LES NOMBRES COMPLEXES

OLIVIER CASTÉRA

Résumé. Le corps des nombres complexes $\mathbb{C}$ forme une extension quadratique du corps des nombres réels $\mathbb{R}$. Les nombres complexes de la forme $(x, 0)$ forment un sous-corps de $\mathbb{C}$ qui est isomorphe au corps $\mathbb{R}$, par l'application qui à $(x, 0)$ fait correspondre x.

Table des matières

1. Groupe

Un groupe est une structure algébrique relativement simple puisqu'elle ne contient qu'une seule opération. Elle est utilisée dans beaucoup d'autres structures algébrique.

Définition 1.1. Un ensemble non vide G muni de l'opération $\square$, est un groupe, noté $(G, \square)$, ssi

(1) l'opération binaire $\square$ est une loi de composition interne : à chaque paire d'éléments de G, elle associe un élément de G

$$\forall (a, b) \in G^2, \quad a \square b \in G$$

(2) l'opération $\square$ est associative

$$\forall (a, b, c) \in G^3, \quad a \square (b \square c) = (a \square b) \square c$$

Date: 4 mai 2015.

(3) Il existe un élément neutre (ou identité) e dans G, pour l'opération $\square$

$$\exists e \in G \ / \ \forall a \in G, \quad e \square a = a \square e = a$$

(4) Tout élément a de G possède un symétrique b dans G

$$\forall a \in G, \ \exists b \in G \ / \quad a \square b = b \square a = e$$

Pour un groupe multiplicatif, la loi de composition est notée par une juxtaposition des éléments. L'élément neutre est l'unité. Le symétrique de a est appelé inverse de a, et noté a^{-1}.
Pour un groupe additif, la loi de composition est notée par $+$. L'élément neutre est l'élément nul ou zéro. Le symétrique de a est appelé l'opposé de a, et noté $-a$.

Théorème 1.1. *Quel que soit le groupe $(G, \square)$, l'élément neutre est unique.*

Démonstration. Supposons que e et e' soient les éléments neutres du groupe $(G, \square)$

$$\forall x \in G, \ x \square e = e \square x = x$$
$$(x = e') \Rightarrow (e' \square e = e \square e' = e')$$

$$\forall x \in G, \ x \square e' = e' \square x = x$$
$$(x = e) \Rightarrow (e \square e' = e' \square e = e)$$

$$(e' \square e = e' \ \text{ et } \ e' \square e = e) \Rightarrow (e' = e)$$

□

Définition 1.2. Un groupe $(G, \square)$ est dit abélien ssi l'opération $\square$ est commutative

$$\forall (a, b) \in G^2, \quad a \square b = b \square a$$

Exemples. Les ensembles des entiers naturels $\mathbb{Z}$, des rationnels $\mathbb{Q}$, et des réels $\mathbb{R}$, sont des groupes abéliens pour l'addition $+$. Les ensembles des rationnels privés de zéro (zéro n'a pas d'inverse), $\mathbb{Q}^*$, et des réels privés de zéro, $\mathbb{R}^*$, sont des groupes abéliens pour la multiplication $\times$.

1.1. **Produit direct de groupes.**

Définition 1.3. Soient $(G, \star)$ et $(H, \star)$ deux groupes munis de la même loi de composition interne $\star$. Considérons le produit cartésien $G \times H$ des ensembles G et H, c'est à dire l'ensemble des paires ordonnées $\{g \in G, h \in H, (g, h)\}$. On munit le produit cartésien $G \times H$ de l'opération $\circledast$

$$\forall (g_1, g_2) \in G^2, \ \forall (h_1, h_2) \in H^2,$$
$$(g_1, h_1) \circledast (g_2, h_2) = (g_1 \star g_2, h_1 \star h_2)$$

$(G \times H, \circledast)$ est appelé produit direct de G et H.

Théorème 1.2. *Le produit direct $(G \times H, \circledast)$ forme un groupe.*

Démonstration.

(1) l'opération $\circledast$ est une loi de composition interne

$$\begin{aligned}
&(G, \star)\, est\, un\, groupe \ : \ \forall (g_1, g_2) \in G^2,\ (g_1 \star g_2) \in G \\
&(H, \star)\, est\, un\, groupe \ : \ \forall (h_1, h_2) \in H^2,\ (h_1 \star h_2) \in H \\
&\forall (g_1, h_1) \in (G \times H),\ \forall (g_2, h_2) \in (G \times H), \\
&\qquad (g_1 \star g_2, h_1 \star h_2) \in (G \times H) \\
&\qquad (g_1, h_1) \circledast (g_2, h_2) \in (G \times H)
\end{aligned}$$

(2) l'opération $\circledast$ est associative

$$\begin{aligned}
&\forall (g_1, h_1), (g_2, h_2), (g_3, h_3) \in (G \times H)^3, \\
(g_1, h_1) \circledast [(g_2, h_2) \circledast (g_3, h_3)] &= (g_1, h_1) \circledast [(g_2 \star g_3, h_2 \star h_3) \\
&= [g_1 \star (g_2 \star g_3), h_1 \star (h_2 \star h_3)]
\end{aligned}$$

et,

$$\begin{aligned}
[(g_1, h_1) \circledast (g_2, h_2)] \circledast (g_3, h_3) &= (g_1 \star g_2, h_1 \star h_2)] \circledast (g_3, h_3) \\
&= [(g_1 \star g_2) \star g_3, (h_1 \star h_2) \star h_3] \\
&= [g_1 \star (g_2 \star g_3), h_1 \star (h_2 \star h_3)]
\end{aligned}$$

où l'on a utilisé l'associativité de la loi $\star$ dans G et dans H. Par conséquent,

$$(g_1, h_1) \circledast [(g_2, h_2) \circledast (g_3, h_3)] = [(g_1, h_1) \circledast (g_2, h_2)] \circledast (g_3, h_3)$$

(3) l'opération $\circledast$ admet un élément neutre dans $G \times H$.
Soit e l'élément neutre du groupe G, et soit e' l'élément neutre du groupe H

$$\begin{aligned}
\forall (g, h) \in (G \times H),\ (e, e') \circledast (g, h) &= (e \star g, e' \star h) \\
&= (g, h)
\end{aligned}$$

$$\begin{aligned}
(g, h) \circledast (e, e') &= (g \star e, h \star e') \\
&= (g, h)
\end{aligned}$$

□

Théorème 1.3. *Si $(G, \star)$ et $(H, \star)$ sont des groupes abéliens, alors le produit direct $(G \times H, \circledast)$ forme un groupe abélien.*

Démonstration.

$$\begin{aligned}(G,\star)\,\text{est un groupe abélien} \;:\; & g_1\star g_2 = g_2\star g_1\\ (H,\star)\,\text{est un groupe abélien} \;:\; & h_1\star h_2 = h_2\star h_1\\ \forall (g_1,h_1),(g_2,h_2)\in (G\times H)^2, (g_1,h_1)\circledast(g_2,h_2) &= (g_1\star g_2, h_1\star h_2)\\ &= (g_2\star g_1, h_2\star h_1)\\ &= (g_2,h_2)\circledast(g_1,h_1)\end{aligned}$$

□

1.2. **Morphisme de groupes.**

Définition 1.4. Soient deux groupes $(G,*)$ et $(G',\star)$. L'application f de $(G,*)$ dans $(G',\star)$ est un morphisme de groupes ssi

$$f : G \to G'$$
$$\forall (x,y)\in G^2,\ f(x*y) = f(x)\star f(y)$$

f est un isomorphisme de groupes ssi f est un morphisme bijectif. Dans ce cas, f^{-1} est aussi un morphisme de groupes.

2. Anneau

Définition 2.1. Un ensemble A muni de deux opérations, notées $\oplus$ et $\odot$, est un anneau, noté $(A,\oplus,\odot)$, ssi

(1) $(A,\oplus)$ est un groupe abélien

(2) l'opération $\odot$ est une loi de composition interne

$$\forall (a,b)\in A^2,\ a\odot b\in A$$

(3) l'opération $\odot$ est associative

$$\forall (a,b,c)\in A^3,\ a\odot(b\odot c) = (a\odot b)\odot c$$

(4) l'opération $\odot$ admet un élément neutre e' dans A

$$\exists e'\in A \;/\; \forall a\in A,\ e'\odot a = a\odot e' = a$$

(5) l'opération $\odot$ est distributive à gauche et à droite par rapport à l'opération $\oplus$

$$\forall x,y,z\in A^3,\ a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c)$$
$$\forall x,y,z\in A^3,\ (b\oplus c)\odot a = (b\odot a)\oplus(c\odot a)$$

Définition 2.2. Un anneau $(A,\oplus,\odot)$ est dit commutatif ssi l'opération $\odot$ est commutative

$$\forall (a,b)\in A^2,\ a\odot b = b\odot a$$

Règles de calcul. Quel que soit l'anneau $(A, \oplus, \odot)$

Soit e l'élément neutre de la loi $\oplus$: $\forall x \in A,\ e \odot x = x \odot e = e$

Soit $\ominus y$ *le symétrique de y pour la loi* $\oplus$:

$$\forall (x, y) \in A^2,\ x \odot (\ominus y) = \ominus (x \odot y)$$

$$\forall (x, y, z) \in A^3,\ x \odot (y \ominus z) = (x \odot y) \ominus (x \odot z)$$

Si $(A, \oplus, \odot)$ *est un anneau commutatif, binôme de Newton* :

$$\forall n \in \mathbb{N},\ \forall (x, y) \in A^2,\ (x \oplus y)^n = \sum_{k=0}^{n} C_n^k x^k \odot y^{n \ominus k}$$

2.1. **Anneau intègre.**

Définition 2.3. Un élément non nul a d'un anneau $(A, \oplus, \odot)$ est un diviseur de zéro à gauche, ssi

$$\exists b \neq e \in A \ / \ a \odot b = e$$

Définition 2.4. Un élément non nul a d'un anneau $(A, \oplus, \odot)$ est un diviseur de zéro à droite, ssi

$$\exists b \neq e \in A \ / \ b \odot a = e$$

Définition 2.5. Un anneau $(A, \oplus, \odot)$ est intègre s'il est différent de l'élément nul $\{e\}$, commutatif, et sans diviseur de zéro.

Théorème 2.1. *Pour tout anneau* $(A, \oplus, \odot)$ *intègre*

$$\forall (a, b) \in A^2,\ (a \odot b = e) \Rightarrow (a = e \ \textit{ou}\ b = e)$$

2.2. **Sous-anneau.**

Définition 2.6. Toute partie A' de l'ensemble A est un sous-anneau de l'anneau $(A, \oplus, \odot)$ ssi

(1) $(A', \oplus, \odot)$ est un anneau

(2) A' est stable pour la loi $\oplus$

$$\forall (a, b) \in A'^2,\ a \oplus b \in A'$$

(3) A' est stable pour la loi $\odot$

$$\forall (a, b) \in A'^2,\ a \odot b \in A'$$

2.3. **Morphisme d'anneaux.**

Définition 2.7. Soient deux anneaux $(A_1, \oplus, \odot)$ et $(A_2, \boxplus, \boxdot)$, et soient e_1 l'élément neutre de $\odot$ dans A_1, et e_2 l'élément neutre de $\boxdot$ dans A_2. L'application f de $(A_1, \oplus, \odot)$ dans $(A_2, \boxplus, \boxdot)$ est un morphisme d'anneaux ssi

(1) $\forall (x, y) \in A_1^2,\ f(x \oplus y) = f(x) \boxplus f(y)$

(2) $\forall (x, y) \in A_1^2,\ f(x \odot y) = f(x) \boxdot f(y)$

(3) $f(e_1) = e_2$

f est un isomorphisme d'anneaux ssi f est un morphisme bijectif. Dans ce cas, f^{-1} est aussi un morphisme d'anneaux.

3. Corps

Définition 3.1. Un ensemble K muni de deux opérations, notées $\oplus$ et $\odot$, est un corps, noté $(K, \oplus, \odot)$, ssi

(1) $(K, \oplus, \odot)$ est un anneau

(2) tout élément non nul a de K possède un inverse, noté a^{-1}, dans K pour l'opération $\odot$

$$\forall a \neq e \in K,\ \exists a^{-1} \in K \ / \ a \odot a^{-1} = a^{-1} \odot a = e'$$

Définition 3.2. Un corps $(K, \oplus, \odot)$ est dit commutatif ssi l'opération $\odot$ est commutative

$$\forall (a, b) \in K^2,\ a \odot b = b \odot a$$

Théorème 3.1. *Si $(K, \oplus, \odot)$ est un corps alors il n'a pas de diviseur de zéro.*

Démonstration. D'après la définition 3.1, si $(K, \oplus, \odot)$ est un corps

$$\forall a \neq e \in K,\ \exists a^{-1} \in K \ / \ a \odot a^{-1} = a^{-1} \odot a = e'$$

Pour démontrer que

$$(a \odot b = e) \Rightarrow (a = e \text{ ou } b = e)$$

nous allons montrer que si $a \odot b = e$ alors il est impossible d'avoir $a \neq e$ et $b \neq e$

$$\begin{aligned} \forall (a, b) \in K^2,\ & a \odot b = e \\ \forall a \neq e \in K,\ & a^{-1} \odot a \odot b = a^{-1} \odot e \\ & e' \odot b = e \\ & b = e \end{aligned}$$

et par symétrie des rôles de a et b, si $b \neq e$ alors $a = e$. □

3.1. Sous-corps.

Définition 3.3. Toute partie K' de l'ensemble K est un sous-corps du corps $(K, \oplus, \odot)$ ssi

(1) $(K', \oplus, \odot)$ est un corps

(2) K' est stable pour la loi $\oplus$

$$\forall (a, b) \in K'^2,\ a \oplus b \in K'$$

(3) K' est stable pour la loi $\odot$

$$\forall (a, b) \in K'^2,\ a \odot b \in K'$$

4. Racines Carrées

Soit $(K, \oplus, \odot)$ un anneau commutatif. Nous dirons qu'un élément α de K est un carré dans K ssi

$$\exists x \in K \ / \ x^2 = \alpha$$

x est appelée racine carrée de α dans $(K, \oplus, \odot)$. Si x est une racine carrée de α dans K alors il en est de même de $\ominus x$, car $(\ominus x)^2 = \alpha$. Si l'anneau $(K, \oplus, \odot)$ est intègre, α ne peut admettre plus de deux racines carrées dans K, car la relation $x^2 = y^2$, qui s'écrit dans tous les cas sous la forme $(x \ominus y)(x \oplus y) = e$, implique soit $x = y$, soit $y = \ominus x$.

Exemples. Si $(K, \oplus, \odot)$ est le corps des nombres réels $(\mathbb{R}, +, \times)$, α est un carré dans K ssi $\alpha \geqslant 0$, par exemple pour $\alpha = 2$. Si $(K, \oplus, \odot)$ est le corps des nombres rationnels $(\mathbb{Q}, +, \times)$, 2 n'est pas un carré.

On est ainsi conduit à examiner le problème suivant :
Soit $(K, \oplus, \odot)$ un anneau commutatif et α un élément de K qui n'est pas un carré dans K. Est-il possible de construire un anneau commutatif $(L, \boxplus, \boxdot)$ possédant les propriétés suivantes :
K est un sous-anneau de L, et α est un carré dans L ?

Soit α un élément d'un anneau commutatif $(K, \oplus, \odot)$, qui n'est pas un carré dans K. Supposons le problème résolu et désignons par $(L, \boxplus, \boxdot)$ un anneau commutatif dont K soit un sous-anneau

$$(K, \oplus, \odot) \subseteq (L, \oplus, \odot)$$

et par ω une racine carrée de α dans L

$$\omega^2 = \alpha$$

Désignons par L' l'ensemble des éléments z de l'anneau commutatif L possédant la propriété

$$\forall z \in L', \ \exists (x, y) \in K^2 \ / \ z = x \oplus (\omega \odot y)$$

Notation. Nous posons que la loi de composition $\odot$ est prioritaire sur la loi de composition $\oplus$, et nous omettrons souvent le symbole $\odot$ pour faciliter la lecture. Par conséquent, nous écrirons

$$z = x \oplus \omega y$$

Théorème 4.1. *$(L', \oplus, \odot)$ est un sous-anneau de $(L, \boxplus, \boxdot)$ contenant $(K, \oplus, \odot)$ et ω.*

Démonstration. En utilisant les propiétés des lois de composition internes d'un anneau, données en définition 2.1, nous avons

$$\forall (x' \oplus \omega y') \in L' \text{ et } \forall (x'' \oplus \omega y'') \in L',$$

$$\begin{aligned}(x' \oplus \omega y') \oplus (x'' \oplus \omega y'') &= x' \oplus \omega y' \oplus x'' \oplus \omega y'' \\ &= x' \oplus x'' \oplus \omega y' \oplus \omega y'' \\ &= (x' \oplus x'') \oplus \omega(y' \oplus y'') \in L' \end{aligned} \tag{1}$$

$$\begin{aligned}(x' \oplus \omega y') \odot (x'' \oplus \omega y'') &= x'x'' \oplus x'\omega y'' \oplus \omega y'x'' \oplus \omega y'\omega y'' \\ &= x'x'' \oplus \alpha y'y'' \oplus x'\omega y'' \oplus \omega y'x'' \\ &= (x'x'' \oplus \alpha y'y'') \oplus \omega(x'y'' \oplus y'x'') \in L' \end{aligned} \tag{2}$$

D'après la définition 2.6, $(L', \oplus, \odot)$ est un sous-anneau de $(L, \boxplus, \boxdot)$. De plus, l'anneau L' contient l'anneau K (poser $y = e$), et il contient aussi ω (poser $x = e$ et $y = e'$). □

Ce résultat montre que si le problème admet une solution, alors on peut construire l'anneau commutatif $(L, \boxplus, \boxdot)$ de telle sorte que chacun de ses éléments s'écrive sous la forme $x \oplus \omega y$ avec $(x, y) \in K^2$.
Autrement dit, si nous introduisons l'application f, telle que

$$\begin{aligned} f : K \times K &\to L \\ f(x, y) &= x \oplus \omega y \end{aligned}$$

alors f est *surjective*

$$\forall u \in L,\ \exists (x, y) \in (K \times K) \ / \ f(x, y) = u$$

Remarque. Si $(K, \oplus, \odot)$ est un corps et si α n'est pas un carré dans $(K, \oplus, \odot)$, l'application f est en outre *injective*

$$\forall (x', y') \in K^2, \forall (x'', y'') \in K^2,\ f(x', y') = f(x'', y'') \Rightarrow (x' = x'', y' = y'')$$

Démonstration. En posant $x = x' \ominus x''$ et $y = y' \ominus y''$, nous avons

$$\begin{aligned} f(x', y') &= f(x'', y'') \\ x' \oplus \omega y' &= x'' \oplus \omega y'' \\ (x' \ominus x'') \oplus \omega(y' \ominus y'') &= e \\ x \oplus \omega y &= e \end{aligned}$$

Raisonnons par l'absurde en supposant $y \neq e$.
y est inversible dans K, puisque par hypothèse K est un corps, et y est aussi inversible dans L puisque $(K, \oplus, \odot) \subseteq (L, \boxplus, \boxdot)$.
Par conséquent

$$\omega = \ominus x y^{-1} \in K$$

contrairement à l'hypothèse que α n'est pas un carré dans K.
Donc $y = e$. Par conséquent $x = e$, $x' = x''$, $y' = y''$ et f est *injective.* □

En introduisant l'application f, les égalités (1) et (2) s'écrivent

$$f(x',y') \oplus f(x'',y'') = f(x' \oplus x'', y' \oplus y'')$$
$$f(x',y') \odot f(x'',y'') = f(x'x'' \oplus \alpha y'y'', x'y'' \oplus y'x'')$$

Ces égalités, obtenues en supposant le problème résolu, vont maintenant nous servir de point de départ pour construire une solution au problème posé.

5. L'anneau L

Soit α un élément d'un anneau commutatif $(K, \oplus, \odot)$, qui n'est pas un carré dans K. Nous allons construire un nouvel anneau $(L, \boxplus, \boxdot)$ dans lequel α est un carré. Soit l'ensemble L, produit cartésien de $K \times K$, tel qu'un élément (x, y) de L soit une paire ordonnée de deux éléments x et y de K.

Définition 5.1. Les deux opérations $\boxplus$ et $\boxdot$ dans $(L, \boxplus, \boxdot)$ sont définies comme suit

$$(x',y') \boxplus (x'',y'') = (x' \oplus x'', y' \oplus y'')$$
$$(x',y') \boxdot (x'',y'') = (x'x'' \oplus \alpha y'y'', x'y'' \oplus y'x'')$$

lesquelles font intervenir à la fois l'élément α et les lois de composition dans l'anneau $(K, \oplus, \odot)$.

Théorème 5.1. *L'ensemble L muni des lois de composition internes $\boxplus$ et $\boxdot$ est un anneau.*

Démonstration. Suivons les cinq points de la définition 2.1.

(1) Montrons que $(L, \boxplus)$ est un groupe abélien.
L'ensemble K muni de la loi de composition $\oplus$ est un groupe abélien. D'après le théorème 1.3, le produit direct des groupes abéliens $K \times K$ est un groupe abélien, donc $(L, \boxplus)$ est un groupe abélien.

(2) Montrons que $\boxdot$ est une loi de composition interne.
$\forall x', y', x'', y''$, quatre éléments de l'anneau K.
$x'x'' \oplus \alpha y'y'' \in K$ et $x'y'' \oplus \alpha y'x'' \in K$
Si l'on pose $a = (x', y')$ et $b = (x'', y'')$, on a :

$$\forall (a,b) \in L^2,\ a \boxdot b \in L$$

(3) Montrons que la loi $\boxdot$ est associative.
En utilisant la définition 5.1

$$(x,y) \boxdot [(x',y') \boxdot (x'',y'')] = (x,y) \boxdot (x'x'' \oplus \alpha y'y'', x'y'' \oplus y'x'')$$
$$= (x(x'x'' \oplus \alpha y'y'') \oplus \alpha y(x'y'' \oplus y'x''), x(x'y'' \oplus y'x'') \oplus y(x'x'' \oplus \alpha y'y''))$$
$$= (xx'x'' \oplus x\alpha y'y'' \oplus \alpha yx'y' \oplus \alpha yy'x'', xx'y'' \oplus xy'x'' \oplus yx'x'' \oplus y\alpha y'y'')$$

et d'autre part

$$\begin{aligned}
&[(x,y)\boxdot(x',y')]\boxdot(x'',y'') = (xx'\oplus\alpha yy', xy'\oplus yx')\boxdot(x'',y'')\\
&= [(xx'\oplus\alpha yy')x''\oplus\alpha(xy'\oplus yx')y'', (xx'\oplus\alpha yy')y''\oplus(xy'\oplus yx')x'']\\
&= (xx'x''\oplus\alpha yy'x''\oplus\alpha xy'y''\oplus\alpha yx'y'', xx'y''\oplus\alpha yy'y''\oplus xy'x''\oplus x'yx'')
\end{aligned}$$

L'associativité s'obtient en comparant les résultats.

(4) Montrons que la loi $\boxdot$ admet (e',e) comme élément neutre

$$\begin{aligned}
(e',e)\boxdot(x,y) &= (e'x\oplus\alpha ey, e'y\oplus ex)\\
&= (x\oplus\alpha e, y\oplus e)\\
&= (x,y)
\end{aligned}$$

(5) Montrons que la loi $\boxdot$ est distributive à gauche par rapport à la loi $\boxplus$

$$\begin{aligned}
&(x,y)\boxdot[(x',y')\boxplus(x'',y'')] = (x,y)\boxdot(x'\oplus x'', y'\oplus y'')\\
&= (x(x'\oplus x'')\oplus\alpha y(y'\oplus y''), x(y'\oplus y'')\oplus y(x'\oplus x''))\\
&= (xx'\oplus xx''\oplus\alpha yy'\oplus\alpha yy'', xy'\oplus xy''\oplus yx'\oplus yx'')\\
&= ((xx'\oplus\alpha yy')\oplus(xx''\oplus\alpha yy''), (xy'\oplus yx')\oplus(xy''\oplus yx''))\\
&= (xx'\oplus\alpha yy', xy'\oplus yx')\boxplus(xx''\oplus\alpha yy'', xy''\oplus yx'')\\
&= [(x,y)\boxdot(x',y')]\boxplus[(x,y)\boxdot(x'',y'')]
\end{aligned}$$

De même pour la distributivité à droite.

□

Théorème 5.2. $(L,\boxplus,\boxdot)$ *est un anneau commutatif.*

Démonstration. Montrons que la loi $\boxdot$ est commutative

$$\begin{aligned}
(x,y)\boxdot(x',y') &= (xx'\oplus\alpha yy', xy'\oplus yx')\\
&= (x'x\oplus\alpha y'y, x'y\oplus y'x)\\
&= (x',y')\boxdot(x,y)
\end{aligned}$$

D'après la définition 2.2, l'ensemble L muni des lois de composition $\boxplus$ et $\boxdot$ est donc un anneau commutatif. □

Théorème 5.3. *L'anneau* $(L,\boxplus,\boxdot)$ *contient un sous-anneau isomorphe à l'anneau* $(K,\oplus,\odot)$.

Démonstration. Considérons l'application

$$\begin{aligned}
f : K &\to K\times K\\
f(x) &= (x,e)
\end{aligned}$$

A tout élément (x,e) de l'ensemble $K\times K$ correspond un élément unique x de l'ensemble K par f. Par conséquent f est bijective

$$\forall(x,e)\in(K\times K),\ \exists!\ x\in K\ /\ f(x) = (x,e)$$

De plus, nous avons les relations suivantes

$$\begin{aligned} f(x') \boxplus f(x'') &= (x', e) \boxplus (x'', e) \\ &= (x' \oplus x'', e \oplus e) \\ &= (x' \oplus x'', e) \\ &= f(x' \oplus x'') \end{aligned}$$

$$\begin{aligned} f(x') \boxdot f(x'') &= (x', e) \boxdot (x'', e) \\ &= (x'x'' \oplus \alpha ee, x'e \oplus x''e) \\ &= (x'x'', e) \\ &= f(x'x'') \end{aligned}$$

$$f(e') = (e', e)$$

D'après la définition 2.7, f est un isomorphisme de l'anneau $(K, \oplus, \odot)$ sur un sous-anneau de l'anneau $(L, \boxplus, \boxdot)$.

Notation. Comme f transforme les lois de compositions de l'anneau $(K, \oplus, \odot)$ en celles du sous-anneau $f(K)$ de l'anneau $(L, \boxplus, \boxdot)$, il n'y a aucun inconvénient à identifier chaque élément x de l'anneau $(K, \oplus, \odot)$ à l'élément $f(x)$ de l'anneau $(L, \boxplus, \boxdot)$. Nous utiliserons la notation (fausse) suivante

$$(x, e) = x$$

or

$$\begin{aligned} (x, y) &= (x \oplus e, e \oplus y) \\ &= (x, e) \boxplus (e, y) \\ &= (x, e) \boxplus (ey \oplus \alpha e'e, ee \oplus e'y) \\ &= (x, e) \boxplus [(e, e') \boxdot (y, e)] \end{aligned}$$

d'où la notation suivante

$$(x, y) = x \oplus \omega y \tag{3}$$

avec en particulier,

$$\begin{aligned} (e', e) &= e' \\ (e, e') &= e \oplus \omega e' \\ &= \omega \end{aligned}$$

En utilisant cette notation, les définitions 5.1 s'écrivent

$$(x' \oplus \omega y') \oplus (x'' \oplus \omega y'') = (x' \oplus x'') \oplus \omega(y' \oplus y'') \tag{4}$$

$$(x' \oplus \omega y') \odot (x'' \oplus \omega y'') = (x'x'' \oplus \alpha y'y'') \oplus \omega(x'y'' \oplus y'x'') \tag{5}$$

Il reste à montrer que α est un carré dans l'anneau $(L, \boxplus, \boxdot)$. Considérons l'élément $\omega = (e, e')$ de l'anneau $(L, \boxplus, \boxdot)$. On a alors

$$\begin{aligned}\omega^2 &= (e, e')(e, e') \\ &= (ee \oplus \alpha e'e', ee' \oplus e'e) \\ &= (\alpha, e) \\ &= \alpha\end{aligned}$$

puisqu'on a convenu d'identifier chaque élément x de l'anneau $(K, \oplus, \odot)$ à l'élément $f(x)$ de l'anneau $(L, \boxplus, \boxdot)$. □

L'anneau $(L, \boxplus, \boxdot)$ se note $K[\sqrt{\alpha}]$ et s'appelle une *extension quadratique de* K. On dit que $K[\sqrt{\alpha}]$ s'obtient par *adjonction à* K *d'une racine carré de* α.

6. Eléments inversibles d'une extension quadratique

Soient K un anneau commutatif et α un élément de K. On considère l'extension quadratique $L = K[\sqrt{\alpha}]$.

Définition 6.1. Soit $z = (x, y) = x \oplus \omega y \in L$. On appelle conjugué de z, l'élément $\bar{z}$ de L, tel que

$$\begin{aligned}\bar{z} &= (x, \ominus y) \\ &= x \ominus \omega y\end{aligned}$$

Définition 6.2. Soit $z = x \oplus \omega y \in L$. On appelle norme de z, l'élément

$$\begin{aligned}N(z) &= \bar{z}z \\ &= (x \ominus \omega y) \odot (x \oplus \omega y) \\ &= x^2 \ominus \omega^2 y^2 \\ &= x^2 \ominus \alpha y^2\end{aligned}$$

On remarque que $N(e') = e'$.

Théorème 6.1.

$$\overline{z' \oplus z''} = \bar{z}' \oplus \bar{z}''$$

Démonstration.

$$\begin{aligned}\overline{z' \oplus z''} &= \overline{(x' \oplus \omega y') \oplus (x'' \oplus \omega y'')} \\ &= \overline{(x' \oplus x'') \oplus \omega(y' \oplus y'')} \\ &= (x' \oplus x'') \ominus \omega(y' \oplus y'') \\ &= (x' \oplus x'') \oplus [\ominus \omega y' \oplus (\ominus \omega y'')] \\ &= (x' \ominus \omega y') \oplus (x'' \ominus \omega y'') \\ &= \bar{z}' \oplus \bar{z}''\end{aligned}$$

□

Théorème 6.2.

$$\overline{z'z''} = \bar{z}'\bar{z}''$$

Démonstration.

$$\begin{aligned}
\overline{z'z''} &= \overline{(x' \oplus \omega y') \odot (x'' \oplus \omega y'')} \\
&= \overline{(x'x'' \oplus \alpha y'y'') \oplus \omega(x'y'' \oplus y'x'')} \\
&= (x'x'' \oplus \alpha y'y'') \ominus \omega(x'y'' \oplus y'x'') \\
&= (x'x'' \oplus \alpha y'y'') \oplus [\ominus\omega x'y'' \oplus (\ominus\omega y'x'')] \\
&= (x' \ominus \omega y') \odot (x'' \ominus \omega y'') \\
&= \bar{z}'\bar{z}''
\end{aligned}$$

□

Théorème 6.3.

$$N(z'z'') = N(z')N(z'')$$

Démonstration.

$$\begin{aligned}
N(z'z'') &= \overline{z'z''} \odot z'z'' \\
&= \overline{z'} \odot \overline{z''} \odot z' \odot z'' \\
&= \overline{z'} \odot z' \odot \overline{z''} \odot z'' \\
&= \overline{z'}z' \odot \overline{z''}z'' \\
&= N(z')N(z'')
\end{aligned}$$

□

Théorème 6.4. *Soient K un anneau commutatif, α un élément de K, et z un élément de l'anneau $K[\sqrt{\alpha}]$. Pour que z soit inversible dans l'anneau $K[\sqrt{\alpha}]$, il faut et il suffit que $N(z)$ le soit dans K. On a alors*

$$z^{-1} = N(z)^{-1}\,\bar{z} \tag{6}$$

Démonstration. Supposons z inversible, alors

$$\begin{aligned}
z^{-1}z &= e' \\
N(z^{-1}z) &= N(e') \\
N(z^{-1})N(z) &= e'
\end{aligned}$$

$N(z)$ est donc bien un élément inversible de l'anneau K.
Inversement, supposons $N(z)$ inversible dans K, alors

$$\begin{aligned}
\bar{z}z &= N(z) \\
N(z)^{-1}\,\bar{z}z &= e' \\
N(z)^{-1}\,\bar{z} &= z^{-1}
\end{aligned}$$

donc z est inversible. □

7. Le corps $\mathbb{R}$ des nombres réels

Prenons le cas où $K = \mathbb{R}$, corps des nombres réel, et $\alpha = -1$. D'après le théorème 6.4, l'anneau $\mathbb{R}[\sqrt{-1}]$ est un corps commutatif. Il s'appelle corps des nombres complexes et se note $\mathbb{C}$. Un nombre complexe est un couple de nombres réels (x, y). Les calculs sur les nombres complexes se font grâce aux égalités 4 et 5.

Propriétés. Dans la pratique on utilise seulement les propriétés suivantes des nombres complexes

(1) les nombres complexes forment un corps commutatif $\mathbb{C}$

(2) le corps $\mathbb{R}$ des nombres réels est un sous-corps de $\mathbb{C}$

(3) il existe un nombre complexe i (cette notation remplace la notation ω utilisée pour les extensions quadratiques générales), tel que
$$i^2 = -1$$

(4) $\forall (x, y) \in \mathbb{R}^2$, tout nombre complexe z s'écrit d'une façon et d'une seule, sous la forme
$$z = x + iy$$
$x + iy$ est appelée forme algébrique du nombre complexe (x, y). x est la partie réelle de z, et y est sa partie imaginaire.

On utilise les notations suivantes
$$x = Re(z)$$
$$y = Im(z)$$

Nous pouvons vérifier que tout élément non nul de $\mathbb{C}$ admet un inverse. Soit $z = x + iy$ un nombre complexe. D'après la définition 6.2, sa norme s'écrit
$$\begin{aligned} N(z) &= x^2 - \alpha y^2 \\ &= x^2 + y^2 \end{aligned}$$
et d'après le théorème 6.4, son inverse s'écrit
$$\begin{aligned} z^{-1} &= N(z)^{-1}\, \bar{z} \\ &= \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2} \end{aligned}$$
le dénominateur ne peut s'annuler que si $x = y = 0$, c'est à dire si $z = 0$.

E-mail address: o.castera@free.fr
URL: http://o.castera.free.fr/