J. FRESLON | S. GUGGER | D. FREDON | J. POINEAU | C. MORIN

MATHS MP

j'intègre

EXERCICES INCONTOURNABLES

3e édition

DUNOD

Conception et création de couverture : Hokus Pokus Créations

11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-077663-4

Avant-propos

Cet ouvrage s'adresse aux élèves de deuxième année de classes préparatoires scientifiques de la filière MP. Il leur propose de mettre en pratique les notions abordées en cours de mathématiques par le biais d'exercices, assortis d'une correction détaillée, dans laquelle l'accent est mis sur la méthode qui mène à la solution.

Le livre est divisé en quinze chapitres, chacun étant consacré à une partie du programme. Nous avons regroupé les chapitres selon les thèmes classiques : Algèbre, Topologie, Analyse et Probabilités. Au sein d'un même chapitre, les exercices, classés par ordre croissant de difficulté, ont été choisis de façon à passer en revue les notions à connaître, mais aussi à présenter les techniques susceptibles d'être utilisées.

En ce qui concerne les corrections, nous avons choisi de séparer clairement la réflexion préliminaire, comprenant analyse du problème et tâtonnements, de la rédaction finale, rigoureuse et précise. Cette dernière étape est signalée, dans le texte, par la présence d'un liseré gris sur la gauche et du pictogramme  . Insistons sur le fait que nous ne prétendons nullement présenter l'unique cheminement permettant d'aboutir à la solution d'un exercice donné, ni la seule rédaction acceptable. Dans les deux cas, bien des possibilités existent.

Par ailleurs, lorsque nous avons souhaité mettre en lumière un point important, nous l'avons rédigé sur un fond grisé et indiqué par  . De même, la présence d'un piège dont il faut se méfier est signalée par  .

Nous remercions Sabrina Bergez, qui a collaboré à la réalisation de ce livre en le relisant en détail et en nous faisant bénéficier de ses nombreuses remarques pertinentes.

Table des matières

Algèbre

Topologie

Analyse

Probabilités

Partie 1

Algèbre

Algèbre

CHAPITRE

Structures algébriques usuelles

1

Exercice 1.1 : Groupe engendré par deux éléments

Soient $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.
Quel est le groupe engendré par A et B ?

Il s'agit d'éléments de $\mathscr{M}_3(\mathbb{R})$. La loi n'est pas précisée. Mais pour l'addition le groupe engendré serait l'ensemble des matrices $pA + qB$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$. Il n'y aurait donc aucun problème : c'est le produit de matrices qu'il faut considérer. Le groupe dans lequel on se place est celui des matrices carrées inversibles d'ordre 3.

Lorsqu'il s'agit de groupes usuels, les énoncés ne prendront généralement pas la peine de préciser la loi utilisée. Lorsque deux lois sont possibles, il faut étudier pour laquelle la question posée a le plus de sens.

Le groupe engendré par A et B est le plus petit (au sens de l'inclusion) sous-groupe contenant les deux matrices. Il est constitué par tous les produits possibles avec A, B et leurs inverses. Remarquons que A et B sont bien inversibles puisque $\det A = -1$ et $\det B = 1$.

Le groupe G cherché contient A et B. Il contient aussi $A^2 = I_3$, ce qui implique que $A^{-1} = A$, $B^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $B^3 = I_3$, ce qui implique que l'on a $B^{-1} = B^2$. On en déduit alors que pour tout $n \in \mathbb{Z}$, $A^n \in \{I_3, A\}$ et que pour tout $p \in \mathbb{Z}$, $B^p \in \{I_3, B, B^2\}$.

Il reste à calculer les produits de A et de B. On a $AB = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ et $BA = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = AB^2$. Ainsi tout élément de G peut s'écrire sous la

forme A^nB^p, $(n,p) \in \mathbb{Z}^2$ (puisqu'on peut commuter A et B en augmentant la puissance de B).
Avec la remarque plus haut, les éléments de G sont les A^nB^p avec $n \in \{0,1\}$ et $p \in \{0,1,2\}$ et

$$G = \{I_3, B, B^2, A, AB, AB^2\}.$$

A et B sont des matrices associées à des permutations des vecteurs de la base canonique (e_1, e_2, e_3) : A est associée à la transposition $\tau_{2,3}$, B au cycle $(1,2,3)$.
Ces deux permutations engendrent $\mathscr{S}_3$, donc G est l'ensemble des six matrices de permutation de la base (e_1, e_2, e_3).

Exercice 1.2 : Centre du groupe symétrique

Démontrer que le centre du groupe symétrique $\mathscr{S}_n$ (c'est-à-dire l'ensemble des éléments de $\mathscr{S}_n$ qui commutent avec tous les éléments de $\mathscr{S}_n$) est réduit à $\{\mathrm{Id}\}$ pour $n \geqslant 3$.

Il faut bien se souvenir que la loi d'un groupe n'est pas, en général, commutative !

Il est clair que Id commute avec tous les éléments de $\mathscr{S}_n$, il faut donc montrer que si une permutation σ commute avec tous les éléments de $\mathscr{S}_n$, c'est l'identité. On raisonne par l'absurde.

Supposons qu'il existe une permutation σ différente de l'identité appartenant au centre de $\mathscr{S}_n$. Il existe alors $a \neq b$ tels que $\sigma(a) = b$.
Introduisons la transposition $\tau_{a,b}$. On a alors : $\sigma \circ \tau_{a,b}(b) = \sigma(a) = b$. Comme σ commute avec tout élément de $\mathscr{S}_n$, on aussi : $\tau_{a,b} \circ \sigma(b) = b$ d'où $\sigma(b) = a$.
Introduisons le cycle $c_{a,b,c}$, avec c distinct de a et b, ce qui est possible car $n \geqslant 3$. On a :

$$\sigma \circ c_{a,b,c}(a) = \sigma(b) = a \text{ et } c_{a,b,c} \circ \sigma(a) = c_{a,b,c}(b) = c.$$

On obtient une contradiction, donc le centre de $\mathscr{S}_n$ est inclus dans $\{\mathrm{Id}\}$. L'inclusion réciproque étant claire, on a le résultat voulu.

Exercice 1.3 : Conjugaison

Soit G un groupe. Pour $a \in G$, on note $f_a : G \to G$, $x \mapsto a^{-1}\,x\,a$.
1. Montrer que pour tout $a \in G$, f_a est un automorphisme de G.
2. Montrer que $\varphi : G \to \mathrm{Aut}(G)$, $a \mapsto f_a$ est un morphisme de groupes.
3. Déterminer le noyau de φ.

1. La loi du groupe G n'est pas précisée, mais vu la définition de f_a, elle est notée comme une multiplication.
Pour $a \in G$, il faut montrer, d'une part que f_a est un morphisme de groupes, d'autre part qu'il est bijectif. Pour le premier point, on vérifie la définition, pour le second on choisit ici de résoudre l'équation $f_a(x) = y$.

Soit $a \in G$. Pour $(x, y) \in G^2$, on a
$f_a(x)\,f_a(y) = (a^{-1}\,x\,a)\,(a^{-1}\,y\,a) = (a^{-1}\,x)\,(a^{-1}\,a)\,(y\,a) = a^{-1}\,x\,y\,a = f_a(x\,y)$
par associativité de la multiplication dans G. Ainsi f_a est un endomorphisme du groupe G.
Soit $y \in G$, l'équation $f_a(x) = y$, d'inconnue $x \in G$, équivaut à $a^{-1}\,x\,a = y$, si et seulement si $a\,(a^{-1}\,x\,a) = a\,y$, i.e. $x\,a = a\,y$, i.e. $(x\,a)\,a^{-1} = a\,y\,a^{-1}$, i.e. $x = a\,y\,a^{-1}$. On a donc une unique solution, et f_a est une bijection de G dans G. Ainsi f_a est un automorphisme du groupe G.

2. La loi du groupe $\mathrm{Aut}(G)$ est la loi $\circ$. Il faut donc montrer que pour $(a, b) \in G^2$, $\varphi(a\,b) = \varphi(a) \circ \varphi(b)$, c'est-à-dire $f_{a\,b} = f_a \circ f_b$.

Ici φ est une fonction qui renvoie des fonctions. Il faut bien faire attention au type des objets manipulés, et ne pas confondre argument de φ ou argument de f_a.

Soit $(a, b) \in G^2$. Pour $x \in G$, on a
$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b^{-1}\,x\,b) = a^{-1}\,b^{-1}\,x\,a\,b = (a\,b)^{-1}\,x\,a\,b = f_{a\,b}(x)$.
Ainsi $f_a \circ f_b = f_{a\,b}$, puis $\varphi(a\,b) = \varphi(a) \circ \varphi(b)$. φ est donc un morphisme de groupes.

3. Le noyau de φ est l'ensemble des éléments de G qui sont envoyés sur le neutre de $\mathrm{Aut}(G)$, ici Id_G. On cherche donc les $a \in G$ tel que $\varphi(a) = \mathrm{Id}_G$.

Le neutre n'est pas toujours le même dans tous les groupes, il faut donc faire attention au neutre du groupe d'arrivée lors d'un calcul de noyau.

Pour $a \in G$, on a $a \in \operatorname{Ker}\varphi$ si et seulement si $\varphi(a) = \mathrm{Id}_G$, c'est-à-dire $f_a = \mathrm{Id}_G$. $a \in \operatorname{Ker}\varphi$ est donc équivalent à $\forall x \in G$, $a^{-1}\,x\,a = x$ i.e. $x\,a = a\,x$. Ainsi $\operatorname{Ker}\varphi$ est le centre de G, c'est-à-dire l'ensemble des éléments a de G qui commutent avec tous les éléments de G.

Exercice 1.4 : Partie génératrice du groupe orthogonal

Soit E un espace euclidien.
1. Soit a et b deux vecteurs distincts de E de même norme. Démontrer qu'il existe une unique réflexion s de E telle que $s(a) = b$ et $s(b) = a$.
2. Montrer que $O(E)$ est engendré par les réflexions.
On pourra montrer par récurrence sur $\dim(E) - \dim(\operatorname{Ker}(f - \mathrm{Id}_E))$ que f peut s'écrire comme composée de réflexions.

$O(E)$ est le groupe des endomorphismes orthogonaux de E, c'est-à-dire les endomorphismes qui conservent le produit scalaire et la norme.
En première année, on a vu le cas $n = 2$. À cette occasion, il a été démontré que le groupe orthogonal du plan est engendré par les réflexions. C'est cette propriété que l'on va généraliser.

1. Pour montrer l'existence et l'unicité, on va raisonner par analyse/synthèse : comme il est nécessaire d'avoir $s(a-b) = s(a) - s(b) = b - a = -(a-b)$, ceci impose que l'hyperplan de la réflexion soit $(a-b)^\perp$.

► **Analyse :**
On suppose avoir une réflexion qui convient, et à partir des propriétés qu'elle vérifie, on obtient ses éléments caractéristiques.

Supposons avoir une réflexion s qui échange a et b.
On a alors $a - b \in \operatorname{Ker}(s + \mathrm{Id}_E)$. Or s est une réflexion donc $\operatorname{Ker}(s + \mathrm{Id}_E)$ est une droite et son orthogonal est $\operatorname{Ker}(s - \mathrm{Id}_E)$ qui est de dimension $n - 1$. Ainsi, s est nécessairement la réflexion par rapport à l'hyperplan $(a-b)^\perp$, et on a l'unicité.

► **Synthèse :**
On pose la forme trouvée à la fin de l'analyse, et on vérifie qu'elle convient bien.

Comme $a \neq b$, on a $a - b \neq 0$. L'orthogonal du vecteur $a - b$ est donc un hyperplan H. Soit s la réflexion par rapport à H. Alors $s(a-b) = -(a-b)$

donc $s(a) - s(b) = b - a$. Par ailleurs,

$$\begin{aligned}\langle a-b|a+b\rangle &= \langle a|a\rangle - \langle b|a\rangle + \langle a|b\rangle - \langle b|b\rangle \\ &= \langle a|a\rangle - \langle b|b\rangle\end{aligned}$$

car $\langle a|b\rangle = \langle b|a\rangle$ (le produit scalaire est symétrique).
Comme a et b sont de même norme, $\langle a|a\rangle = \langle b|b\rangle$, donc $a-b$ et $a+b$ sont orthogonaux ; ainsi, $a+b \in H$ et $s(a+b) = a+b$, soit $s(a)+s(b) = a+b$.
On en déduit $s(a) = b$ et $s(b) = a$ et on a l'existence.

2. Comme donné en indication, on raisonne par récurrence sur l'entier

$$k = \dim(E) - \dim(\mathrm{Ker}(f - \mathrm{Id}_E)).$$

L'initialisation correspond donc au cas où $\mathrm{Ker}(f-\mathrm{Id}_E) = E$, soit $f = \mathrm{Id}_E$, ce qui est facile. Pour l'hérédité, on doit donc trouver, à partir de f, une fonction g telle que $\mathrm{Ker}(g-\mathrm{Id}_E)$ soit strictement plus grand que $\mathrm{Ker}(f-\mathrm{Id}_E)$. Pour utiliser la question 1, on pense alors à échanger a et $f(a)$, si a est un vecteur qui n'est pas dans $\mathrm{Ker}(f-\mathrm{Id}_E)$. On a une réflexion s qui fait ceci, et on va regarder la fonction $g = s \circ f$.
Cependant, pour que g conserve les invariants de f, il faut que a soit orthogonal à $\mathrm{Ker}(f - \mathrm{Id}_E)$.

En algèbre linéaire, le complémentaire d'un espace vectoriel n'a aucun intérêt : ce n'est jamais un espace vectoriel. Il faut donc considérer un supplémentaire (voire le supplémentaire orthogonal dans le cas euclidien).

On note $n = \dim(E)$. Montrons par récurrence sur $k \in \{0,\dots,n\}$ la propriété H_k : « Si $f \in O(E)$ vérifie $\dim(\mathrm{Ker}(f-\mathrm{Id}_E)) = n-k$, alors f est composée de réflexions. »

- Soit $f \in O(E)$ tel que $\dim(\mathrm{Ker}(f-\mathrm{Id}_E)) = n$. Alors $\mathrm{Ker}(f-\mathrm{Id}_E) = E$ donc $f = \mathrm{Id}$. f s'écrit donc $s \circ s$ pour n'importe quelle réflexion s, et on a H_0.
- Soit $k \in \{0,\dots,n-1\}$ tel que H_l est vraie pour tous les l entre 0 et k. Soit $f \in O(E)$ tel que $\dim(\mathrm{Ker}(f-\mathrm{Id}_E)) = n-k-1$. Alors $\mathrm{Ker}(f-\mathrm{Id}_E) \neq E$ donc $[\mathrm{Ker}(f-\mathrm{Id}_E)]^\perp \neq \{0\}$, et on a $a \in [\mathrm{Ker}(f-\mathrm{Id}_E)]^\perp$ tel que $f(a) \neq a$. Notons $b = f(a)$. Alors $a \neq b$ par définition de a et a et b ont même norme car $b = f(a)$ et f est orthogonal. Ainsi, il existe une réflexion s de E telle que $s(a) = b$ et $s(b) = a$, c'est la réflexion par rapport à $(a-b)^\perp$ comme vu au 1. On a donc $(s \circ f)(a) = a$.
  Si $x \in \mathrm{Ker}(f-\mathrm{Id}_E)$, on a $\langle x|a\rangle = 0$ donc $\langle x|b\rangle = \langle f(x)|f(a)\rangle = 0$; par suite $\langle x|a-b\rangle = 0$ et donc $s(x) = x$ et $s\circ f(x) = x$. Ainsi, $\mathrm{Ker}(s\circ f - \mathrm{Id}_E)$ est un sous-espace vectoriel de E qui contient $\mathrm{Ker}(f-\mathrm{Id}_E)$. Cette inclusion est stricte puisque $\mathrm{Ker}(s\circ f - \mathrm{Id}_E)$ contient aussi a, qui n'est pas dans $\mathrm{Ker}(f-\mathrm{Id}_E)$. Ainsi $\dim(\mathrm{Ker}(s\circ f - \mathrm{Id}_E)) = n-l$ avec $l \leqslant k$.

Par hypothèse de récurrence, on peut donc écrire $s \circ f$ comme composée de réflexions : $s \circ f = r_1 \circ \ldots \circ r_t$, et alors $f = s \circ r_1 \circ \ldots \circ r_t$ peut s'écrire comme composée de réflexions, donc on a H_{k+1}, ce qui conclut la récurrence.

Exercice 1.5 : Anneau $\mathbb{Z}[\sqrt{2}]$

1. Soit $P = \mathbb{Z} \cup \{\sqrt{2}\}$. Montrer que le sous-anneau de $\mathbb{R}$ engendré par P est :

$$A = \{m + n\sqrt{2} \ ; (m,n) \in \mathbb{Z}^2\}.$$

Comme pour les groupes, il s'agit du plus petit sous-anneau de $\mathbb{R}$ contenant P. On note U le groupe des éléments inversibles de A .
2. On pose $N\big(m + n\sqrt{2}\big) = \big|m^2 - 2n^2\big|$. Pour a et b éléments de A, calculer $N(ab)$. Montrer que $z \in U$ si, et seulement si, $N(z) = 1$.
3. Soit $z \in U$ tel que $z = x + y\sqrt{2}$ avec x et $y \in \mathbb{N}$, $x \neq 0$. Montrer qu'il existe un unique $n \in \mathbb{N}$ tel que $(1+\sqrt{2})^n \leqslant z < (1+\sqrt{2})^{n+1}$, puis que $z(1+\sqrt{2})^{-n}$ s'écrit sous la forme $x' + y'\sqrt{2}$ avec x' et $y' \in \mathbb{N}$.
4. Montrer que $U = \big\{ \pm (1+\sqrt{2})^n \ ; n \in \mathbb{Z}\big\}$.

1. Comme toujours il faut montrer deux inclusions pour avoir l'égalité d'ensembles voulue. Tout d'abord, le sous-anneau de $\mathbb{R}$ engendré par P contient $\mathbb{Z}$ et $\sqrt{2}$. Il contient donc toutes les sommes, et leurs opposées, que l'on peut obtenir à partir de 1 et de $\sqrt{2}$, c'est-à-dire tous les réels du type $m + n\sqrt{2}$ avec $m \in \mathbb{Z}$ et $n \in \mathbb{Z}$.

Notons B le sous-anneau de $\mathbb{R}$ engendré par P. Alors $1 \in B$ et $\sqrt{2} \in B$. Pour $(m,n) \in \mathbb{Z}^2$, m est la puissance m-ième de 1 pour la loi $+$, donc est dans B. De même $n\sqrt{2}$ est la puissance n-ième de $\sqrt{2}$ pour la loi $+$, donc est dans B. Par suite $m + n\sqrt{2} \in B$ et $A \subset B$.

Pour montrer l'inclusion réciproque, il suffit de montrer que A est un sous-anneau de $\mathbb{R}$ contenant P. Par minimalité de B, on aura alors $B \subset A$.

Soient $a = m_1 + n_1\sqrt{2}$ et $b = m_2 + n_2\sqrt{2}$ avec $(m_1, n_1, m_2, n_2) \in \mathbb{Z}^4$.
D'une part :

$$a - b = (m_1 - m_2) + (n_1 - n_2)\sqrt{2} \in A$$

car $m_1 - n_1 \in \mathbb{Z}$ et $m_2 - n_2 \in \mathbb{Z}$.
D'autre part :

$$ab = (m_1 m_2 + 2n_1 n_2) + \sqrt{2}(n_1 m_2 + m_1 n_2) \in A$$

car $m_1 m_2 + 2n_1 n_2 \in \mathbb{Z}$ et $n_1 m_2 + m_1 n_2 \in \mathbb{Z}$.
Enfin, $1 = 1 + 0 \times \sqrt{2} \in A$, donc A est un sous-annneau de $\mathbb{R}$. Comme P est clairement inclus dans A, et comme B est le plus petit (au sens de l'inclusion) sous-anneau de $\mathbb{R}$ contenant P, on a $B \subset A$.
Ainsi, on a l'égalité cherchée.

Il faut vérifier que le neutre pour la multiplication est bien dans A, puisqu'on ne peut pas le déduire des propriétés de stabilité.

2. Cette question a pour objectif de caractériser les éléments de U.

Soit $a = m_1 + n_1\sqrt{2} \in A$ et $b = m_2 + n_2\sqrt{2} \in A$.
On a $ab = (m_1m_2 + 2n_1n_2) + \sqrt{2}(n_1m_2 + m_1n_2)$, ce qui entraîne :

$$\begin{aligned} N(ab) &= \left|(m_1m_2 + 2n_1n_2)^2 - 2(n_1m_2 + m_1n_2)^2\right| \\ &= \left|m_1^2m_2^2 + 4n_1^2n_2^2 - 2n_1^2m_2^2 - 2m_1^2n_2^2\right| \end{aligned}$$

Ce calcul n'a pas beaucoup d'intérêt si on s'arrête là. Soyons optimiste : calculons $N(a)N(b)$ en espérant découvrir quelque chose.

Par ailleurs :

$$\begin{aligned} N(a)N(b) &= \left|(m_1^2 - 2n_1^2)(m_2^2 - 2n_2^2)\right| \\ &= \left|m_1^2m_2^2 + 4n_1^2n_2^2 - 2n_1^2m_2^2 - 2m_1^2n_2^2\right| \\ &= N(ab). \end{aligned}$$

Le sens facile est celui où l'on suppose $z \in U$, puisqu'on peut alors utiliser son inverse ; l'autre implication nécessite de prouver l'existence de cet inverse, ce qui est *a priori* plus difficile.

Supposons $z \in U$. Il existe donc $z' \in U$ tel que $zz' = 1$. D'après ce qu'on vient d'obtenir, on en déduit que $N(z)N(z') = N(1) = 1$. Comme $N(z)$ et $N(z')$ appartiennent à $\mathbb{N}^*$, on conclut que $N(z) = 1$.

Passons à la réciproque : pour $z \in A$ tel que $N(z) = 1$, on cherche $z' \in A$ tel que $zz' = 1$.

Réciproquement, considérons $z = m + n\sqrt{2} \in A$ avec $N(z) = 1$.
Remarquons d'abord que : $(m + n\sqrt{2})(m - n\sqrt{2}) = m^2 - 2n^2$.
Comme $N(z) = \left|m^2 - 2n^2\right| = 1$, z est inversible : selon que $m^2 - 2n^2$ est égal à 1 ou -1, son inverse est $m - n\sqrt{2}$ ou $-m + n\sqrt{2}$.
z appartient donc bien à U.

On remarque l'analogie des formules, propriétés et démonstrations avec les calculs dans $\mathbb{C}$ utilisant le module.

3. Pour avoir l'existence et l'unicité de n, on se ramène à un encadrement de définition de partie entière.

Pour $n \in \mathbb{N}$, on a $(1+\sqrt{2})^n \leqslant z < (1+\sqrt{2})^{n+1}$ si et seulement si

$$n\ln(1+\sqrt{2}) \leqslant \ln(z) < (n+1)\ln(1+\sqrt{2})$$

par stricte croissante de ln, $\ln(z)$ étant bien défini puisque $z \geqslant x \geqslant 1$. Comme $\ln(1+\sqrt{2}) > 0$, ceci équivaut à

$$n \leqslant \frac{\ln(z)}{\ln(1+\sqrt{2})} < n+1$$

donc n existe et est unique par définition de la partie entière.

Pour la seconde partie de la question, on commence par montrer que $z(1+\sqrt{2})^{-n}$ est de la forme cherchée avec x' et y' dans $\mathbb{Z}$. Ceci vient de l'inversibilité de $(1+\sqrt{2})^n$. On manipule ensuite les inégalités pour avoir x' et $y' \geqslant 0$.

Comme $N((1+\sqrt{2})^n) = N(1+\sqrt{2})^n = 1$, $(1+\sqrt{2})^n$ est un élément inversible de A. On peut donc poser :

$$\frac{x+y\sqrt{2}}{(1+\sqrt{2})^n} = x'+y'\sqrt{2} \text{ avec } x' \in \mathbb{Z} \text{ et } y' \in \mathbb{Z}$$

et on a :

$$N(x'+y'\sqrt{2}) = 1 = \left|x'^2 - 2y'^2\right| = \left|x'+y'\sqrt{2}\right| \times \left|x'-y'\sqrt{2}\right|$$

On a nécessairement $x' \neq 0$ (sinon $2(y')^2 = 1$ mais 1 est impair).
Supposons $y' \neq 0$; x' et y' sont alors de même signe. En effet, supposons-les de signe distinct, par exemple $x' \geqslant 0$ et $y' \leqslant 0$ pour fixer les idées. Comme $x' \neq 0$, $x' \geqslant 1$. Alors on a :

$$1 \leqslant x'+y'\sqrt{2} < x'-y'\sqrt{2}$$

qui entraîne $\left|x'^2 - 2y'^2\right| > 1$... absurde !
Par suite x' et y' sont positifs, quitte à changer x' et y' en leurs opposés.

4. On doit montrer deux inclusions pour cette égalité d'ensembles. L'inclusion simple est celle qui consiste à *vérifier* que tout nombre élément de A de la forme $\pm(1+\sqrt{2})^n$ est inversible, ce qui est facile en utilisant N (qui est un morphisme de groupes par le 2).

Si $z = \pm(1+\sqrt{2})^n$ avec $n \in \mathbb{Z}$, on a $N(z) = \left[N(1+\sqrt{2})\right]^n = 1$; z appartient donc à U.

Pour la réciproque, on utilise la question précédente.

Réciproquement, soit $z = x+y\sqrt{2} \in U$, ce qui est équivalent à $\left|x^2 - 2y^2\right| = 1$. Les éléments $\pm x \pm y\sqrt{2}$ vérifient cette équation, et sont aussi inversibles. On peut donc suppposer $x > 0$ et $y \geqslant 0$.
Notons n, x' et y' les entiers donnés par la question précédente. On a alors

$$1 \leqslant \frac{x+y\sqrt{2}}{(1+\sqrt{2})^n} = x'+y'\sqrt{2} < 1+\sqrt{2}.$$

On a donc $y' = 0$ et $x' = 1$ et on obtient : $z = x + y\sqrt{2} = (1+\sqrt{2})^n$.
Les autres cas possibles sur z donnent $-(1+\sqrt{2})^n$, ou $x - y\sqrt{2} = \pm(1+\sqrt{2})^{-n}$.
z est donc toujours de la forme annoncée.

Exercice 1.6 : Groupe multiplicatif d'un corps fini

Soit G un groupe fini de neutre e. On note m le ppcm des ordres des éléments de G et $m = p_1^{\alpha_1} \cdots p_d^{\alpha_d}$ sa décomposition en facteurs premiers.
1. Montrer que pour i entre 1 et d, G admet un élément d'ordre $p_i^{\alpha_i}$ (on pourra commencer par chercher un élément dont l'ordre est divisible par $p_i^{\alpha_i}$).
2. Montrer que G admet un élément d'ordre m.
3. Soit $\mathbb{K}$ un corps fini, montrer que $(\mathbb{K}^*, \times)$ est cyclique. On admettra que tout polynôme à coefficients dans $\mathbb{K}$ a moins de racines que son degré, et on pourra considérer le polynôme $X^m - 1$.

1. En suivant l'indication, il faut commencer par trouver un élément dans G dont l'ordre est divisible par $p_i^{\alpha_i}$. Pour ce faire, on raisonne par l'absurde : si aucun élément dans G n'a d'ordre divisant $p_i^{\alpha_i}$ alors on va réussir à trouver un multiple commun plus petit que m.

Soit $i \in \{1, \ldots, d\}$. Supposons que l'ordre de tout élément de G ne soit pas divisible par $p_i^{\alpha_i}$. Si $x \in G$, l'ordre n de x divise m, donc a une décomposition en facteurs premiers de la forme $p_1^{\beta_1} \cdots p_d^{\beta_d}$, avec, pour k entre 1 et d, $\beta_k \leqslant \alpha_k$. Comme x n'est pas divisible par $p_i^{\alpha_i}$, $\beta_i \leqslant \alpha_i - 1$. Ainsi n divise l'entier

$$q = p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_i^{\alpha_i - 1} p_{i+1}^{\alpha_{i+1}} \cdots p_d^{\alpha_d}.$$

Ceci vaut pour tout x dans G, donc les ordres de tous les éléments de G divisent $q < m$... absurde, puisque m est le ppcm de ces ordres ! Ainsi on a $x \in G$ tel que $p_i^{\alpha_i}$ divise n, l'ordre de x.

Dans un deuxième temps, on va utiliser x pour construire un élément d'ordre $p_i^{\alpha_i}$. Comme $p_i^{\alpha_i}$ divise n, on a $k \in \mathbb{N}$ tel que $n = p_i^{\alpha_i} k$. On a alors

$$e = x^n = x^{p_i^{\alpha_i} k} = (x^k)^{p_i^{\alpha_i}},$$

ce qui encourage à regarder x^k.

Notons $k = n\, p_i^{-\alpha_i}$ et posons $y = x^k$. Alors $y^{p_i^{\alpha_i}} = x^{k p_i^{\alpha_i}} = x^n = e$. Pour $l < p_i^{\alpha_i} - 1$, on a $kl < n - 1$, donc $x^{k\,l} \neq e$ i.e. $y^l \neq e$. Ainsi $p_i^{\alpha_i}$ est l'ordre de y dans G.

Il ne faut pas oublier que pour prouver que y est d'ordre d, il faut montrer que $y^d = e$ et $y^l \neq e$ pour tout l entre 1 et $d - 1$.