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. Cependant, la notion d'élément symétrique revient à introduire une seconde 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

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

Date: 6 novembre 2017.

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

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

(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 dans G, noté $\bar{a}$

$$\forall a \in G, \; \exists \bar{a} \in G \;/ \quad a \square \bar{a} = \bar{a} \square a = e$$

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

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 $(G, \square)$

$$\begin{aligned}
&\forall x \in G, \; x \square e = e \square x = x \\
&(x = e') \Rightarrow (e' \square e = e \square e' = e')
\end{aligned}$$

$$\begin{aligned}
&\forall x \in G, \; x \square e' = e' \square x = x \\
&(x = e) \Rightarrow (e \square e' = e' \square e = e)
\end{aligned}$$

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

□

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 +. On note ces groupes respectivement $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$.

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 $\times$. On note ces groupes respectivement $(\mathbb{Q}^*, \times)$ et $(\mathbb{R}^*, \times)$.

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 $\circledast$

$$\begin{gathered}\forall (g_1,g_2)\in G^2,\ \forall (h_1,h_2)\in H^2,\\ (g_1,h_1)\circledast(g_2,h_2) = (g_1\star g_2, h_1\star h_2)\end{gathered}$$

$(G\times H,\circledast)$ 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

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

(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.

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

□

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, l'addition notée + et la multiplication notée ×, est un anneau noté $(A,+,\times)$, ssi

(1) $(A,+)$ est un groupe abélien
(2) la multiplication est une loi de composition interne
$$\forall (a,b) \in A^2,\ a \times b \in A$$
(3) la multiplication est associative
$$\forall (a,b,c) \in A^3,\ a \times (b \times c) = (a \times b) \times c$$
(4) la multiplication admet un élément neutre 1 dans A
$$\exists 1 \in A \ /\ \forall a \in A,\ 1 \times a = a \times 1 = a$$

(5) la multiplication est distributive à gauche et à droite par rapport à l'addition

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

Définition 2.2. Un anneau $(A, +, \times)$ est dit commutatif ssi la multiplication est commutative

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

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

Soit 0 *l'élément neutre de la loi* $+$: $\forall x \in A,\ 0 \times x = x \times 0 = 0$

Soit $-y$ *le symétrique de* y *pour la loi* $+$:

$$\forall (x, y) \in A^2,\ x \times (-y) = -(x \times y)$$
$$\forall (x, y, z) \in A^3,\ x \times [y + (-z)] = (x \times y) + [x \times (-z)]$$

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

$$\forall n \in \mathbb{N},\ \forall (x, y) \in A^2,\ (x + y)^n = \sum_{k=0}^{n} C_n^k x^k \times y^{n+(-k)}$$

2.1. **Anneau intègre.**

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

$$\exists b \neq 0 \in A \ / \ a \times b = 0$$

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

$$\exists b \neq 0 \in A \ / \ b \times a = 0$$

Définition 2.5. Un anneau $(A, +, \times)$ est intègre s'il est différent de l'élément nul $\{0\}$, commutatif, et sans diviseur de zéro.

Théorème 2.1. *Pour tout anneau* $(A, +, \times)$ *intègre*

$$\forall (a, b) \in A^2,\ (a \times b = 0) \Rightarrow (a = 0 \ \text{ou}\ b = 0)$$

2.2. **Sous-anneau.**

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

(1) $(A', +, \times)$ est un anneau

(2) A' est stable pour l'addition

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

(3) A' est stable pour la multiplication

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

2.3. **Morphisme d'anneaux.**

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

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

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

(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 l'addition $+$ et de la multiplication $\times$ est un corps, noté $(K, +, \times)$, ssi

(1) $(K, +, \times)$ est un anneau
(2) tout élément non nul a de K possède un inverse dans K pour la multiplication, noté a^{-1},
$$\forall a \in K,\ a \neq 0,\ \exists a^{-1} \in K \ /\ a \times a^{-1} = a^{-1} \times a = 1$$

Définition 3.2. Un corps $(K, +, \times)$ est dit commutatif ssi la multiplication est commutative
$$\forall (a,b) \in K^2,\ a \times b = b \times a$$

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

Démonstration. D'après la définition 3.1, si $(K, +, \times)$ est un corps
$$\forall a \in K,\ a \neq 0,\ \exists a^{-1} \in K \ /\ a \times a^{-1} = a^{-1} \times a = 1$$
Pour démontrer que
$$(a \times b = 0) \Rightarrow (a = 0 \text{ ou } b = 0)$$
nous allons montrer que si $a \times b = 0$ alors il est impossible d'avoir à la fois $a \neq 0$ et $b \neq 0$.
$$\begin{aligned} \forall (a,b) \in K^2,\ a \times b &= 0 \\ \forall a \in K,\ a \neq 0,\ a^{-1} \times a \times b &= a^{-1} \times 0 \\ 1 \times b &= 0 \\ b &= 0 \end{aligned}$$
Et par symétrie des rôles de a et b, si $b \neq 0$ alors $a = 0$. □

3.1. **Sous-corps.**

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

(1) $(K', +, \times)$ est un corps
(2) K' est stable pour l'addition

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

(3) K' est stable pour la multiplication

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

4. Racines Carrées

Soit $(A, +, \times)$ un anneau commutatif. Nous dirons qu'un élément α de A est un carré dans A ssi

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

x est appelée racine carrée de α dans $(A, +, \times)$. Si x est une racine carrée de α dans A alors il en est de même de $-x$, car $(-x)^2 = \alpha$. Si l'anneau $(A, +, \times)$ est intègre, α ne peut admettre plus de deux racines carrées dans A, car la relation $x^2 = y^2$, qui s'écrit dans tous les cas sous la forme $(x - y)(x + y) = 0$, implique soit $x = y$, soit $x = -y$.

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

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

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

$$(A, +, \times) \subseteq (L, +, \times)$$

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

$$\forall z \in L',\ \exists (x,y) \in A^2 \ / \ z = x + (\omega \times y)$$

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

$$z = x + \omega y$$

Théorème 4.1. $(L', +, \times)$ *est un sous-anneau de* $(L, \boxplus, \boxdot)$ *contenant* $(A, +, \times)$ *et* ω*.*

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

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

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

$$\begin{aligned}
(x' + \omega y') \times (x'' + \omega y'') &= x'x'' + x'\omega y'' + \omega y' x'' + \omega y' \omega y'' \\
&= x'x'' + \alpha y' y'' + x' \omega y'' + \omega y' x'' \\
&= (x'x'' + \alpha y'y'') + \omega (x'y'' + y'x'') \in L' \qquad (2)
\end{aligned}$$

L' est donc stable pour les lois $+$ et $\times$. D'après la définition 2.6, $(L', +, \times)$ est un sous-anneau de $(L, \boxplus, \boxdot)$. De plus, l'anneau L' contient l'anneau A (poser $y = 0$), et il contient aussi ω (poser $x = 0$ et $y = 1$). □

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

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

alors f est *surjective*

$$\forall u \in L,\ \exists (x, y) \in A^2 \ /\ f(x, y) = u$$

Remarque. Si $(A, +, \times)$ est un corps et si α n'est pas un carré dans $(A, +, \times)$, alors l'application f est *injective*

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

Démonstration.

$$\begin{aligned}
f(x', y') &= f(x'', y'') \\
x' + \omega y' &= x'' + \omega y'' \\
(x' - x'') + \omega (y' - y'') &= 0
\end{aligned}$$

Posons $X = x' - x'' \in A$, et $Y = y' - y'' \in A$

$$X + \omega Y = 0$$

Raisonnons par l'absurde. Commençons par supposer $Y \neq 0$.

Y est inversible dans A puisque par hypothèse A est un corps, par conséquent

$$\omega = (-X)Y^{-1} \in A$$

contrairement à l'hypothèse que α n'est pas un carré dans A.
Donc $Y = 0$. Par conséquent $X = 0$, $x' = x''$, $y' = y''$ et f est *injective.* □

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

$$f(x', y') + f(x'', y'') = f(x' + x'', y' + y'')$$
$$f(x', y') \times f(x'', y'') = f(x'x'' + \alpha y'y'', x'y'' + y'x'')$$

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

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

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

lesquelles font intervenir à la fois l'élément α et les lois de composition dans l'anneau $(A, +, \times)$.

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 A muni de la loi de composition $+$ est un groupe abélien. D'après le théorème 1.3, le produit direct des groupes abéliens $A \times A$ 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 A.

$x'x'' + \alpha y'y'' \in A$ et $x'y'' + \alpha y'x'' \in A$
On pose $a = (x', y') \in L$ et $b = (x'', y'') \in L$

$$\begin{aligned} a \boxdot b &= (x', y') \boxdot (x'', y'') \\ &= (x'x'' + \alpha y'y'', x'y'' + y'x'') \end{aligned}$$

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

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

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

et d'autre part

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

L'associativité s'obtient en comparant les résultats.

(4) Montrons que la loi $\boxdot$ admet $(1, 0)$ comme élément neutre

$$\begin{aligned} (1, 0) \boxdot (x, y) &= (1x + \alpha 0y, 1y + 0x) \\ &= (x + \alpha 0, y + 0) \\ &= (x, y) \end{aligned}$$

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

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

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

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

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

Théorème 5.3. *L'anneau* $(L, \boxplus, \boxdot)$ *contient un sous-anneau isomorphe à l'anneau* $(A, +, \times)$.

Démonstration. Considérons l'application

$$f : A \to A \times A$$
$$f(x) = (x, 0)$$

A tout élément $(x, 0)$ de l'ensemble $A \times A$ correspond un élément unique x de l'ensemble A par f. Par conséquent f est bijective

$$\forall (x, 0) \in A^2, \ \exists! \ x \in A \ / \ f(x) = (x, 0)$$

De plus, nous avons les relations suivantes

$$\begin{aligned} f(x') \boxplus f(x'') &= (x', 0) \boxplus (x'', 0) \\ &= (x' + x'', 0 + 0) \\ &= (x' + x'', 0) \\ &= f(x' + x'') \end{aligned}$$

$$\begin{aligned} f(x') \boxdot f(x'') &= (x', 0) \boxdot (x'', 0) \\ &= (x'x'' + \alpha 0 \times 0, x'0 + x''0) \\ &= (x'x'', 0) \\ &= f(x'x'') \end{aligned}$$

$$f(1) = (1, 0)$$

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

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

$$(x, e) = x$$

or

$$\begin{aligned} (x, y) &= (x + 0, 0 + y) \\ &= (x, 0) \boxplus (0, y) \\ &= (x, 0) \boxplus (0y + \alpha 1 \times 0, 0 \times 0 + 1y) \\ &= (x, 0) \boxplus [(0, 1) \boxdot (y, 0)] \end{aligned}$$

d'où la notation suivante

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

avec en particulier,

$$\begin{aligned}(1,0) &= 1\\ (0,1) &= 0 + \omega 1\\ &= \omega\end{aligned}$$

En utilisant cette notation, les définitions 5.1 s'écrivent

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

$$(x' + \omega y') \times (x'' + \omega y'') = (x'x'' + \alpha y'y'') + \omega(x'y'' + y'x'') \tag{5}$$

Il reste à montrer que α est un carré dans l'anneau $(L, \boxplus, \boxdot)$. Considérons l'élément $\omega = (0,1)$ de l'anneau $(L, \boxplus, \boxdot)$. On a alors

$$\begin{aligned}\omega^2 &= (0,1)(0,1)\\ &= (0 \times 0 + \alpha 1 \times 1, 0 \times 1 + 1 \times 0)\\ &= (\alpha, 0)\\ &= \alpha\end{aligned}$$

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

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

6. Eléments inversibles d'une extension quadratique

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

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

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

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

$$\begin{aligned}N(z) &= \bar{z}z\\ &= (x - \omega y) \times (x + \omega y)\\ &= x^2 - \omega^2 y^2\\ &= x^2 - \alpha y^2\end{aligned}$$

On remarque que $N(1) = 1$.

Théorème 6.1.

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

Démonstration.

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

□

Théorème 6.2.

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

Démonstration.

$$\begin{aligned}
\overline{z' z''} &= \overline{(x' + \omega y') \times (x'' + \omega y'')} \\
&= \overline{(x'x'' + \alpha y'y'') + \omega(x'y'' + y'x'')} \\
&= (x'x'' + \alpha y'y'') - \omega(x'y'' + y'x'') \\
&= (x'x'' + \alpha y'y'') + [-\omega x'y'' + (-\omega y'x'')] \\
&= (x' - \omega y') \times (x'' - \omega y'') \\
&= \bar{z}' \bar{z}''
\end{aligned}$$

□

Théorème 6.3.

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

Démonstration.

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

□

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

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

Démonstration. Supposons z inversible, alors

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

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

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

donc z est inversible. □

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

Prenons le cas où $A = \mathbb{R}$, corps des nombres réel, et $\alpha = -1$. D'après le théorème 5.2, $\mathbb{R}[\sqrt{-1}]$ 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

$$\begin{aligned} x &= Re(z) \\ y &= Im(z) \end{aligned}$$

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/`