Anneaux booléens

Partie 1: Etude de la différence symétrique.

Soient A et B deux sous-ensembles d'un ensemble E. On appelle *différence symétrique* de A et B le sous-ensemble:

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

1. Démontrer que la différence symétrique est commutative.
2. Est-elle associative?
3. Admet-elle un élément neutre?
4. Montrer que $A\Delta B = (A \cup B) \setminus (A \cap B)$.
5. Montrer que l'intersection est distributive sur la différence symétrique.

Partie 2: Etude d'un anneau de Boole

On considère un anneau A dont l'addition (loi de groupe) et la multiplication sont respectivement notées $+$ et $\times$. On note 0 l'élément neutre de l'addition. On dit que l'anneau A est un *anneau de Boole* si tout élément de A est idempotent pour la multiplication, c'est-à-dire si

$$\forall x \in A, \quad x \times x = x$$

1. Montrer que l'anneau $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est un anneau de Boole.
2. (a) Montrer que dans un anneau de Boole, tout élément est son propre symétrique pour l'addition.
   (b) En déduire qu'un anneau de Boole est nécessairement commutatif.
3. On suppose que A est intègre. Montrer alors que $Card(A) \leq 2$.

Partie 3: Exemple d'anneau de Boole en théorie des ensembles

1. Dans cette question, on considère E un ensemble non vide et on désigne par $\mathcal{P}(E)$ l'ensemble des parties de E. En utilisant la première partie, montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.
2. Dans la suite de ce problème, $(A, +, \times)$ désignera un anneau de Boole, et on désigne par E l'ensemble des éléments m de A, non nuls et tels que pour tout $x \in A$, $mx = 0$ ou $mx = m$.

   Montrer que si m et m' sont deux éléments distincts de E alors $mm' = 0$.
3. Pour tout élément $x \in E$, on définit la partie

   $$\Phi(x) = \{m \in E | mx = m\}.$$

   (a) Montrer que, pour tout x et y de A, $\Phi(xy) = \Phi(x) \cap \Phi(y)$.
   (b) Montrer que, pour tout $(x, y) \in A^2$, $\Phi(x + y + xy) = \Phi(x) \cup \Phi(y)$.
   (c) Montrer que pour tout $x \in A$, $\Phi(1 + x) = \overline{\Phi(x)}$ (le complémentaire est dans E).
   (d) Montrer que, pour tout $(x, y) \in A^2$, $\Phi(x)\Delta\Phi(y) = \Phi(x + y)$.
   (e) En déduire que Φ est un morphisme d'anneaux de $(A, +, \times)$ dans $(\mathcal{P}(E), \Delta; \cap)$.
4. On suppose à présent que $(A, +, \times)$ est un anneau de Boole de cardinal fini.
5. (a) Soit x_0 un élément non nul de A. Montrer que si $x_0 \notin E$, il existe $x_1 \in A$ tel que $x_0x_1 \neq 0$ et $x_0x_1 \neq x_0$. En déduire l'existence d'un élément $y \in A$ tel que $x_0y \in E$.
   (b) En déduire que le morphisme Φ est injectif.
   (c) Soit F un sous-ensemble de E, et soit S_F la somme des éléments de F (avec par convention $S_\emptyset = 0$). Déterminer la partie $\Phi(S_F)$. En déduire que le morphisme Φ est surjectif.
   (d) Prouver que le cardinal d'un anneau booléen fini est une puissance de 2.

Solution du problème: Anneaux booléens

Partie 1: Etude de la différence symétrique.

Soient A et B deux sous-ensembles d'un ensemble E. On appelle *différence symétrique* de A et B le sous-ensemble:

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

1. Cela résulte directement du fait que l'union et l'intersection sont commutatives:

$$\begin{aligned} A\Delta B &= (A \setminus B) \cup (B \setminus A) && \text{(par définition)} \\ &= (B \setminus A) \cup (A \setminus B) && \text{(car l'union est commutative)} \\ &= B\Delta A && \text{(par définition)} \end{aligned}$$

2. *Nous allons utiliser les fonctions caractéristiques.* Soient A, B et C trois sous-ensembles de E. De la définition de la différence symétrique, nous avons:

$$\begin{aligned} \varphi_{A\Delta B} &= \varphi_{A\setminus B} + \varphi_{B\setminus A} - \varphi_{A\setminus B}\varphi_{B\setminus A} \\ &= \varphi_A - \varphi_A\varphi_B + \varphi_B - \varphi_B\varphi_A - (\varphi_A - \varphi_A\varphi_B)(\varphi_B - \varphi_B\varphi_A) \\ &= \varphi_A + \varphi_B - 2\varphi_A\varphi_B \end{aligned} .$$

Ainsi, avons-nous:

$$\begin{aligned} \varphi_{A\Delta(B\Delta C)} &= \varphi_A + \varphi_{B\Delta C} - 2\varphi_A\varphi_{B\Delta C} \\ &= \varphi_A + (\varphi_B + \varphi_C - 2\varphi_B\varphi_C) - 1\varphi_A\,(\varphi_B + \varphi_C - 2\varphi_B\varphi_C) \\ &= \varphi_A + \varphi_B + \varphi_C - 2\varphi_B\varphi_C - 2\varphi_A\varphi_B - 2\varphi_A\varphi_C + 4\varphi_A\varphi_B\varphi_C \end{aligned} .$$

Par permutation circulaire des lettres, nous obtenons alors $\varphi_{A\Delta(B\Delta C)} = \varphi_{C\Delta(A\Delta B)}$. Cela implique l'égalité suivante: $A\Delta(B\Delta C) = C\Delta(A\Delta B)$. Par commutativité, nous obtenons $A\Delta(B\Delta C) = (A\Delta B)\Delta C$, d'où nous concluons à l'associativité de la différence symétrique.

3. Nous constatons que $\emptyset$ est le neutre de Δ puisque, $\forall A \in \mathcal{P}(E)$, $A\Delta\emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \setminus = A$.

4. Calculons la fonction caractéristique de $(A \cup B) \setminus (A \cap B)$.

$$\begin{aligned} \varphi_{(A\cup B)\setminus(A\cap B)} &= \varphi_{A\cup B}(1 - \varphi_{A\cap B}) \\ &= (\varphi_A + \varphi_B - \varphi_A\varphi_B)(1 - \varphi_A\varphi_B) \\ &= \varphi_A + \varphi_B - \varphi_A\varphi_B - \varphi_A\varphi_A\varphi_B - \varphi_B\varphi_A\varphi_B + \varphi_A\varphi_B\varphi_A\varphi_B \\ &= \varphi_A + \varphi_B - 2\varphi_A\varphi_B \end{aligned} .$$

Nous reconnaissons alors la fonction caractéristique de $\varphi_{A\Delta B}$ et nous concluons à l'égalité des deux ensembles.

5. *Il faut montrer l'égalité $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$. On peut (encore) recourrir aux fonctions caractéristiques ou utiliser la précédente question.* Nous avons $A \cap (B\Delta C) = A \cap ((B \cup C) \setminus (B \cap C)) = A \cap \big((B \cup C) \cap (\overline{B} \cup \overline{C})\big)$. D'autre part, nous avons $(A \cap B)\Delta(A \cap C) = (A \cap (B \cup C)) \cap \overline{(A \cap B \cap C)}$. De l'égalité $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cap \overline{C}$, nous déduisons: $(A \cap B)\Delta(A \cap C) = \big(A \cap (B \cup C) \cap \overline{A}\big) \cup \big(A \cap (B \cup C) \cap (\overline{B} \cup \overline{C})\big)$. Le premier membre est nul ($A \cap \overline{A} = \emptyset$), et nous obtenons l'égalité:

$$A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C).$$

Partie 2: Etude d'un anneau de Boole

1. Nous savons que $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est un anneau (c'est même un corps). Il nous reste alors à montrer que tout élément est idempotent. Or $\mathbb{Z}/2\mathbb{Z} = \{\overset{\circ}{0}; \overset{\circ}{1}\}$ et sont tous deux idempotents: il s'agit donc bien d'un anneau de Boole.

2.a.

> **Méthode** Dans ce genre de questions, il faut savoir faire preuve d'initiative en utilisant au maximum toutes les caractéristiques des lois ou des éléments. Ici ils sont idempotents... Un bon point de départ est de tester au brouillon à quoi mène l'égalité $(x+y)^2 = x+y$. Nous avons $(x+y)^2 = x^2 + xy + yx + y^2$ (attention, l'anneau n'est pas à priori commutatif!). Cela implique que $xy + yx = 0$, avec n'importe quel élément y. Ainsi, si l'on prend le neutre pour la multiplication, cela nous donne $x + x = 0$ et permet de conclure.
> On rédige directement en développant $(1+x)^2 = 1 + x + x + x^2 = 1 + x + x + x = 1 + x$, d'où $x + x = 0$.

Autre méthode: Nous avons $(x+x)^2 = x+x$. Or, $(x+x)^2 = x^2+x^2+x^2+x^2 = x+x+x+x$. De la précédente égalité, nous déduisons $x + x = 0$.

2.b. En développant $(x+y)^2 = x+y$, nous obtenons $x^2+y^2+xy+yx = x+y$. Or, $x^2 = x$ et $y^2 = y$, d'où finalement $xy+yx = 0$. On ajoute yx aux deux membres de l'égalité et en utilisant la précédente question, nous obtenons $xy = yx$.

3. Supposons A intègre. Tout élément $x \in A$ est idempotent, d'où $x^2 = x$ ce qui nous conduit à: $\forall x \in A$, $x(x-1) = 0$. Si A est intègre, cela implique alors que $x = 0$ ou $x = 1$. Ainsi, le cardinal de A est-il au plus 2.

Partie 3: Exemple d'anneau de Boole en théorie des ensembles

1. Rappelons que pour montrer que $(A, +, \times)$ est un anneau, il faut: $(A; +)$ soit un groupe abélien, que $\times$ soit une loi de composition interne *associative*, que A possède un élément neutre pour la multiplication (*on dit parfois anneau unitaire*), et que la loi $\times$ est distributive par rapport à l'addition.

Montrons déjà que $(\mathcal{P}(E), \Delta)$ est un groupe abélien. Nous savons que Δ est une loi associative, de neutre $\emptyset$: il reste à montrer que tout élément admet un symétrique. Or, nous remarquons que $\forall A \in \mathcal{P}(E)$, $A\Delta A = \emptyset$. Enfin, nous avons précédemment démontré que Δ est commutative, donc $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.

Comme de plus l'intersection est distributive sur la différence symétrique, nous concluons au fait que $(\mathcal{P}(E); \Delta; \cap)$ est un anneau de Boole.

2. Soient m et m' deux éléments distincts de E. De $m \in E$ et $m' \in A$, nous déduisons que $mm' \in \{0; m\}$. D'autre part, de $m' \in E$ et $m \in A$, nous déduisons que $m'm \in \{0; m'\}$. Or, l'anneau de Boole étant commutatif, $mm' = m'm$ et donc, puisque $m \neq m'$ nous en déduisons que $mm' \in \{0; m\} \cap \{0, m'\} = \{0\}$.

3.a.

> **Méthode** Pour montrer l'égalité de deux ensembles, on procède très souvent par la double inclusion.

Soient x et y dans A et $m \in \Phi(x) \cap \Phi(y)$. Nous avons donc $mx = my = m$ et donc par associativité de la loi multiplicative, nous obtenons: $m(xy) = (mx)y = my = m$, d'où $m \in \Phi(xy)$. Aussi avons-nous $\Phi(x) \cap \Phi(y) \subset \Phi(xy)$.

Réciproquement soit $m \in \Phi(xy)$. Alors $m(xy) = m$. En multipliant les deux membres par y, nous obtenons: $mxy^2 = my$. Or, dans un anneau de Boole, tout élément est idempotent donc $y^2 = y$ ce qui nous donne l'égalité $(mx)y = my$, d'où nous déduisons $m = my$ (car $m \in \Phi(xy)$). Ainsi $m \in \Phi(y)$. Nous déduisons que $m \in \Phi(x)$ en multipliant la précédente égalité par x (et en utilisant la commutativité de la loi multiplicative dans un anneau de Boole). Il s'ensuit que $\Phi(xy) = \Phi(x) \cap \Phi(y)$.

Nous avons donc bien démontré l'égalité $\Phi(xy) = \Phi(x) \cap \Phi(y)$ par double inclusion.

3.b. Soit $m \in \Phi(x) \cup \Phi(y)$. Supposons que $m \in \Phi(x)$. Alors $m(x+y+xy) = mx+my+mxy = m+my+my$. Or, dans un anneau de Boole, tout élément est son propre symétrique (pour la loi additive), i.e. $\forall \gamma \in A$, $\gamma+\gamma = 0$. Ainsi, $m(x+y+xy) = m$ et donc $m \in \Phi(x+y+xy)$.
On procède de même dans le cas où $m \in \Phi(y)$.

Réciproquement, supposons que $m \in \Phi(x+y+xy)$, soit $mx+my+mxy = m$. Puisque $m \in E$, nous savons que my e mx sont dans $\{0; m\}$.
Si $mx = my = 0$ alors la relation $mx+my+mxy = m$ implique que $m = 0$, ce qui est absurde par définition de E. Ainsi, au moins l'un des éléments $\{my; my\}$ est égal à m, c'est-à-dire que $m \in \Phi(x)$ ou $m \in \Phi(y)$, soit $m \in \Phi(x) \cup \Phi(y)$.

Ainsi nous avons obtenu, par double inclusion, l'égalité recherchée.

3.c. Soit $m \in \Phi(1+x)$. Nous avons alors $m(1+x) = m$, soit $m+mx = m$ et donc (en ajoutant m à chacun des deux membres) $mx = 0$. Ainsi, $m \notin \Phi(x)$ et donc $m \in \overline{\Phi(x)}$. Nous avons donc l'inclusion $\Phi(1+x) \subset \overline{\Phi(x)}$.

Réciproquement, soit $m \in \overline{\Phi(x)}$, c'est-à-dire que $mx \neq m$. Or, $m \in E$ donc $mx = 0$, ce qui implique que $m+mx = m$, soit encore $m \in \Phi(1+x)$. Nous avons alors l'inclusion $\Phi(1+x) \subset \overline{\Phi(x)}$.

En définitive, nous avons démontré l'égalité $\Phi(1+x) = \overline{\Phi(x)}$.

3.d. Par définition, $A\Delta B = (A \setminus B) \cup (B \setminus A)$, soit encore $A\Delta B = (A \cap \overline{B}) \cup (B \cap \overline{A})$. Aussi avons-nous: $\Phi(x)\Delta\Phi(y) = \left(\Phi(x) \cap \overline{\Phi(y)}\right) \cup \left(\Phi(y) \cap \overline{\Phi(x)}\right)$. En utilisant les précédents résultats, nous obtenons:

$$\begin{aligned}
\Phi(x)\Delta\Phi(y) &= (\Phi(x) \cap \Phi(1+y)) \cup (\Phi(y) \cap \Phi(1+x)) && \text{car } \overline{\Phi(x)} = \Phi(1+x)\\
&= \Phi(x(1+y)) \cup Phi(y(1+x)) && \text{car } \Phi(x) \cap \Phi(y) = \Phi(xy)\\
&= \Phi(x(1+y)+y(1+x)+xy(1+x)(1+y) && \text{car } \Phi(x) \cup \Phi(y) = \Phi(x+y+xy)\\
&= \Phi(x+xy+y+yx+xy(1+x+y+xy))\\
&= \Phi(x+y+(xy+xy)+xy+xy+xy+xy) && \text{car } x^2 = x \text{ et } y^2 = y\\
&= \Phi(x+y) && \text{car } xy+xy = 0
\end{aligned}$$

Nous obtenons bien l'égalité recherchée.

3.e. Nous avons $\Phi(1) = E$ (puisque $\forall m \in E$, $m \times 1 = m$. De plus, $\forall (x, y) \in A^2$, nous avons $\Phi(x+y) = \Phi(x)\Delta\Phi(y)$ et $\Phi(xy) = \Phi(x) \cap \Phi(y)$. Aussi Φ est-il un morphisme d'anneau de $(A, +, \times)$ dans $(\mathcal{P}(E), \Delta, \cap)$.

4.a. Soit $x_0 \in A$ non nul. Par définition de E, nous avons:

$$x_0 \in E \ \Leftrightarrow \ \forall x_1 \in A, \ x_0 x_1 \in \{0, x_0\}.$$

d'où l'on tire:

$$x_0 \notin E \ \Leftrightarrow \ \exists x_1 \in A, \ x_0 x_1 \notin \{0, x_0\}.$$

Si x_1 vérifie $x_0 x_1 \in E$ alors $y = x_1$. Sinon, $x_0 x_1 \notin E$, et il existe donc $x_2 \in A$ tel que $x_0 x_1 x_2 \neq 0$ et $x_0 x_1 x_2 \neq x_0 x_1$. De plus, $x_0 x_1 x_2 \neq x_0$ car dans le cas contraire, en multipliant par x_1 nous obtiendrons $x_0 x_1 x_2 = x_0 x_1$ ce qui serait contradictoire.

S'il n'existe aucun élément $y \in A$ tel que $x_0 y \in E$, nous pourrions alors construire une suite infinie d'éléments $(x_0, x_0 x_1, x_0 x_1 x_2, \cdots)$ d'éléments de A deux à deux disctincts, ce qui contredit la finitude de A.

Ainsi, il existe $y \in A$ tel que $x_0 y \in E$.

4.b. Déterminons le noyau du morphisme Φ. Soit $x \in Ker(\Phi)$, i.e. $\Phi(x) = \emptyset$, soit encore $\forall m \in E$, $mx = 0$.

Si $x \neq 0$, la question précédente implique l'existence d'un élément $y \in A$ tel que $xy \in E$, et donc $xyx = 0$, soit $xy = 0$ ce qui contredit la définition de E. Ainsi, $Ker(\Phi) = \{0\}$ et le morphisme Φ est injectif.

4.c.

> **Méthode** Nous allons montrer que Φ est surjective: pour cela, il faut montrer que toute partie $F \subset E$ admet un antécédent par Φ, et pour cela, nous devons visiblement utiliser S_F...

Soit $F = \{m_1, m_2, \cdots, m_n\}$. Si $m \in \Phi(S_F)$, alors $m(m_1 + m_2 + \cdots + m_n) = m$.

Si $m \notin F$ alors pour tout $i \in \{1, \cdots, n\}$, $m m_i = 0$ et donc $m S_F = 0$ et $m \notin \Phi(S(F))$, ce qui est absurde. Ainsi, $\Phi(S_F) \subset F$.

Réciproquement, si $m \in F$, alors il existe $j \in \{1, \cdots, n\}$ tel que $m = m_j$. Ainsi, $m S_F = m_j = m$ et donc $F \subset \Phi(S_F)$.

Ainsi, nous avons démontré que $\forall F \subset E$, $\Phi(S_F) = F$: le morphisme Φ est surjectif.

4.d. Nous savons donc que tout anneau booléen fini A est isomorphe à un anneau de la forme $(\mathcal{P}(E), \Delta, \cap)$. Or, le cardinal de $\mathcal{P}(E)$ est une puissance de 2, d'où le cardinal de tout anneau booléen est une puissance de 2.

Problème 1: Nombres quadratiques.

Dans ce problème, on considère d en entier autre que 0 ou 1 qui soit *libre de carré*, c'est-à-dire tel que pour tout p nombre premier divisant d, p^2 ne divise pas d. S'il en est ainsi, aucun carré autre que 1 ne divise d. On autorise l'abus d'écriture suivant: pour $d \in \mathbb{Z}$, on note $\sqrt{d}$ le réel valant $\sqrt{d}$ si $d > 0$ et le complexe $i\sqrt{-d}$ si $d < 0$.

Partie 1: Nombre entier de $\mathbb{Q}[\sqrt{d}]$

1. Montrer que $\sqrt{d} \notin \mathbb{Q}$ et $\sqrt{d} \notin i\mathbb{Q}$.

2. Si p est un nombre premier et n un entier non nul, on note $v_p(n)$ la puissance (éventuellement nulle) à laquelle figure p dans la décomposition de n en produit de facteurs premiers. On appelle $v_p(n)$ *l'exposant de p dans n*.
   Montrer, en utilisant la notion d'exposant de p dans n, que s'il existe $n \in \mathbb{N}^*$ et $r \geq 2$ tel que $\sqrt[r]{n} \in \mathbb{Q}$, alors $\sqrt[r]{n} \in \mathbb{Z}$.

3. On considère l'ensemble $\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} | (r,s) \in \mathbb{Q}^2\}$.
   Montrer que si $z \in \mathbb{Q}[\sqrt{d}]$ alors il existe un unique couple $(r;s) \in \mathbb{Q}^2$ tel que $z = r + s\sqrt{d}$.
   Montrer que $\mathbb{Q}[\sqrt{d}]$ est un sous-anneau de $\mathbb{R}$ ou de $\mathbb{C}$ (selon le signe de d).
   Soit $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.

4. On appelle l'application *conjuguée* de $\mathbb{Q}[\sqrt{d}]$ l'application: $\sigma : \begin{array}{ccc} \mathbb{Q}[\sqrt{d}] & \longrightarrow & \mathbb{Q}[\sqrt{d}] \\ r + s\sqrt{d} & \mapsto & r - s\sqrt{d} \end{array}$.
   Montrer que l'application σ est un automorphisme involutif d'anneau.

5. Pour $z \in \mathbb{Q}[\sqrt{d}]$, on appelle *norme*[1] *de z* le nombre $N(z) = z \times \sigma(z)$.

   (a) Montrer que $N(z) \in \mathbb{Q}$.

   (b) On définit alors l'application $N : \begin{array}{ccc} \mathbb{Q}[\sqrt{d}] & \to & \mathbb{Q} \\ z & \mapsto & N(z) = z \times \sigma z \end{array}$.
   Montrer que cette application est multiplicative, c'est-à-dire que $\forall (z,z') \in \mathbb{Q}[\sqrt{d}]^2$, $N(z \times z') = N(z) \times N(z')$.
   Montrer que N induit un morphisme de groupe de $(\mathbb{Q}[\sqrt{d}] \setminus \{0\}; \times)$ dans $(\mathbb{Q}^*; \times)$.

6. On définit l'application *trace*[2] par: $T : \begin{array}{ccc} \mathbb{Q}[\sqrt{d}] & \to & \mathbb{Q}[\sqrt{d}] \\ z & \mapsto & T(z) = z + \sigma(z) \end{array}$.
   Montrer que T est un morphisme de groupes additifs et préciser son noyau.

7. Montrer que tout élément $z \in \mathbb{Q}[\sqrt{d}]$ est racine d'une équation du second degré à coefficients dans $\mathbb{Q}$ et de coefficient de plus haut degré est égal à 1. En déduire alors que tout élément $z \in \mathbb{Q}[\sqrt{d}]$ est solution d'une équation du second degré à coefficients dans $\mathbb{Z}$ (sans précision sur le coefficient de plus haut degré).
   Exemple: Préciser les deux équations obtenues pour $z = \frac{1+\sqrt{3}}{2}$ et $z = \frac{1+i\sqrt{5}}{2}$.

8. Un élément $z \in \mathbb{Q}[\sqrt{d}]$ est dit *entier*[3] s'il est solution d'une équation du second degré à coefficient dans $\mathbb{Z}$ et dont le coefficient de plus haut degré est égal à 1. On note $E(\sqrt{d})$ l'ensemble des éléments entiers de $\mathbb{Q}[\sqrt{d}]$.
   Montrer que $\mathbb{Z}[\sqrt{d}] \subset E(\sqrt{d})$.
   Que pensez-vous de l'inclusion réciproque ? On pourra considérer le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ ou j.

9. Soit $P(X) = X^2 + \alpha X + \beta$ une fonction polynômiale à coefficients dans $\mathbb{Z}$. Montrer que si $z \in \mathbb{Q}[\sqrt{d}]$ vérifie $P(z) = 0$, alors $P(\sigma(z)) = 0$.
   En déduire que si $z \notin \mathbb{Q}$, z et $\sigma(z)$ sont des racines de P et que $T(z) = -\alpha$ et $N(z) = \beta$.

[1] la définition qui suit est uniquement valable dans le cadre arithmétique: elle ne doit pas être confondue avec la notion de norme sur un espace vectoriel réel ou complexe. On l'appelle ainsi car elle présente quelques similarités avec une norme (au sens classique des e.v.n.) mais n'en est pas une!

[2] Même remarque que précédemment, cette définition arithmétique ne correspond pas à la notion classique

[3] Même remarque que précédemment, cette notion ne coincide pas avec la définition classique

10. Réciproquement, si $z \in \mathbb{Q}[\sqrt{d}]$ vérifie $T(z) = -\alpha$ et $N(z) = \beta$ avec $(\alpha, \beta) \in \mathbb{Z}^2$, montrer que $z \in E(\sqrt{d})$.

11. Montrer qu'un élément de $\mathbb{Q}[\sqrt{d}]$ est entier si et seulement si sa norme et sa trace sont dans $\mathbb{Z}$.

12. Ici, d est fixé. Montrer que $z = r + s\sqrt{d}$ est entier si et seulement si on a les deux conditions suivantes:

    - $2r \in \mathbb{Z}$
    - $r^2 - ds^2 \in \mathbb{Z}$.

Partie 2: Unités de $\mathbb{Q}[\sqrt{d}]$

Nous avons donc démontré dans la dernière question de la partie précédente qu'un élément $z = r + s\sqrt{d}$ est entier si et seulement si on a $2r \in \mathbb{Z}$ et $r^2 - ds^2 \in \mathbb{Z}$.

1. Soit z un entier de $\mathbb{Q}[\sqrt{d}]$. Montrer alors que $2s \in \mathbb{Z}$. On pose alors $u = 2r$ et $v = 2s$.

2. (a) Montrer que l'on doit avoir $u^2 - dv^2 \in 4\mathbb{Z}$.
   (b) Montrer que si v est pair, alors u l'est et que si v impair on doit avoir $d \equiv 1 \mod 4$ et u impair.
   (c) Montrer alors que si d n'est pas congru à 1 modulo 4, $E(\sqrt{d}) \subset \mathbb{Z}[\sqrt{d}]$, et que si $d \equiv 1 \mod 4$ alors $E(\sqrt{d}) \subset \{\frac{u+v\sqrt{d}}{2};\ (u,v) \in \mathbb{Z}^2,\ u \equiv v \mod 2\}$.
   (d) Montrer que dans chacun des cas précédents, on obtient en fait une égalité.
   (e) En déduire au théorème suivant:

   Théorème 1

   Soit $\mathbb{Q}[\sqrt{d}]$ un corps quadratique. Si $d \equiv 1 \mod 4$, on pose $\omega = \frac{1+\sqrt{d}}{2}$, et dans le cas contraire on pose $\omega = \sqrt{d}$. Alors l'ensemble $E(\sqrt{d})$ des entiers de $\mathbb{Q}[\sqrt{d}]$ est l'ensemble $\mathbb{Z}[\omega]$.

3. On reprends les notations du théorème précédent. Montrer que si $z \in \mathbb{Z}[\omega]$ alors $\exists!(a,b) \in \mathbb{Z}^2$ tel que $z = a + b\omega$.

4. Montrer que $\mathbb{Z}[\omega]$ est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$.

5. Montrer que les unités de cet anneau sont les éléments de norme égale à 1 ou -1.

6. Déterminer les unités dans le cas $d < 0$ (on pourra distinguer le cas d non congru à 1 modulo 4, du cas $d \equiv 1 \mod 4$, $|d| \geq 7$ et enfin $d = -3$).

7. Montrer que l'anneau $\mathbb{Z}[\sqrt{2}]$ admet une infinité d'unités.