l \leq \frac{n}{d}$ (remarquons que $\frac{n}{d}$ est entier).
Réciproquement, tout entier $k = d \times l$ avec $l \wedge \frac{n}{d} = 1$ et $1 \leq l \leq \frac{n}{d}$ est élément de A_d. On en déduit que

$$\text{card}(A_d) = \phi\left(\frac{n}{d}\right).$$

2. Il est clair que les ensembles A_d, pour $d|n$, forment une partition de $\{1, \ldots, n\}$. Ainsi, on a

$$n = \sum_{d|n} \text{card}(A_d) = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

Pour obtenir la dernière inégalité, on a effectué le changement de variables $d' = n/d$.

Solution 15. Il faut traduire ceci en termes de congruences. On a :

$$\begin{cases} x & \equiv & 3\ [17] \\ x & \equiv & 4\ [11] \\ x & \equiv & 5\ [6] \end{cases}$$

On remarque que 37 est tel que $37 \equiv 3\ [17]$ et $37 \equiv 4\ [11]$. Puisque $17 \wedge 11 = 1$, on sait d'après le théorème chinois que

$$\begin{cases} x & \equiv & 3\ [17] \\ x & \equiv & 4\ [11] \end{cases} \iff x \equiv 37[187].$$

On doit donc résoudre le système

$$\begin{cases} x & \equiv & 37\ [187] \\ x & \equiv & 5\ [6]. \end{cases}$$

Or, $1 = 1 \times 187 - 6 \times 37$. L'ensemble des solutions de ce système est donc :

$$\{37 + 187 \times 1 \times (5 - 37) + 1122k;\ k \in \mathbb{Z}\} = \{-5947 + 1122k;\ k \in \mathbb{Z}\}.$$

Le plus petit entier positif est obtenu pour $k = 6$ et donne 785. Le cuisinier est sûr d'obtenir au moins 785 pièces d'or.

Solution 16. 1. L'application $x \mapsto \dfrac{1}{x}$ est involutive donc bijective. Le groupe étant commutatif, c'est un morphisme de groupes.

2. En faisant une réindexation $\displaystyle\sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=1}^{p-1} \frac{1}{p-i}$ et donc

$$2 \times \sum_{i=1}^{p-1} \frac{1}{i} = \sum_{i=1}^{p-1} \frac{p}{i(p-i)} \Rightarrow \frac{2m}{(p-1)!} = \sum_{i=1}^{p-1} \frac{p}{i(p-i)}.$$

Comme p est premier impair, on en déduit que $p|m$: $m = m'p$ d'où

$$\frac{2m'}{(p-1)!} = \sum_{i=1}^{p-1} \frac{1}{i(p-i)}.$$

Or, $(p-1)! \equiv -1 \mod (p)$ et $i(p-i) = -i^2$. Comme φ est bijective :

$$2m' \equiv \sum_{i=1}^{p-1} i^2 \mod p \equiv \frac{p(p+1)(2p+1)}{6} \mod p \equiv 0 \mod p.$$

On utilise que p est premier avec 6, car nombre premier ≥ 5.

Solution 17. Soir $\deg P = n$. On calcule $\dfrac{P'}{P} = \dfrac{n}{X-a}$.

Puis $\left(\dfrac{P}{(X-a)^n}\right)' = 0$, d'où $P = \lambda(X-a)^n$.

Ou encore utiliser $\dfrac{P'}{P} = \displaystyle\sum_{k=1}^{l} \frac{\alpha_i}{x-a_i}$ où a_i sont les racines de P de multiplicité α_i. On en déduit que a est l'unique racine de multiplicité n.

Solution 18. 1. (a) Soit z une racine de P. L'équation vérifiée par P s'écrit aussi $P\big((X+1)^2\big) = P(X)P(X+2)$, et donc $(z+1)^2$ est aussi racine de P. De même, $(z-1)^2$ est aussi racine de P. On va prouver qu'au moins un des deux nombres complexes $(z+1)^2$ ou $(z-1)^2$ est de module supérieur strict à z. En effet, $(z+1)^2 - (z-1)^2 = 4z$, et donc

$$4|z| \leq |z+1|^2 + |z-1|^2.$$

Ainsi, l'un de ces deux nombres complexes est de module supérieur ou égal à $2|z|$. Si $|z| \neq 0$, le résultat est prouvé. Sinon, si $z = 0$, le résultat est trivial.

(b) Si P admet une racine (complexe), alors il en admet d'après la question précédente une infinité. C'est donc le polynôme nul. Les polynômes qui sont solutions de l'équation ne peuvent donc être que des polynômes constants, et les seuls polynômes constants solutions sont les polynômes $P(X) = 0$ et $P(X) = 1$.

2. (a) En raisonnant comme dans le premier cas, on voit que si z est racine de P, alors z^2 et $(z+1)^2$ sont aussi solutions. Par récurrence, z^{2n} et $(z+1)^{2n}$ seront racines pour tout entier n. Puisque le polynôme n'admet qu'un nombre fini de racines, les suites $(z^{2n})_n$ et $\big((z+1)^{2n}\big)_n$ ne peuvent prendre qu'un nombre fini de valeurs. Le premier point nous dit qu'on a nécessairement $z = 0$ ou $|z| = 1$. On note Γ_1 cet ensemble. Le second point nous dit que $z = -1$ ou $|z+1| = 1$, ensemble que l'on note Γ_2. Il est facile de vérifier (par exemple, en dessinant ses ensembles), que les points d'intersection de Γ_1 et Γ_2 sont $0, 1, j$ et j^2. Mais si $z = 0$ est racine, alors $(z+1)^2 = 1$ est aussi racine, ce qui n'est pas possible. De même, si $z = -1$ est racine, alors $(z+1)^2 = 0$ est racine, ce qui n'est pas (plus) possible. Donc les seules racines de P sont j et j^2.

(b) Puisque P est à coefficients réels, j et j^2, qui sont des complexes conjugués, doivent être des racines de même multiplicité. On doit donc avoir $P(X) = \lambda(X-j)^n(X-j^2)^n = \lambda(X^2+X+1)^n$. Par identification des coefficients dominants, on trouve $\lambda = 1$. Réciproquement, on vérifie facilement que les polynômes $P(X) = (X^2+X+1)^n$ sont solutions de l'équation.

Solution 19. Une idée possible est d'appliquer l'algorithme d'Euclide pour calculer le pgcd de ces deux polynômes. On suppose par exemple $n > m$, et on écrit $n = mq + r$, avec $0 \leq r < m$. Alors on a :

$$X^n - 1 = X^{mp+r} - 1 = X^r(X^{mp} - 1) + X^r - 1.$$

Le point crucial est que $X^{mp} - 1$ est divisible par $X^m - 1$. En effet,

$$X^{mp} - 1 = (X^m - 1)(X^{m(p-1)} + X^{m(p-1)} + \cdots + X^m + 1).$$

Ainsi, $\operatorname{pgcd}(X^n - 1, X^m - 1) = \operatorname{pgcd}(X^m - 1, X^r - 1)$. Mais puisque $\operatorname{pgcd}(n, m) = \operatorname{pgcd}(m, r)$, on en déduit finalement que

$$\operatorname{pgcd}(X^n - 1, X^m - 1) = X^{\operatorname{pgcd}(n,m)} - 1.$$

Solution 20.

1. Si $z = x + iy$ et $z' = x' + iy'$, alors $(xx' - yy')^2 + (xy' + x'y)^2 = (x^2+y^2)(x'^2+y'^2)$ dont on déduit que si $P = Q^2 + R^2$ et $P' = Q'^2 + R'^2$, alors $PP' = (QQ' - RR')^2 + (QR' + Q'R)^2$.
Cela nous permet de procéder par récurrence sur le degré de P pour la seconde partie. Tout d'abord, si P est un polynôme tel que $P(t) \geq 0$ pour tout $t \in \mathbb{R}$, alors les limites en $\pm\infty$ montrent que P est de degré pair et de coefficient dominant positif.

Si P est un polynôme contant $P=\alpha\geq 0$, alors $P=(\sqrt{\alpha})^2+0$.
Si P est de degré 2 unitaire $P=a^2(X^2+2bX+c)$, alors $P=(a(X+b))^2+a^2(c-b^2)$. En évaluant en $X=-b$, on obtient $c-b^2\geq 0$ et donc $P=(a(x-c))^2+(a\sqrt{c-b^2})^2$ et la propriété est vérifiée.
Supposons que la propriété est vraie pour tout polynôme de degré $2n\geq 2$, et soit P de degré $2(n+1)$ tel que $P(t)\geq 0$ pour tout $t\in\mathbb{R}$. Si P admet une racine réelle a de multiplicité impaire, alors P s'annule et change de signe au voisinage de a, ce qui est contradictoire ; donc toutes les racines réelles de P sont de multiplicité paires. On en déduit que décomposition en polynôme irréductible :

$$P=\alpha\prod_{k=1}^{n}(X-a_i)^{2n_i}\prod_{k=1}^{m}(X^2+b_iX+c_i)^{2m_i}$$

et par hypothèse de récurrence chacun des facteurs vérifent la propriété de l'énoncé et par récurrence se décompose en une somme de deux carrées de polynôme. mais la formule préliminaire montre alors que P se décompose aussi comme un produit de deux carrés.

2. On procède de même en écrivant que

$$(A^2+(\sqrt{X}B)^2)(C+(\sqrt{X}D)^2)=(AC-XBC)^2+X(AD+BC)^2.$$

Ce qui permet de precéder à nouveau par récurrence sur le degré.
Pour les polynômes de degré 0, $P=\alpha=(\sqrt{\alpha})^2$.
Si P est de degré 1, alors $P=\alpha X+\beta$, avec $\alpha,\beta\geq 0$ et $P=(\sqrt{\alpha})^2+X(\sqrt{\beta})^2$.
Si P est de degré 2, soit c'est un carré, soit c'est produit de deux polynômes de degré à racines négatives, et la formule précédente montre que le produit s'écrit dans ces deux cas comme attendu.
Enfin si c'est un polynôme irréductible de degré 2 à racines complexes conjuguées non réelles, alors $P=X^2+2aX+b$ avec $a^2-b<0$. Soit $\alpha=a-\sqrt{b}<0$, $P=(X+a+\alpha)^2-2\alpha X$, d'où la déomposition.
Enfin tout polynôme de degré ≥ 2 s'cérit comme produit de polynômes de degré 0,1,2 vérifiant la propriété et on conclut comme précédemment.

Solution 21.

1. Soit P un tel polynôme non constant (sinon $P=\pm 1$) de degré $n\geq 1$.
Alors $P(e^{i\theta})\overline{P(e^{i\theta})}=1$ donc

$$P(X)\big(X^n\overline{P}(\frac{1}{X})\big)=X^n$$

avec $X^n\overline{P}(1/X)$ polynôme de degré d tel que $n+d=n$, donc $d=0$.
On en déduit facilement que $P=uX^n$ avec $|u|=1$.

2. On écrit $F=\dfrac{P}{Q}$ avec P et Q premiers et P unitaire $\deg P=d$, $\deg Q=d'$. De plus, quitte à factoriser P ou Q par X^l, on peut supposer que $X\not| P$ et $X\not| Q$.
Comme précédemment

$$\frac{P(X)}{Q(X)}\frac{X^d\overline{P}(1/X)}{X^{d'}\overline{Q}(1/X)}=X^{d-d'}$$

On en déduit $2d-2d'=d-d'$ puis $d=d'$ et

$$P(X)\left[X^d\bar{P}(1/X)\right]=Q(X)\left[X^d\bar{Q}(1/X)\right].$$

On en déduit comme P et Q sont premiers que P divise $X^{d'}\bar{Q}(1/X)$ et Q divise $X^{d'}\bar{P}(1/X)$.
On a donc $Q=cX^d\bar{P}(1/X)$ et comme $F(1)\in\mathbb{U}$, on en déduit que $c\in\mathbb{U}$.
Les fractions rationnelles sont donc de la forme $F=cX^k\dfrac{P(X)}{X^d\overline{P}(1/X)}$.
Si $|\omega|\neq 1$, alors $F(z)=\dfrac{z-\omega}{1-\overline{\omega}z}$ vérifie la propriété.

Solution 22.

1. Si $P = RS$, alors $R(a_i)S(a_i) = -1$ donc $R + S$ s'annule en a_i. Si R et S sont de degré strictement inférieur à n, alors $R + S = 0$, ce qui donne $P = -S^2$. On obtient une contradiction en faisant tendre x vers $+\infty$.
2. De même $R - S = 0$ et $Q = R^2$, donc de degré pair et alors

$$R^2 - 1 = (R-1)(R+1) = (X - a_1)\cdots(X - a_n) \quad (*).$$

- Si $n = 2$, $Q = (X - a_1)(X - a_2) + 1 = R^2$ implique que le polynôme de degré 2 a un discriminant nul :

$$\Delta = (a_1 + a_2)^2 - 4(1 + a_1a_2) = (a_1 - a_2 + 2)(a_1 - a_2 - 2) = 0$$

et alors la racine double vaut $a_1 \pm 1$. Donc Q est réductible ssi $a_2 = a_1 + 2$ (quitte à intervertir a_1 et a_2) et alors $Q = \big(X - (a_1 + 1)\big)^2$.

- Si $n = 4$, alors $Q = (X-a_1)\cdots(X-a_4)+1 = R^2 = (X^2+\alpha X+\beta)^2$ avec R polynôme irréductible car si a_1 et a_2 sont les racines de $R + 1$, la question 1/ nous dit que $R = (X - a_1)(X - a_2) - 1$ est irréductible. D' après $(*)$, $R = (X - a_3)(X - a_4) + 1$, donc

$$\begin{cases} a_1 + a_2 = a_3 + a_4 \\ a_1a_2 - 1 = a_3a_4 + 1 \end{cases} \iff \begin{cases} a_4 = a_1 + a_2 - a_3 \\ a_3^2 - (a_1 + a_2)a_3 + a_1a_2 - 2 = 0 \end{cases} \iff \begin{cases} a_1 + a_2 = a_3 + a_4 \\ a_3 = \dfrac{a_1 + a_2 \pm \sqrt{(a_1 - a_2)^2 + 8}}{2} \end{cases}$$

Commer a_3 doit être un entier, il faut que $(a_1 - a_2)^2 + 8$ soit un carré, ce qui implique $a_2 = a_1 + 1$ (quitte à intervertir a_1 et a_2). On en déduit $a_3 = a_1 + 2$ et $a_4 = a_1 - 1$ (quitte à intervertir a_3 et a_4). La condition est nécessaire et suffisante et on a

$$P = (X - a + 1)(X - a)(X - a + 1)(X - a + 2) + 1 = [(X - a)(X - a + 1) - 1]^2$$

- si n impair, $P = R^2$ est impossible, donc P est irréductible.

-si $n = 2p > 4$ pair, d'après $(*)$ et quitte à réordonner les a_i on peut

$$R + 1 = \prod_{k=1}^{p}(X - a_k) \quad R - 1 = \prod_{k=p+1}^{n}(X - a_k)$$

Pour tout $i \in [\![1, p]\!]$, $R(a_i) = 1 = \prod_{k=p+1}^{n}(a_i - a_k)$. Or les $a_i - a_k$ sont des entiers dont le produit fait 1, donc $p \leq 2$ (cf cas précédents). On en déduit que P est bien irréductible.

Solution 23. La matrice transposée de la comatrice de A, notée $\tilde{A}$, est à coefficients entiers (ses coefficients sont au signe près des déterminants de matrices à coefficients entiers). De plus $A\tilde{A} = \det A I_n$. D'après le théorème de Bézout, il existe des entiers p et q tels que $p \det A + q \det B = 1$. On obtient une solution avec $U = p\widetilde{A}$ et $V = q\widetilde{B}$.

Solution 24. On suppose que $P = QR$ avec $Q = \sum_0^d b_k X^k$ et $R = \sum_0^{d'} c_k$. Comme $a_0 = b_0c_0$, p ne divise qu'un seul des entiers b_0 et c_0 car $p^2 \not| a_0$.
Supposons que $p|b_0$ et si p divise b_0, ...,b_{k-1}, alors on montre que $p|b_k$, donc p divise tous les coefficients b_k ce qui est absurde car P unitaire.

Solution 25.

1. L'algorithme d'Euclide nous donne l'existence d'un tel couple. Si vous n'aviez pas remarqué que le couple (R, S) vérifie alors les conditions de degré, reprenez l'algorithme en Python du cours et demandez-vous quelle condition rajouter sur le couple (u, v) ?
Pour l'unicité, quitte à diviser par P et Q par $P \wedge Q$, on peut supposer P et Q premiers entre eux. Si l'on a un second couple (R_1, Q_1) qui satisfait les conditions, alors

$$PR + QS = PR_1 + QS_1 \Rightarrow P(R - R_1) = Q(S_1 - S) \underset{(P\wedge Q)=1}{\Rightarrow} P|(S_1 - S) \text{ et } Q|(R - R_1).$$

Or, par hypothèse, $\deg(S_1 - S) < \deg P$ et $\deg(R - R_1) < \deg S$. On en déduit $R = R_1$ et $S = S_1$.

2. On calcule l'image de $(X^{n-l}, 0)$ pour $l \in [\![1, n]\!]$:

$$\varphi(X^{n-l}, 0) = X^{n-l} \times P = \sum_{k=0}^{m} a_k X^{k+n-l}$$

On en déduit que la l-ième colonne est

$$(0 \ \cdots 0 \underbrace{a_m}_{\deg=m+n-l} \cdot \underbrace{a_0}_{\deg=n-l}^{m+l} 0 \cdots \ 0)^T.$$

Le calcul est identique pour $\varphi(0, X^{m-l})$, $l \in [\![1, m]\!]$.

3. φ est bijective alors elle est surjective et si $\varphi^{-1}(0 \cdots 0 \ 1) = (R, S)$, alors $PR + QS = 1$ et donc $P \wedge Q = 1$.
Récirpoquement, si $P \wedge Q = 1$, alors $\varphi(R, S) = 0$ si et seulement si $PR = -QS$, d'où $Q|R$ et $P|S$. Par hypothèse sur les degrés, $R = S = 0$. On en déduit que φ est injective. Pour des raisons de dimension, φ est bijective.
Comme une matrice est inversible si et seulement si son déterminant est non nul, on en déduit le résultat.

4. Dans $\mathbb{C}[X]$ un polynôme est scindé à racines simples si et seulement si $P \wedge P' = 1$. Donc si et seulement si $Res(P, P') \neq 0$. Or, l'application $P \mapsto Res(P, P')$ est clairement polynomiale en les coefficients de P. Elle est donc continue. L'image réciproque de l'ouvert $\mathbb{C}^*$ par cette application est un ouvert, et c'est exactement l'ensemble des polynômes scindé à racines simples.