Chapitre II

Arithmétique

1 Divisibilité

Remarque : dans ce chapitre, on désignera par **entier** un élément de $\mathbb{Z}$. Les éléments de $\mathbb{N}$ seront appelés **entiers positifs**.

1.2 Généralités

Définition

Soient $a, b \in \mathbb{Z}$, on dit que a **divise** b ou que a est un **diviseur** de b ou encore que b est un **multiple** de a si et seulement si il existe $q \in \mathbb{Z}$ tel que $b = a\,q$.

Propriétés immédiates

- Les seuls diviseurs de 1 sont 1 et -1,
  car pour tout $a, q \in \mathbb{Z}$, $aq = 1$ implique a inversible dans $\mathbb{Z}$, c.a.d. $a = 1$ ou $a = -1$.
- Tout entier divise 0, c.a.d. 0 est un multiple de tout entier,
  car pour tout $a \in \mathbb{Z}$, $a.0 = 0$.
- Le seul multiple de 0 est 0 c.a.d. 0 est le seul entier divisible par 0,
  car pour tout b enier, s'il existe $q \in \mathbb{Z}$ tel que $b = 0.q$ alors $b = 0$.
- Tout entier n est divisible par 1 et -1,
  car $n = 1.n = (-1).(-n)$.
- Tout entier n est divisible par lui-même et par son opposé $-n$,
  car $n = 1.n = (-1).(-n)$.

Propriété

Soit $b \in \mathbb{Z}^*$ (b entier non nul). Si a est un diviseur de b alors il existe un **unique** q tel que $b = a\,q$.

Démonstration
Rappelons la définition de b divise a : $\exists q \in \mathbb{Z},\ a = b\,q$.
La nouvelle propriété que nous venons d'énoncer, ajoute que si b est non nul, alors l'entier q est unique.
En effet, supposons q et q' tels que $a = b\,q = b\,q'$ alors $b(q - q') = 0$ or b est non nul donc $q = q'$.

Propriété

Soient a, b et c des entiers.

1) Si a divise b et b divise c alors a divise c.
2) Si a divise b et b divise a alors $a = \pm b$.
3) Si a divise b et c alors a divise $b + c$.
4) Si a divise b alors a divise bc.
5) Si a divise b alors ac divise bc.

Démonstrations :

1) Supposons que a divise b et b divise c alors il existe des entiers q et q' tels que $b = qa$ et $c = q'b$.
   Il suit que $c = qq'\,a$. Comme qq' est entier, on conclut que a divise c.
2) Supposons que a divise b et b divise a. Alors il existe deux entiers q et q' tels que $a = qb$ et $b = q'a$.
   Il suit que $a = qq'\,a$ c.a.d. $a(qq' - 1) = 0$ (1).
   Cas $a = 0$: comme $a = 0$ divise b, nécessairement $b = 0$ car le seul entier divisible par 0 est 0 donc $a = b$.
   Cas $a \neq 0$: alors (1) implique $qq' = 1$.
   Il suit que q est un entier inversible. Or les seuls entiers inversibles sont 1 et -1.
   Conclusion : $a = \pm b$.
3) Supposons que a divise b et c alors il existe des entiers q et q' tels que $b = qa$ et $c = q'a$.
   Il suit que $b + c = (q + q')a$. Comme $q + q'$ est entier, on en conclut que a divise $b + c$.
4) Supposons que a divise b alors il existe un entier q tel que $b = qa$.
   Il suit que $bc = qca$ donc a divise bc.
5) Supposons que a divise b alors il existe un entier q tel que $b = qa$.
   Il suit que $bc = qac$ donc ac divise bc.

Lemme

Soit $a \in \mathbb{N}^*$ (a entier positif non nul). Si d est un diviseur de a alors $-a \leqslant d \leqslant a$.

Démonstration

Soit d un diviseur de a, alors il existe q tel que $a = d\,q$.

Cas d positif : comme $a > 0$ par hypothèse, on a aussi $q > 0$, c.a.d. $q \geqslant 1$. Supposons par l'absurde $d > a$ alors, par multiplication sur des nombres strictement positifs, on aurait $a = dq > 1.a = a$. Contradiction. Donc $d \leqslant a$.

Cas d négatif : $-d$ est un diviseur positif de a donc d'après ce qui précède, $-d \leqslant a$ c.a.d. $-a \leqslant d$.

1.3 Division euclidienne

Propriété

Soit a un entier et b un entier **positif non nul**.
Il existe un unique couple d'entier (q, r) tel que :

$$a = b\,q + r \quad et \quad 0 \leqslant r < b$$

On dit que q est le **quotient** et r est le **reste** de la **division euclidienne** de a par b.

Exemple :
Division euclidienne de 51 par 8 :
On a $51 = 8.6 + 3$ avec $0 \leqslant 3 < 8$, donc 6 est le quotient et 3 le reste de la division euclidienne de 51 par 8.

Démonstration : soit a un entier et b un entier **positif non nul**.

- **Existence du couple** (q, r).

- Cas $a = 0$: $(q, r) = (0, 0)$ convient car $a = 0 = 0.b + 0$ et le reste vérifie $0 < b$.
- Cas $a > 0$: introduisons l'ensemble $M = \{k \mid k \in \mathbb{N} \text{ et } k\,b \leqslant a\}$.
  M est non vide car $0.b \leqslant a$ donc M contient 0.
  De plus, si k est un élément de M, comme $b \geqslant 1$, on ne peut pas avoir $k > a$ sinon on aurait $k\,b > a$ contradictoire avec $k \in M$. Donc $M \subset \{0, \ldots, a\}$.
  Mais les entiers compris entre 0 et a sont en nombre fini donc a fortiori M est fini.
  Il suit que M admet un plus grand élément que l'on note q. Et l'on pose $r = a - bq$.
  Par définition de M, $bq \leqslant a$ donc $r \geqslant 0$.
  De plus, supposons par l'absurde $r \geqslant b$, on aurait alors $a - bq \geqslant b$ donc $a - b(q + 1) \geqslant 0$. Il suivrait que $q + 1 \in M$ en contradiction avec q est le plus grand élément de M.
  Conclusion : le couple (q, r) vérifie la propriété $a = b\,q + r \quad et \quad 0 \leqslant r < b$.
- Cas $a < 0$: on applique ce qui précède à $a' = -a$, il existe $(q', r') \in \mathbb{Z}^2$ tel que $a' = b\,q' + r' \quad$ et $0 \leqslant r' < b$.
  Si $r' = 0$, alors on pose $q = -q'$ et $r = 0$. On a $a = -a' = -bq' = bq$. Donc le couple (q, r) convient.
  Sinon on a $0 < r' < b$. On pose $q = -q' - 1$ et $r = b - r'$.
  On a $a = -a' = -b\,q' - r' = b\,(-q' - 1) + (b - r') = b\,q + r$.
  De $0 < r' < b$, on déduit $-b < -r' < 0$ c.a.d. $0 < r = b - r' < b$.
  Donc le couple (q, r) convient.

- **Unicité du couple** (q, r).
  Supposons l'existence de deux couples d'entiers (q, r) et (q', r') vérifiant $a = b\,q + r = b'\,q + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b$.
  On a $b(q - q') + (r - r') = 0$ donc $b(q - q') = r' - r$. (1)
  $-b < -r \leqslant 0$ et $0 \leqslant r' < b$ implique par addition que $-b < r' - r < b$ donc d'après (1), $-b < b(q - q') < b$.
  Comme b est strictement positif, il suit que $-1 < q - q' < 1$.
  Comme $q - q'$ est un entier on conclut que $q = q'$.
  Par conséquent, $r = a - bq = a - b'q = r'$. (CQFD)

Propriété

Soit a un entier et b un entier **positif non nul**.
a est divisible par b si et seulement si le reste de la division euclidienne de a par b est nul.

Démonstration : soit a un entier et b un entier **positif non nul**. Supposons que a est divisible par b, alors il existe q tel que $a = bq$. Le couple $(q, 0)$ convient pour la division euclidienne de a par b. Par unicité de la division euclidienne, son reste est nul.

Supposons que le reste de la division euclidienne de a par b est nul, alors cette division s'écrit $a = q\,b$. Il découle que a est divisible par b.

1.4 Congruence

Définition

Soient a, b et n des entiers, on dit que a **est congru à** b **modulo** n et on note $a \equiv b[n]$ si et seulement si $a - b$ est un multiple de n.

Règles de calcul

Soient n, m et a, b, c, d des entiers :

- Si $a \equiv b\,[n]$ alors $b \equiv a\,[n]$.
- Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.
- Si $a \equiv c\,[n]$ et $b \equiv d\,[n]$ alors $a + b \equiv c + d\,[n]$.
- Si $a \equiv c\,[n]$ et $b \equiv d\,[n]$ alors $ab \equiv cd\,[n]$.
- Si $a \equiv b\,[n]$ alors $ma \equiv mb\,[mn]$.

Démonstration

1) Si n divise $a-b$ alors n divise $b-a$ (CQFD).
2) Si n divise $a-b$ et n divise $b-c$ alors n divise $a-b+b-c=a-c$ (CQFD).
3) Si n divise $a-c$ et n divise $b-d$ alors n divise $a-c+b-d=(a+b)-(c+d)$ donc $a+b \equiv c+d\,[n]$.
4) Si n divise $a-c$ et n divise $b-d$ alors n divise $b(a-c)$ et $c(b-d)$ donc n divise $b(a-c)+c(b-d)=ab-cd$ c.a.d. $ab \equiv cd\,[n]$.
5) Si n divise $a-b$ alors mn divise $m(b-a)=mb-ma$ (CQFD).

1.5 Plus grand commun diviseur (PGCD)

Définition

Soient $a, b \in \mathbb{Z}$ non tous deux nuls (c.a.d. $a \neq 0$ ou $b \neq 0$).
Le plus grand entier qui divise a et b s'appelle le **plus grand diviseur commun** de a et b et se note $\text{pgcd}(a,b)$.

Justification : Cette définition a un sens car l'ensemble D des diviseurs communs à a et b est fini et non vide, il en découle que D admet un plus grand élément.

En effet, D est non vide car il contient 1 qui est un diviseur commun à tous les entiers.

De plus, on sait que a ou b est non nul. Supposons que ce soit a, tout diviseur de a est un diviseur de $|a| > 0$ et d'après une propriété précédente, tout diviseur d de $|a|$ vérifie $-|a| \leqslant d \leqslant |a|$.

A fortiori les diviseurs d communs à a et b vérifient $-|a| \leqslant d \leqslant |a|$ donc D est donc un ensemble fini.

Propriétés immédiates

- $\text{pgcd}(a,b) = \text{pgcd}(b,a)$ pour tous les entiers a, b non tous deux nuls.
- $\text{pgcd}(0,a) = a$ pour tout entier $a > 0$.
- $\text{pgcd}(1,a) = 1$ pour tout entier a.

Propriété

Soient a et b des entiers **positifs** avec b **non nul**.
Si r est le reste de la division euclidienne de a par b alors $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

Démonstration

Comme $b > 0$, la division euclidienne de a par b est bien définie. Notons q le quotient, on a $a = bq + r$.
Notons D l'ensemble des diviseurs communs de a et b et D' l'ensemble des diviseurs communs de b et r.
On veut montrer que $D = D'$.

- $D \subset D'$: soit $d \in D$, d divise a et b, donc d divise $-bq$ et d divise $a - bq = r$, il suit que $d \in D'$.
- $D' \subset D$: soit $d \in D'$, d divise b et r, donc d divise bq et d divise $bq + r = a$, il suit que $d \in D$.

$D = D'$ donc le plus grand élément de D qui est $\text{pgcd}(a,b)$ est aussi le plus grand élément de D' qui est $\text{pgcd}(b,r)$.

Algorithme d'Euclide

```
entrées : a, b positifs, b ≠ 0
sortie : pgcd(a,b)

1    Tant que b ≠ 0 faire
2        q, r ← quotient, reste de la division euclidienne de a par b
3        a ← b
4        b ← r
5    retourner a
```

Propriété

Soit a et b des entiers **positifs** avec b **non nul**.
La valeur de retour de l'algorithme d'Euclide est le pgcd de a et b.

Preuve
On note a_0 et b_0 les valeurs initiales de a et b.

Numérotons chaque exécution de la ligne 1 en commençant à 1.

On définit la propriété P_k :
"A la k-ième exécution de la ligne 1, $\text{pgcd}(a, b) = \text{pgcd}(a_0, b_0)$ et a, b sont positifs".

Initialisation : P(1) est vraie car alors $a = a_0 \geqslant 0$ et $b = b_0 \geqslant 0$.

Hérédité : supposons que $P(k)$ est vraie. Il y a deux cas pour la k-ième exécution de la ligne 1 :

- Si $b = 0$ alors on sort de l'algorithme.
- Si $b \neq 0$ alors d'après P_k, on a $a \geqslant 0$ et $b > 0$ donc on peut appliquer la propriété précédente et après la ligne 2, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.
  Par hypothèse de récurrence, il suit que $\text{pgcd}(b, r) = \text{pgcd}(a_0, b_0)$.
  D'après les propriétés de la division euclidienne, $0 \leqslant r < b$.
  Après les affectations des lignes 3 et 4, donc à l'itération $k+1$ de la ligne 1, on a $\text{pgcd}(a, b) = \text{pgcd}(a_0, b_0)$ et $a > b \geqslant 0$, ce qui implique P_{k+1}.

On en conclut par récurrence que P_k est vraie tant que l'algorithme continue.

L'algorithme se termine nécessairement car b décroit strictement à chaque itération d'après la propriété $r < b$ de la division euclidienne.

A la sortie de l'algorithme, en notant f le numéro de la dernière itération de la ligne 1, on a P_f avec $b = 0$ donc $\text{pgcd}(a_0, b_0) = \text{pgcd}(a, 0) = a$. CQFD car a est la valeur de retour.

2 Nombres premiers entre eux

2.2 Définition et propriétés

Définition

Soient a et b des entiers **non tous deux nuls**, on dit que a et b sont premiers entre eux si $\text{pgcd}(a, b) = 1$.

Propriété

Soient a et b des entiers **non nuls**, les quotients de a et b par $\text{pgcd}(a, b)$ sont des nombres premiers entre eux.

Démonstration
Posons $d := \text{pgcd}(a, b)$ et q et q' les quotients de a et b par d. On note aussi $k := \text{pgcd}(q, q')$. On veut montrer que $k = 1$.

D'après ces définitions, k divise q et q', donc dk divise $a = dq$ et $b = dq'$, donc $dk \leqslant d$ par définition du pgcd.
Par propriété du pgcd, a et b étant non nul, $d \geqslant 1$ et il suit que $dk \leqslant d$ implique $k \leqslant 1$.
Toujours par propriété du pgcd, a et b étant non nul, q et q' sont non nuls donc $k \geqslant 1$.
Conclusion : $k = 1$ (CQFD).

Théorème de Bezout

Soient a et b des entiers **positifs non nuls**, alors il existe des entiers u et v tels que $\text{pgcd}(a, b) = a\,u + b\,v$.

Démonstration : cette existence est montrée dans la preuve de l'algorithme d'Euclide étendu.

Algorithme d'Euclide étendu

Soient a et b des entiers **positifs non nuls**. L'**algorithme d'Euclide étendu** est :

entrées : a, b positifs non nuls
sortie : $r = \text{pgcd}(a,b)$ et u, v entiers tels que $r = au + bv$

```
1    Initialisation : (r, u, v, r', u', v') ← (a, 1, 0, b, 0, 1)
2    Tant que r' ≠ 0 faire
3        q ← quotient de la division euclidienne de r par r'
4        (r, u, v, r', u', v') ← ( r', u' , v' , r - q r' , u - q u' , v - q v' )
5    retourner (r, u, v)
```

Propriété

Soient a et b des entiers **positifs non nuls**, l'algorithme d'Euclide étendu retourne $\text{pgcd}(a,b)$ et u, v tels que $\text{pgcd}(a,b) = a\ u + b\ v$.

Preuve
Si on regarde seulement les variables r et r', il s'agit du même algorithme que celui d'Euclide. Ce qui prouve la terminaison et qu'en sortie, $r = \text{pgcd}(a,b)$.

Etudions maintenant la propriété Q_k : "à la k-ième exécution de la ligne 2, $au+bv = r$ et $a'u'+b'v' = r'$ ".

Initialisation : Q_1 est vraie car à l'initialisation, $r = a$, $u = 1$ et $v = 0$ d'une part, $r' = b$, $u' = 0$ et $v' = 1$ d'autre part.

Hérédité : supposons Q_k vraie, il y a deux cas pour la k-ième exécution de la ligne 2 :

- Si $r' = 0$ alors on sort de l'algorithme.
- Si $r' \neq 0$ alors on peut effectuer la division euclidienne de r par r' et à la ligne 3, q reçoit son quotient. D'après Q_k, $au+bv = r$ et $a'u'+b'v' = r'$ donc $r-qr' = (au+bv)-q(a'u'+b'v') = au-qa'u'+bv-qb'v' = a(u-qu') + b(v-qv')$. (1)
  D'une part, la ligne 4 effectue les affectations $r \leftarrow r'$, $u \leftarrow u'$ et $v \leftarrow v'$ donc par hypothèse de récurrence, on a à l'issue, $au + bv = r$.
  D'autre part, la ligne 4 effectue $r' \leftarrow r - qr'$, $u' \leftarrow u - qu'$ et $v' \leftarrow v - qv'$ donc , d'après (1), on a à l'issue, $a'u' + b'v' = r'$.
  On a donc bien Q_{k+1}.

On en conclut par récurrence que Q_k est vraie tant que l'algorithme continue.

A la sortie de l'algorithme, on sait par la preuve de l'algorithme d'Euclide que $r = \text{pgcd}(a,b)$.
De plus, en notant f le numéro de la dernière itération de la ligne 1, on a Q_f donc $au+bv = r = \text{pgcd}(a,b)$.

Propriété

Soient a et b des entiers **positifs non nuls**, alors a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que $a\ u + b\ v = 1$.

Démonstration
Si a et b sont premiers entre eux, le théorème de Bezout affirme l'existence d'entiers u et v tels que $au + bv = \text{pgcd}(a,b) = 1$.

Si il existe des entiers u et v tels que $a\ u + b\ v = 1$, considérons un diviseur positif d de a et b, alors d divise au et divise bv donc d divise $au + bv = 1$. Il suit que $d = 1$.
On en conclut que $\text{pgcd}(a,b) = 1$.

Remarque
Cette prorpiété est une réciproque au théorème de Bezout **uniquement pour des nombres premiers entre eux.**

Il n'y a pas de réciproque au théorème de Bezout dans le cas général.
Voici un contre-exemple avec $a = 2$ et $b = 3$: $2.4 - 3.2 = 2$ donc il existe u et v tels que $au + bv = 2$ et pourtant $\text{pgcd}(2, 3) = 1$.

Propriété

Soient a et b des entiers **positifs non nuls** :

1) Tout diviseur commun à a et b divise $\text{pgcd}(a, b)$.
2) Soit d un diviseur **positif** commun à a et b, alors $d = \text{pgcd}(a, b)$ si et seulement si d est divisible par tout diviseur commun à a et b.
3) Pour tout entier m positif non nul, $\text{pgcd}(ma, mb) = m\ \text{pgcd}(a, b)$.

Démonstration

1) Posons $d := \text{pgcd}(a, b)$. D'après le théorème de Bezout, il existe des entiers u et v tels que $d = au + bv$. Considérons p un diviseur commun à a et b. Il divise donc au et bv donc il divise aussi $au + bv = d$. (CQFD)
2) Soit d un diviseur **positif** commun à a et b. Par définition du pgcd, $d \leqslant \text{pgcd}(a, b)$. (1)
   Supposons $d = \text{pgcd}(a, b)$ alors on vient de montrer qu'il est divisible par tout diviseur commun à a et b.
   Inversement, supposons que d est divisible par tout diviseur commun à a et b, il est divisible aussi par le plus grand d'entre eux qui est $\text{pgcd}(a, b)$.
   Comme d est strictement positif, il suit que $\text{pgcd}(a, b) \leqslant d$. (2)
   D'après (1) et (2), $d = \text{pgcd}(a, b)$.
3) Posons $d := pgcd(a, b)$. Soit un entier $m > 0$.
   Comme $d \geqslant 0$ et d divise a et b, md est un diviseur positif de ma et mb. (1)
   D'après le théorème de Bezout, il existe des entiers u et v tels que $d = au + bv$.
   Considérons un diviseur positif k commun à ma et mb, alors k divise mau et mbv,
   donc k divise $md = mau + mbv$. (2)
   D'après la proposition démontrée en 2), les résultats (1) et (2) impliquent que $md = \text{pgcd}(ma, mb)$. (CQFD)

Théorème de Gauss

Soient a, b et c des entiers **positifs non nuls**. Si a divise $b\,c$ et si a est premier avec b, alors a divise c.

Démonstration
D'après la propriété précédente, $\text{pgcd}(ac, bc) = c\ \text{pgcd}(a, b) = c$ puisque a et b sont premiers entre eux.
Comme a divise bc par hypothèse, et de manière évidente a divise ac, il suit, d'après la propriété 1) précédente, que a divise aussi $\text{pgcd}(ac, bc)$, c'est-à-dire a divise c.

2.3 Plus petit commun multiple

Propriété et définition

Soient a et b des entiers non nuls, il existe un plus petit commun multiple positif et non nul de a et b qui est noté $\text{ppcm}(a, b)$.

Justification : l'ensemble des multiples strictement positifs communs à a et b est non vide car il contient $|ab|$. Or toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Donc l'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément.

Propriétés immédiates

- $\text{ppcm}(a, b) = \text{ppcm}(b, a)$ pour tous les entiers a, b.
- $\text{ppcm}(1, a) = a$ pour tout entier $a \geqslant 0$.

Propriété

Soient a et b des entiers **positifs non nuls**, $a\,b = \text{pgcd}(a,b)\ \text{ppcm}(a,b)$.

Démonstration
Notons $d := \text{pgcd}(a,b)$, q et q' les quotients respectifs de a et b par d. D'après un théorème de la section précédente, on sait que $\text{pgcd}(q,q') = 1$.
Posons $m := q\,d\,q'$.

D'après ces définitions, $dm = d\,q\,d\,q' = ab$. (1)

On a aussi $m = aq' = qb$ donc m est un multiple commun à a et b. Montrons que $m = \text{ppcm}(a,b)$.

Soit l un multiple strictement positif de a et b. Notons k et k' les quotients respectifs de l par a et b.

On a $l = ka = k'b$ et donc, $kqd = k'q'd$. (2)

Comme $d \neq 0$ car a et b sont non nuls, (2) implique $kq = k'q'$.

q divise $k'q'$ et $\text{pgcd}(q,q') = 1$, donc, par le théorème de Gauss, q divise k'. Donc $bq = m$ divise $bk' = l$.

De $l > 0$ et m divise l, on déduit $m \leqslant l$.

On a montré que m est un multiple commun à a et b et que tout multiple l commun à a et b est supérieur à m donc $m = \text{ppcm}(a,b)$.

Conclusion : l'égalité (1) s'écrit $ab = \text{pgcd}(a,b).\,\text{ppcm}(a,b)$.

Propriété

Soient a et b des entiers **non nuls**, a et b sont premiers entre eux si et seulement si $\text{ppcm}(a,b) = ab$.

Démonstration
On sait que $a\,b = \text{pgcd}(a,b)\ \text{ppcm}(a,b)$.
Comme par hypothèse, $ab \neq 0$, il suit que $\text{pgcd}(a,b) = 1 \ \Leftrightarrow\ \text{ppcm}(a,b) = ab$.

2.4 Équation diophantienne

2.4.1 Problème

Soient a, b et c des entiers avec a **et** b **non nuls**.
Résoudre dans $\mathbb{Z}$ l'équation (E) $ax + by = c$ d'inconnues x et y.
Une telle équation est appelée équation diophantienne.

2.4.2 Méthode

La résolution d'une telle équation utilise les théorèmes de Bezout et Gauss. On l'effectue en trois étapes.

Etape 1 : calculer $pgcd(a,b)$.

Si c **n'est pas un multiple** de $\text{pgcd}(a,b)$, l'équation $au + bv = c$ n'a **pas de solution**.

Démonstration
Posons $d := \text{pgcd}(a,b)$.
Pour tout couple (x,y) d'entiers, d divise a donc ax et d divise b donc by. Il suit que d divise $ax + by$.
Comme c n'est pas divisible par d, nécessairement (x,y) n'est pas solution.

Etape 2 : si c est un **multiple** de $\text{pgcd}(a,b)$, l'équation $ax + by = c$ admet des solutions et on recherche une **solution particulière**.

On note $d := \text{pgcd}(a, b)$. On calcule le quotient de c par d que l'on note m.
L'algorithme d'Euclide étendu appliqué à a et b fournit des entiers u et v tels que $au + bv = d$.
Une solution particulière de l'équation $ax + by = c$ est $(x_0, y_0) = (mu, mv)$.

Démonstration
Le couple (u, v) vérifie $au+bv = d$ donc $(x_0, y_0) = (mu, mv)$ vérifie $ax_0+by_0 = amu+bmv = m(au+bv) = md = c$. (CQFD)

Cas particulier : si a et b sont premiers entre eux, c est toujours un multiple de $1 = \text{pgcd}(a, b)$ donc l'équation $ax + by = c$ admet des solutions.

Cas particulier $c = \text{pgcd}(a, b)$: dans ce cas, l'algorithme d'Euclide étendu fournit directement une solution (u, v) de (E).

Etape 3 : si c est un multiple de $\text{pgcd}(a, b)$, on recherche **toutes les solutions** de l'équation $ax + by = c$.

On note $d := \text{pgcd}(a, b)$ et (x_0, y_0) la solution particulière déterminée à l'étape 2.
On calcule a' et b' les quotients respectifs de a et b par d.
L'ensemble des solutions est $S = \{(x_0 + kb', y_0 - ka') \,|\, k \in \mathbb{Z}\}$.

Démonstration
On rappelle que $\text{pgcd}(a', b') = 1$, d'après une propriété démontrée précédemment.

Soit (x, y) un couple d'entier.
(x, y) est solution de (E) si et seulement si $ax + by = c = au + bv$.

Mais $ax + by = au + bv \Leftrightarrow a(x - u) = b(v - y) \Leftrightarrow a'(x - u) = b'(v - y)$ (1).

La dernière équivalence est permise car $d \neq 0$.

Supposons que (x, y) est solution alors, d'après (1), a' divise $b'(v - y)$, mais comme a' est premier avec b', d'après le théorème de Gauss, a' divise $(v - y)$ donc il existe un entier k tel que $v - y = k\,a'$.
De même pour b' et $a'(x - u)$, qui implique qu'il existe un entier l tel que $x - u = l\,b'$.

(1) s'écrit alors : $a'lb' = b'ka'$.

Comme a' et b' sont non nuls parce que a et b ne le sont pas, (1) implique $l = k$.

Finalement, une condition nécessaire est : $\exists k \in \mathbb{Z}$, tels que $(x, y) = (u + kb', v - ka')$.

Inversement, soit un couple $(x, y) = (u + kb', v - ka')$ avec $k \in \mathbb{Z}$.

$dab' = ab = da'b$ par définition de a' et b'. Il suit que $d(ab' - a'b) = 0$ donc $ab' = a'b$ car $d \neq 0$.

Alors $ax + by = a(u + kb') + b(v - ka') = au + bv + k(ab' - a'b) = au + bv = d$.

On en conclut que (x, y) est bien solution. (CQFD)

2.4.3 Problème dérivé

Soient a, b et c des entiers avec a **et** b **non nuls**.
Résoudre dans $\mathbb{Z}$ l'équation $ax \equiv c[b]$.

On remarque que l'entier x est solution de $ax \equiv c[b]$ si et seulement il existe un entier y tel que $ax = c - by$, c.a.d. $ax + by = c$.

La méthode de résolution en découle directement.

2.4.4 Méthode

Etape 1 : calculer $pgcd(a, b)$.

Si c **n'est pas un multiple** de $\text{pgcd}(a, b)$, l'équation $ax \equiv c[b]$ n'a **pas de solution**.

Etape 2 : si c est un **multiple** de $\text{pgcd}(a, b)$, l'équation $ax \equiv c[b]$ admet des solutions et on recherche une **solution particulière**.

On note $d := \text{pgcd}(a, b)$. On calcule le quotient de c par d que l'on note m.
L'algorithme d'Euclide étendu appliqué à a et b fournit des entiers u et v tels que $au + bv = d$.
Une solution particulière de l'équation $ax \equiv c[b]$ est $x_0 = mu$.

Etape 3 : si c est un multiple de $\text{pgcd}(a, b)$, on recherche **toutes les solutions** de l'équation $ax \equiv c[b]$.

On note $d := \text{pgcd}(a, b)$ et x_0 la solution particulière déterminée à l'étape 2.
On calcule b' le quotient de b par d.
L'ensemble des solutions est $S = \{x_0 + kb' \mid k \in \mathbb{Z}\}$.

3 Nombres premiers

3.2 Définition et propriétés

Définition

On appelle nombre premier tout entier $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.

Exemples : Les nombres premiers inférieurs à 100 sont :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Propriété

Soient n un entier et p un nombre premier, alors ou bien p divise n ou bien p et n sont premiers entre eux.

Démonstration
Notons $d := \text{pgcd}(n, p)$, alors d est un diviseur de p et par définition d'un nombre premier, ou bien $d = p$ et donc p est un diviseur de n, ou bien $d = 1$ et p est premier avec n.

Propriété

Tout entier $n \geqslant 2$ a au moins un facteur premier.

Démonstration
Soit $n \geqslant 2$.
n admet au moins un diviseur supérieur ou égal à 2, c'est lui-même.
Notons p le plus petit diviseur de n supérieur ou égal à 2.
Soit d un diviseur positif de p, alors d divise a fortiori n. Remarquons que $d \neq 0$ car $n \neq 0$.
Si $d \neq 1$ alors $d \geqslant 2$ et par définition de p, $d \geqslant p$. (1)
Mais on sait aussi que d divise p et $p > 0$ implique $d \leqslant p$. (2)
(1) et (2) impliquent $d = p$.
On a montré que les seuls diviseurs de p sont 1 et p donc p est premier. (CQFD)

Lemme d'Euclide

Soient a et b des entiers et p un nombre premier.
Si p divise ab, alors p divise a ou p divise b.

Démonstration
Supposons que p ne divise pas a, alors, comme p est premier, a et p sont premiers entre eux, et d'après le théorème de Gauss, p divise ab implique p divise b.

Contraposée du lemme d'Euclide

Soient a et b des entiers et p un nombre premier.
Si p ne divise pas a et p ne divise pas b alors p ne divise pas ab.

Décomposition en facteurs premiers

Soit $n \geqslant 2$ un entier, il existe un unique entier $r \geqslant 1$ et des nombres premiers $p_1 \leqslant \cdots \leqslant p_r$ uniques tels que $n = p_1 \dots p_r$.

Démonstration

- **Existence** : démonstration par récurrence de la propriété P_n :
"pour tout entier $k \in [\![2, n]\!]$, il existe une décomposition en facteurs premiers".

  Initialisation : pour $n = 2$, il existe une décomposition triviale en facteur premier qui est $n = 2$.

  Hérédité : soit $n \geqslant 2$ un entier, supposons l'existence de la décomposition pour les entiers de 2 à n.
  D'après une propriété précédente, $n + 1 \geqslant 3$ admet au moins un diviseur premier que l'on note p.
  Notons n' le quotient de $n + 1$ par p, remarquons que $n' > 0$ car $n + 1 > 0$ et $p > 0$.
  Comme $p \geqslant 2$ (par définition d'un nombre premier), on a $n + 1 = pn' \geqslant 2n' = n' + n' > n'$.
  Il suit que $n' < n + 1$ et que l'on peut appliquer l'hypothèse de récurrence à n'.
  Par suite il existe s et $q_1 \leqslant \cdots \leqslant q_s$ tels que $n' = q_1 \dots q_s$.
  Il suit que $n + 1 = p\, q_1 \dots q_s$.
  On pose $r := s + 1$, puis en classant p dans la liste de nombres triés $q_1 \leqslant \cdots \leqslant q_s$, on obtient un liste de nombre $p_1 \leqslant \cdots \leqslant p_r$ telle que $n + 1 = p_1 \dots p_r$. (CQFD)

- **Unicité** : on montre également par récurrence la propriété Q_n :
"pour tout entier $k \in [\![2, n]\!]$, la décomposition en facteurs premiers est unique".

  Initialisation : pour $n = 2$. Soit p un diviseur premier de 2, $p \leqslant 2$ par propriété des diviseurs d'un nombre strictement positifs. Mais par définition d'un nombre premier, $p \geqslant 2$ donc $p = 2$.
  Donc une décomposition en facteurs premiers de 2 s'écrit 2^r avec $r \geqslant 1$. Mais $r > 1$ implique $2^r > 2$ donc nécessairement $r = 1$.
  On a montré que l'unique décomposition de 2 en produits de facteurs premiers est 2.

  Hérédité : soit $n \geqslant 2$ un entier, supposons que Q_n est vraie et considérons $n + 1$.
  Notons $p_1 \leqslant \cdots \leqslant p_r$ et $q_1 \leqslant \cdots \leqslant q_s$ deux décompositions de $n + 1$ et montrons qu'elles sont nécessairement égales.

  Supposons par l'absurde que $p_1 < q_1$, alors pour tout $i \in [\![1, s]\!]$, $p_1 < q_1 \leqslant q_i$. Comme on a aussi $p_1 > 1$ (par définition d'un nombre premier), p_1 ne divise pas q_i car les seuls diviseurs de q_i sont 1 et lui-même (par définition d'un nombre premier).
  Il suit, d'après la contraposée du lemme d'Euclide, que p_1 ne divise pas le produit $q_1 \dots q_s = n + 1$ ce qui est contradictoire avec l'écriture $n + 1 = p_1 \dots p_r$.

  De même si on suppose $q_1 < p_1$, on obtient la contradiction que q_1 ne divise pas $n + 1$.

  Il suit que $p_1 = q_1$. Notons n' le quotient de $n+1$ par p_1, remarquons que $n' > 0$ car $n+1 > 0$ et $p_1 > 0$.
  Si $n' = 1$ alors nécessairement $r = s = 1$, les deux décompositions sont donc p_1 et q_1 et on vient de montrer qu'elles sont identiques.
  Si $n' \geqslant 2$, alors nécessairement $r \geqslant 2$, $s \geqslant 2$ et $n' = p_2 \dots p_r = q_2 \dots q_s$.
  $p_1 \geqslant 2$ (par définition d'un nombre premier) implique $n + 1 = p_1 n' \geqslant 2n' = n' + n' > n'$.
  On a donc $n' < n + 1$ et on peut appliquer l'hypothèse de récurrence à n'.
  Il suit que la décomposition de n' est unique, c.a.d. que $r = s$ et pour tout $i \in [\![2, r]\!]$, $p_i = q_i$.
  On en conclut que les deux décompositions $n+1 = p_1 \dots p_r$ et $n+1 = q_1 \dots q_s$ sont identiques. (CQFD)

Chapitre III

Nombres complexes

1 Ecriture (ou forme) algébrique

1.2 Parties réelles et imaginaires

Propriété

Soit z un nombre complexe, z s'écrit de manière unique sous la forme $a + ib$ où a et b sont des réels. Cette écriture s'appelle écriture algébrique de z. On appelle partie réelle de z notée $\mathrm{Re}(z)$ le réel a et partie imaginaire de z notée $\mathrm{Im}(z)$ le réel b.

Corollaire 1

Si a, b, c et d sont des réels, $a + ib = c + id \Leftrightarrow (a = c)$ et $(b = d)$. On dit que l'on peut identifier les parties réelles et imaginaires.

Corollaire 2

Pour tous réels x et y, $x + iy = 0 \Leftrightarrow x = 0$ et $y = 0$

1.3 Règles de calcul

Propriété : addition et multiplication

Soient z et z' quelconques dans $\mathbb{C}$, $a + ib$ et $c + id$ leurs écritures algébriques :

- $z + z' = (a + ib) + (c + id) = (a + c) + i(b + d)$
- $zz' = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$
- Si $z \neq 0$, $\dfrac{1}{z} = \dfrac{a}{a^2 + b^2} - i\dfrac{b}{a^2 + b^2}$

Propriété : linéarité des parties réelles et imaginaires

Soient z et z' quelconques dans $\mathbb{C}$, λ quelconque dans $\mathbb{R}$:

- $\mathrm{Re}(z + z') = \mathrm{Re}(z) + \mathrm{Re}(z')$
- $\mathrm{Im}(z + z') = \mathrm{Im}(z) + \mathrm{Im}(z')$
- $\mathrm{Re}(\lambda z) = \lambda\,\mathrm{Re}(z)$
- $\mathrm{Im}(\lambda z) = \lambda\,\mathrm{Im}(z)$

1.4 Réels et imaginaires purs

Définition

Tout nombre complexe de la forme $z = ib$ avec b **réel** est appelé imaginaire pur.
L'ensemble des imaginaires purs est noté $i\mathbb{R}$.

Propriété

Pour tout nombre complexe z, on a
- z est réel si et seulement si $\text{Im}(z) = 0$,
- z est imaginaire pur si et seulement si $\text{Re}(z) = 0$.

2 Représentation géométrique des nombres complexes

2.2 Affixe

Dans cette sous-section, on se place dans un plan affine P muni d'un repère orthonormé direct $(O, \vec{u}, \vec{v})$.

Définition et propriété

On associe à tout nombre complexe z d'écriture algébrique $a + ib$ le point M de coordonnées (a, b) dans le repère $(O, \vec{u}, \vec{v})$. z détermine M de manière unique et inversement.
Le nombre z est appelée **affixe** du point M et du vecteur $\overrightarrow{OM}$. Sa partie réelle est l'abscisse de M dans le repère $(O, \vec{u}, \vec{v})$ et sa partie imaginaire l'ordonnée.

Notation : $M(z)$, $\overrightarrow{OM}(z)$

Faire un schéma.

Propriété

- Soit deux points $M(z)$ et $M'(z')$, l'affixe du vecteur $\overrightarrow{MM'}$ est $z' - z$,
- Soit deux vecteurs $\overrightarrow{w}(z)$ et $\overrightarrow{w'}(z')$, l'affixe du vecteur $\overrightarrow{w} + \overrightarrow{w'}$ est $z + z'$,
- Soit un réel k et un vecteur $\overrightarrow{w}(z)$, l'affixe du vecteur $k.\overrightarrow{w}$ est kz,
- Soit deux vecteurs $\overrightarrow{w}(z)$ et $\overrightarrow{w'}(z')$, $\overrightarrow{w} = \overrightarrow{w'} \Leftrightarrow z = z'$.

2.3 Plan complexe

Pour simplifier cette représentation géométrique, on peut ne représenter que les affixes, sans les points ou les vecteurs. On fait alors abstraction du plan affine pour ne s'intéresser qu'aux nombres complexes. On parle de **plan complexe**. C'est la représentation géométrique habituelle des nombres complexes.

Représentation : avec module et argument, droites des réels et des imaginaires purs

3 Conjugué

3.2 Définition

Soit z un nombre complexe d'écriture algébrique $a + ib$ (a et b réels), on appelle conjugué de z et on note $\bar{z}$ le nombre $a - ib$.

Interprétation géométrique
Dans le plan complexe, $\bar{z}$ est le symétrique de z par rapport à la droite des réels.

3.3 Règles de calcul

Propriété

Soient z et z' quelconques dans $\mathbb{C}$, on a :
- $\overline{\overline{z}} = z$ (la conjugaison est une involution),
- $\overline{z+z'} = \overline{z} + \overline{z'}$ (compatibilité de la conjugaison avec l'addition),
- $\overline{zz'} = \overline{z}\,\overline{z'}$ (compatibilité de la conjugaison avec la multiplication),
- Si $z \neq 0$, $\overline{(1/z)} = 1/\overline{z}$ (compatibilité de la conjugaison avec l'inverse, conséquence de la propriété précédente).

Propriété importante

- $\mathrm{Re}(z) = \dfrac{1}{2}(z + \overline{z})$
- $\mathrm{Im}(z) = \dfrac{1}{2i}(z - \overline{z})$

3.4 Caractérisation des réels et imaginaires purs

Propriété

Soit z quelconque dans $\mathbb{C}$, on a :
$z \in \mathbb{R} \Leftrightarrow z = \overline{z}$
$z \in i\mathbb{R} \Leftrightarrow z = -\overline{z}$

4 Module

4.2 Définition

Soit z un nombre complexe d'écriture algébrique $a + ib$ (a et b réels), on appelle **module** de z et on note $|z|$ le réel positif $\sqrt{a^2 + b^2}$.

Module et valeur absolue
Si $z \in \mathbb{R}$, son module est égale à la valeur absolue définie pour les nombres réels, d'où le choix d'une même notation. On dit que le module des nombres complexes prolonge la valeur absolue des réels.

Interprétation géométrique
Soit $M(z)$ et $M'(z')$ dans un plan affine muni d'un repère orthonormé $(O, \vec{u}, \vec{v})$, $OM = |z|$ et $MM' = |z' - z|$.

4.3 Règles de calcul

Dans cette sous-section, z et z' sont des nombres complexes quelconques.

Propriété

- $|\overline{z}| = |z|$ (le module est invariant par conjugaison),
- $|zz'| = |z||z'|$ (compatibilité du module avec la multiplication),
- Si $z \neq 0$, $|1/z| = 1/|z|$ (compatibilité du module avec l'inverse, conséquence de la propriété précédente).

Propriétés importantes

- $|z| = 0 \quad \Leftrightarrow \quad z = 0$
- $|z|^2 = z\overline{z}$
- Si $z \neq 0$, $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$

Démonstration (utiliser la forme algébrique)

Application
Calculer l'inverse de $z = 5 - 3i$.

Propriété

Le module n'est pas compatible avec l'addition mais on a la formule :
$|z + z'|^2 = |z|^2 + 2\,\mathrm{Re}(z'\overline{z}) + |z'|^2$

Démonstration (utiliser le conjugué)

Application
Calculer $\left|e^{i\theta} + 3e^{i2\theta}\right|$ où θ est un réel quelconque.

4.4 Nombres complexes de module 1

Définition

On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1.

Remarque : dans le plan complexe, $\mathbb{U}$ est le cercle de centre 0 et de rayon 1.

Propriété

Soient z et z' des nombres complexes de **module 1** :
- $\overline{z}$ est de module 1 ($\mathbb{U}$ est stable pour la conjugaison),
- zz' est de module 1 ($\mathbb{U}$ est stable pour la multiplication),
- $\dfrac{1}{z}$ est de module 1 ($\mathbb{U}$ est stable pour l'inverse).

Représentation graphique

Propriété

L'égalité entre inverse et conjugué caractérise les éléments de $\mathbb{U}$, c.a.d.
pour tout $z \in \mathbb{C}^*$, $|z| = 1 \quad \Leftrightarrow \quad \dfrac{1}{z} = \overline{z}$

Démonstration

4.5 Inégalité triangulaire

Propriété

Pour tout z et z' dans $\mathbb{C}$, $|z + z'| \leqslant |z| + |z'|$

Interprétation géométrique
schéma

Démonstration
Lemme : Pour tout $z \in \mathbb{C}$, on a $|Re(z)| \leqslant |z|$ et $|Im(z)| \leqslant |z|$

Puis utiliser $|z + z'|^2 = |z|^2 + 2\,Re(z'\overline{z}) + |z'|^2$

Corollaire utile

Pour tout z et z' dans $\mathbb{C}$, $||z| - |z'|| \leqslant |z - z'|$

Démonstration (écrire z=(z-z')+z)

5 Argument

Dans cette section, on se place dans un plan affine P muni d'un repère orthonormé direct $(O, \vec{u}, \vec{v})$.

5.2 Définition

Définition : congruence

Soit x, y et m des réels, on dit que a est congru à b modulo m et on note $a \equiv b\,[m]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $a = b + k\,m$.

Remarque : la notation $a = b\,[m]$ est acceptée.

Définition : argument

Soit z un nombre complexe **non nul**, on considère le point $M(z)$ dans le repère $(O, \vec{u}, \vec{v})$. On appelle argument de z et on note $\arg z$ toute mesure de l'angle $(\vec{u}, \overrightarrow{OM})$.
On appelle argument principal la mesure de cet angle qui appartient à $[0, 2\pi[$ (d'autres définitions utilisent l'intervalle $]-\pi, \pi]$).

Schéma

Remarque : l'argument est donc défini à $2k\pi$ près avec $k \in \mathbb{Z}$.
Par exemple, on écrit $\arg(1+i) = \dfrac{\pi}{4} + 2k\pi$ avec $k \in \mathbb{Z}$
ou bien $\arg(1+i) \equiv \dfrac{\pi}{4}[2\pi]$ (congru à ... modulo ...)

Propriété

Soient deux points $M(z)$ et $M'(z')$ dans le repère $(O, \vec{u}, \vec{v})$, $\quad (\vec{u}, \overrightarrow{MM'}) \equiv \arg(z' - z)[2\pi]$.

Propriété

Soient $z \in \mathbb{C}^*$ et θ un argument de z, $\quad \cos\theta = \dfrac{\mathrm{Re}(z)}{|z|} \quad$ et $\quad \sin\theta = \dfrac{\mathrm{Im}(z)}{|z|}$.

5.3 Règles de calcul

Propriété

Pour tous nombres complexes z et z' non nuls, on a :
- $\arg(-z) \equiv \pi + \arg z[2\pi]$
- $\arg(zz') \equiv \arg z + \arg z'[2\pi]$
- $\arg(\frac{1}{z}) \equiv -\arg z[2\pi]$
- $\arg(\overline{z}) \equiv -\arg z[2\pi]$

Application : Soit $z \in \mathbb{C}^*$ et $n \in \mathbb{N}$, calculer $\arg(z^n)$ à partir de $\arg z$.

6 Rappel de trigonométrie

6.2 Formules d'addition

Propriété

Pour tous réels θ et θ' :
- $\cos(\theta + \theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta'$.
- $\sin(\theta + \theta') = \cos\theta\sin\theta' + \sin\theta\cos\theta'$.

Démonstration

- **Formule d'addition des cosinus**.
  Soient θ et θ' des réels. On pose $\theta'' = -\theta'$.
  Dans un plan P muni d'un repère orthonormé direct $(O, \vec{u}, \vec{v})$, on considère les points $M(\cos\theta + i\sin\theta)$ et $M''(\cos\theta'' + i\sin\theta'')$ situés sur le cercle unité.
  $\overrightarrow{OM}.\overrightarrow{OM''} = \cos\theta\cos\theta'' + \sin\theta\sin\theta''$.
  Par ailleurs l'angle $(\overrightarrow{OM}, \overrightarrow{OM''})$ admet pour mesure $\theta'' - \theta$.
  On a donc $\overrightarrow{OM}.\overrightarrow{OM''} = \cos(\theta'' - \theta)$.
  On en conclut que $\cos(\theta - \theta'') = \cos(\theta'' - \theta) = \cos\theta\cos\theta'' + \sin\theta\sin\theta''$ qui s'écrit aussi $\cos(\theta + \theta') = \cos\theta\cos(-\theta') + \sin\theta\sin(-\theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta'$ (CQFD).
- **Formule d'addition des sinus**.
  Soient θ et θ' des réels.
  On sait que $\forall x \in \mathbb{R}$, $\sin x = \cos(\pi/2 - x)$ et $\cos x = \sin(\pi/2 - x)$.
  Donc $\sin(\theta + \theta') = \cos\big(\pi/2 - (\theta + \theta')\big) = \cos\big((\pi/2 - \theta) - \theta'\big)$.
  Or d'après la formule d'addition des cosinus, $\cos\big((\pi/2 - \theta) - \theta'\big) = \cos(\pi/2 - \theta)\cos\theta' + \sin(\pi/2 - \theta)\sin\theta'$.
  Donc $\sin(\theta + \theta') = \sin\theta\cos\theta' + \cos\theta\sin\theta'$ (CQFD).

6.3 Formules de duplication

Propriété

Pour tout réel θ :
- $\cos(2\theta) = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta$.
- $\sin(2\theta) = 2\cos\theta\sin\theta$.

Corollaire : linéarisation du carré

Pour tout réel θ :
- $\cos^2\theta = \dfrac{1 + \cos(2\theta)}{2}$.
- $\sin^2\theta = \dfrac{1 - \cos(2\theta)}{2}$.

7 Ecriture trigonométrique (ou polaire)

7.2 Définition

Théorème

Soit z un nombre complexe **non nul**. En notant θ un argument de z et $r = |z|$, on a $z = r(\cos\theta + i\sin\theta)$.
Cette forme est appelée écriture trigonométrique (ou polaire) de z.
Dans cette écriture, r est un réel **positif** et est unique, θ est un réel déterminé à $2k\pi$ près ($k \in \mathbb{Z}$).

Remarque : attention à vérifier que r est positif.

7.3 Fonction exponentielle complexe

Définition et propriété

$$\text{La fonction } f : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & e^a(\cos b + i\sin b) \end{array} \quad \text{où } a + ib \text{ est l'écriture algébrique de } z$$

est un prolongement de la fonction exponentielle à variable réelle.
Elle est appelée fonction exponentielle complexe et notée e^z.

Propriété fondamentale

$\forall z, z' \in \mathbb{C}, \quad e^{z+z'} = e^z\, e^{z'}$.

Corollaire

- $\forall z \in \mathbb{C}$, $e^{-z} = (e^z)^{-1}$.
- $\forall z \in \mathbb{C}$, $\forall p \in \mathbb{Z}$, $e^{pz} = (e^z)^p$.

Corollaire : dans le cas particulier des imaginaires purs.

- $\forall \theta, \theta' \in \mathbb{R}$, $e^{i(\theta+\theta')} = e^{i\theta}\, e^{i\theta'}$,
- $\forall \theta \in \mathbb{R}$, $\forall p \in \mathbb{Z}$, $e^{ip\theta} = \left(e^{i\theta}\right)^p$.

Propriété fondamentale

Pour tout réel θ, $\quad \overline{e^{i\theta}} = e^{-i\theta} = \dfrac{1}{e^{i\theta}}$.

7.4 Notation exponentielle de la forme trigonométrique

Propriété

Soit $z \in \mathbb{C}^*$, en notant θ un argument de z et $r = |z|$, z peut s'écrire en notation exponentielle $z = re^{i\theta}$.

Remarque : c'est l'écriture couramment utilisée pour la forme trigonométrique.

7.5 Formules d'Euler

Propriété

Pour tout $\theta \in \mathbb{R}$,

- $\cos\theta = \dfrac{e^{i\theta} + e^{-i\theta}}{2}$
- $\sin\theta = \dfrac{e^{i\theta} - e^{-i\theta}}{2i}$

7.6 Formule de Moivre

Propriété

Pour tous réel θ et entier n, on a $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$

7.7 Interprétation géométrique des opérations sur les nombres complexes

Propriété

Dans le plan complexe :

- L'application $z \to z + t$ avec $t \in \mathbb{C}$ est la translation de vecteur $\vec{v}(t)$.
- L'application $z \to \overline{z}$ est la symétrie axiale d'axe la droite des réels.
- L'application $z \to -z$ est la symétrie centrale de centre 0.
- L'application $z \to -\overline{z}$ est la symétrie axiale d'axe la droite des imaginaires purs.
- L'application $z \to k.z$ avec $k \in \mathbb{R}$ est une homothétie de centre 0 et de rapport k.
- L'application $z \to e^{i\theta}.z$ avec $\theta \in \mathbb{R}$ est une rotation de centre 0 et d'angle θ.

Exemple :
Interpréter géométriquement l'application $z \mapsto az + b$ où a et b sont des réels.

8 Trigonométrie

8.2 Formule du binôme de Newton

Propriété

Pour tous réels a, b et tout entier n, $\quad (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}\, b^k$.

Rappel : triangle de Pascal

Soient n et m des entiers naturels tels $n > m > 0$, on a la relation de récurrence suivante :

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

8.3 Expression de $\cos n\theta$ et $\sin n\theta$ en fonction de $\cos\theta$ et $\sin\theta$

Méthode sur un exemple
Exprimer $\cos 4\theta$ et $\sin 4\theta$ en fonction de $\cos\theta$ et $\sin\theta$.

D'après la formule de Moivre : $\cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n$.
On utilise la formule du binôme de Newton pour développer le second membre puis on regroupe les parties réelles et imaginaires.
On peut alors identifier ces dernières avec $\cos n\theta$ *et* $\sin n\theta$.

8.4 Linéarisation de $(\cos\theta)^n$ et $(\sin\theta)^n$

Linéariser $\approx$ *transformer un produit en une somme*

Rappel

Soit θ un réel et n un entier naturel, on a $\cos\theta = \dfrac{e^{i\theta} + e^{-i\theta}}{2}$ et $\sin\theta = \dfrac{e^{i\theta} - e^{-i\theta}}{2i}$

Méthode sur un exemple
Linéariser $(\cos\theta)^3$ et $(\sin\theta)^3$.

On utilise l'une ou l'autre des formules précédentes selon que l'on veut linéariser un cosinus ou un sinus. On a par exemple pour le cosinus :

$$\cos^n\theta = \left(\frac{e^{i\theta} + e^{-i\theta}}{2}\right)^n = \frac{1}{2^n}(e^{i\theta} + e^{-i\theta})^n$$

On utilise la formule du binôme de Newton pour développer $(e^{i\theta} + e^{-i\theta})^n$ *puis on regroupe les termes en* $e^{ik\theta}$ *et* $e^{-ik\theta}$.
On peut alors simplifier en utilisant $e^{ik\theta} + e^{-ik\theta} = 2\cos(k\theta)$ *et* $e^{ik\theta} - e^{-ik\theta} = 2i\sin(k\theta)$.
Puis on obtient la linéarisation de $(\cos\theta)^n$ *en multipliant le résultat par* $\dfrac{1}{2^n}$. *S'il n'y a pas d'erreurs de calcul, on doit obtenir un nombre réel.*

9 Racines carrées d'un nombre complexe

9.2 Ecriture algébrique des racines carrées d'un nombre complexe

Propriété

Tout nombre complexe z possède deux racines carrées opposées, distinctes si $z \neq 0$.

Attention : La notation racine carrée n'a pas de sens pour les nombres complexes car elle doit désigner un nombre de manière univoque.

NB : absence d'ordre compatible avec les opérations sur $\mathbb{C}$.

Méthode de calcul générale

Soit z un nombre complexe de forme algébrique $a+ib$ (a et b réels). Pour tous x et y réels, on a l'équivalence :

$$(x+iy)^2 = a+bi \Leftrightarrow \left\{ \begin{array}{l} x^2-y^2=a \\ 2xy=b \end{array} \right.$$

De plus : $(x+iy)^2 = a+bi \Rightarrow x^2+y^2 = \sqrt{a^2+b^2}$ (égalité des modules).

Nous avons donc a fortiori l'équivalence :

$$(x+iy)^2 = a+bi \Leftrightarrow \left\{ \begin{array}{l} x^2-y^2=a \\ 2xy=b \\ x^2+y^2=\sqrt{a^2+b^2} \end{array} \right.$$

et en faisant la somme et la différence de la première et de la troisième égalité, on obtient :

$$(x+iy)^2 = a+bi \Leftrightarrow \left\{ \begin{array}{l} 2x^2=\sqrt{a^2+b^2}+a \\ 2y^2=\sqrt{a^2+b^2}-a \\ 2xy=b \end{array} \right.$$

Puisqu'on a $b^2 \geq 0$, les nombres réels $\sqrt{a^2+b^2}+a$ et $\sqrt{a^2+b^2}-a$ sont positifs, donc il vient :

$$|x| = \frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}+a} \quad \text{et} \quad |y| = \frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}-a}$$

Enfin, l'égalité $2xy=b$ implique que xy a le signe de b.

On obtient donc deux solutions possibles pour le couple (x,y), c'est-à-dire deux racines carrées pour z.

Formellement, en notant ϵ le signe de b dans le sens où ϵ vaut -1 si $b<0$, 1 si $b=0$ (on pourrait aussi choisir -1), 1 si $b>0$, les deux racines de $z=a+ib$, sont

$$\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a}+\epsilon i\sqrt{\sqrt{a^2+b^2}-a}\right)$$

et l'opposé, c'est-à-dire

$$-\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a}+\epsilon i\sqrt{\sqrt{a^2+b^2}-a}\right)$$

Exemple : Calculons les racines carrées du nombre complexe $3-4i$. Soit x et y réels, on a les équivalences :

$$(x+iy)^2 = 3-4i \Leftrightarrow \left\{ \begin{array}{l} x^2-y^2=3 \\ 2xy=-4 \\ x^2+y^2=5 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} x^2=4 \\ y^2=1 \\ xy=-2 \end{array} \right. \Leftrightarrow x+iy=2-i \text{ ou } x+iy=-2+i$$

Les racines carrées de $3-4i$ sont donc $2-i$ et $-2+i$.

9.3 Equations du second degré à coefficients complexes

Propriété

Soient $a \neq 0$, b et c des nombres complexes et E l'équation $a\,z^2 + b\,z + c = 0$ d'inconnue complexe z.
On appelle discriminant de E le nombre complexe $\Delta = b^2 - 4\,ac$.
L'équation E admet pour solutions les nombres complexes $z_1 = \dfrac{-b + \delta_1}{2a}$ et $z_2 = \dfrac{-b + \delta_2}{2a}$ où δ_1 et $\delta_2 = -\delta_1$ sont les racines carrées de Δ.
Si $\Delta = 0$, ces deux solutions sont confondues, on dit que E admet une solution double.

Application :
Calculer les solutions de l'équation $z^2 - (2+3i)z - 2 + 4i = 0$.
Discriminant $3 - 4i$*, racines* $2 + i$ *et* $2i$.

10 Racines n-ièmes d'un nombre complexe

10.2 Définition

Soit Z un nombre complexe et un n un entier naturel non nul, on appelle racine n-ième de Z tout nombre complexe z vérifiant $z^n = Z$.

Cas particuliers :
- Pour $n = 2$, on parle des racines carrées.
- Pour $Z = 1$, on parle des racines n-ièmes de l'unité.

10.3 Existence et nombre de racines n-ièmes

Propriété

Soit $n \in \mathbb{N}^*$, toute suite géométrique de raison $e^{i\frac{2\pi}{n}}$ est une suite périodique de période n qui prend n valeurs distinctes.

Démonstration :
On note u_0 le premier terme de la suite.

Soit $k \in \mathbb{N}$, on a $u_k = \left(e^{i\frac{2\pi}{n}}\right)^k u_0 = e^{i\frac{2k\pi}{n}} u_0$.

Donc $u_{k+n} = \left(e^{i\frac{2\pi}{n}}\right)^n u_k = e^{i\frac{2n\pi}{n}} u_k = u_k$.

De plus, les nombres u_0, u_1, …, u_{n-1} sont distincts deux à deux.

Supposons qu'il existe $k, k' \in [0, n-1]$ tels que $u_k = u_{k'}$, on a alors $u_0 e^{i\frac{2k\pi}{n}} = u_0 e^{i\frac{2k'\pi}{n}}$ donc $e^{i2\pi\frac{k-k'}{n}} = 1$ qui implique que $\frac{k-k'}{n}$ est un entier c'est-à-dire $k - k'$ est un multiple de n.

De plus $0 \leqslant k \leqslant n-1$ et $-(n-1) \leqslant -k' \leqslant 0$ implique $-(n-1) \leqslant k - k' \leqslant n-1$.

Comme le seul multiple de n de l'intervalle $[-(n-1), n-1]$ est 0, on en conclut que $k = k'$ (CQFD).

Propriété

Soit n un entier naturel non nul, tout nombre complexe non nul possède n racines n-ièmes **distinctes**.

Démonstration :
Soit Z un nombre complexe non nul et $re^{i\theta}$ sa forme polaire. r est un réel positif donc $\sqrt[n]{r}$ est défini.
On pose, pour tout $k \in \mathbb{N}$, $z_k = \sqrt[n]{r}\; e^{i(\frac{\theta+2k\pi}{n})}$.

Soit $k \in \mathbb{N}$, on a $z_k^n = (\sqrt[n]{r})^n \left(e^{i(\frac{\theta+2k\pi}{n})}\right)^n = r\, e^{i(\theta+2k\pi)} = r\, e^{i\theta} = Z$.
Donc z_k est racine n-ième de z.

Inversement, soit z une racine n-ième de Z. On a $z^n = Z$ donc $|z^n| = Z$ et $\arg z^n = Z$ c'est-à-dire $|z| = \sqrt[n]{r}$ et $\arg z \equiv \frac{\theta}{n}\ [\frac{2\pi}{n}]$. On en conclut que z est un des termes de la suite $(z_k)_{k\in\mathbb{N}}$.

Donc l'ensemble des racines n-ièmes est exactement l'ensemble des nombres z_k.

De plus, la suite $(z_k)_{k\in\mathbb{N}}$ est une suite géométrique de raison $e^{i\frac{2\pi}{n}}$, donc elle est périodique de période n et prend n valeurs distinctes (CQFD).

10.4 Méthode de calcul

Propriété

Soient n un entier naturel non nul et Z un nombre complexe non nul de forme polaire $re^{i\theta}$, les n racines n-ième de Z sont les n termes successifs d'une suite géométrique de premier terme $z_0 = \sqrt[n]{r}\ e^{i\frac{\theta}{n}}$ et de raison $e^{i\frac{2\pi}{n}}$.
Cette suite est périodique de période n et ses n valeurs distinctes sont les nombres
$z_k = \sqrt[n]{r}\ e^{i(\frac{\theta+2k\pi}{n})}$ avec $k \in [0, n-1]$.

Exercice : calculer les racines carrées et cinquièmes de $16 - 16\sqrt{3}i$.

10.5 Racines n-ième de l'unité

Il s'agit des racines de 1.

Propriété

Soient n un entier naturel non nul, les n racines n-ièmes de l'unité sont les nombres $e^{i\frac{2k\pi}{n}}$ où k varie de 0 à $n-1$.

Propriété

Soient n un entier naturel non nul et Z un nombre complexe non nul dont z_0 est une racine n-ième connue, les n racines n-ièmes de Z s'obtiennent en multipliant z_0 par chacune des n racines n-ièmes de l'unité.

Démonstration : en notant $u_k = e^{i\frac{2k\pi}{n}}$ où $k \in [0, n-1]$, les racines n-ièmes de l'unité, les n nombres z_0u_k ($k \in [0, n-1]$) sont distincts deux à deux et $(z_0u_k)^n = Z$.

10.6 Interprétation géométrique

Propriété

Soient n un entier vérifiant $n \geqslant 2$ et Z un nombre complexe non nul, les n racines n-ièmes de Z sont les sommets d'un polygone régulier de centre 0 à n sommets dont le cercle circonscrit a pour rayon $\sqrt[n]{|Z|}$.

schéma

Démonstration :
Pour tout $k \in [0, n-1]$, on note A_k le sommet d'affixe $z_k = \sqrt[n]{r}\ e^{i(\frac{\theta+2k\pi}{n})}$. Si $k \neq 0$, on a $z_k = e^{i\frac{2\pi}{n}}z_{k-1}$ et $z_0 = e^{i\frac{2\pi}{n}}z_{n-1}$, donc chaque sommet est l'image du précédent par une rotation de centre 0 et d'angle $\frac{2\pi}{n}$ ce qui caractérise un polygone régulier à n sommets de centre 0.

Propriété

Soient n un entier vérifiant $n \geqslant 2$ et Z un nombre complexe non nul, la somme des n racines n-ièmes de Z est nulle.

Démonstration : Cette somme est l'affixe de l'isobarycentre des points dont les affixes sont les racines de z. Or ces points sont les sommets d'un polygone régulier de centre O d'affixe 0, et le centre d'un polygone régulier est l'isobarycentre de ses sommets.

Chapitre IV

Transformations du plan

Dans tout ce chapitre, on se place dans **un plan P muni d'un repère orthonormé direct $\mathcal{R}$.**

1 Généralités

Définition

On appelle transformation du plan P, toute application $T : P \to P$.
On appelle transformation du plan complexe, toute application $f : \mathbb{C} \to \mathbb{C}$.

Propriété : écriture complexe d'une transformation, transformation complexe associée

Soit T une transformation de P, on appelle **écriture complexe** de T dans le repère $\mathcal{R}$, **ou bien transformation complexe associée** à T dans le repère $\mathcal{R}$, l'application f définie par :

$$\begin{array}{rccl} f: & \mathbb{C} & \to & \mathbb{C} \\ & z & \mapsto & z', \text{ tel que } M'(z') = T\left(M(z)\right) \text{ dans le repère } \mathcal{R} \end{array}$$

On retiendra : Soit f l'écriture complexe de T (ou bien la transformation complexe associée à T),

Pour tous points $M(z)$ et $M'(z')$, $\quad M' = T(M) \Leftrightarrow z' = f(z)$.

NB : dans la suite de ce chapitre, on utilisera le terme **transformation** à la place de **transformation du plan** P.

Remarques :

- On peut définir une transformation par son écriture complexe.
- L'identité du plan, notée Id_P, a pour écriture complexe l'identité de $\mathbb{C}$, notée $Id_{\mathbb{C}}$.

Propriété : écriture complexe d'une composée

Soit T, T' des transformations et f, f' les transformations complexes associées, $f \circ f'$ est la transformation complexe associée à $T \circ T'$.

Démonstration :
Soient $M(z)$ et $M''(z'')$ des points, on note $M'(z') = T'(M)$, on a $z' = f'(z)$.
$M'' = T \circ T'(M) \Leftrightarrow M'' = T(M') \Leftrightarrow z'' = f(z') \Leftrightarrow z'' = f(f'(z)) = f \circ f'(z)$. (CQFD)

Propriété : transformation bijective

Soit T une transformation et f la transformation complexe associée, T est bijective si et seulement si f est bijective. Alors f^{-1} est la transformation complexe associée à T^{-1}.

Démonstration du même type que précédemment

Définition : isométrie

Soit T une transformation d'écriture complexe f, T est une isométrie si et seulement si elle conserve les distances, c'est-à-dire $\forall M, M' \in P, \| \overrightarrow{T(M)T(M')} \| = \| \overrightarrow{MM'} \|$.
Cette propriété s'écrit sous forme complexe : $\forall z, z' \in \mathbb{C}, |f(z') - f(z)| = |z' - z|$
c'est-à-dire f est une isométrie du plan complexe.

Théorème

Toute isométrie est bijective.

La surjectivité est admise.

Définitions

Soit T une transformation d'écriture complexe f

- M est un **point invariant** de T si et seulement si $T(M) = M$.
- E est **stable** par T si et seulement si $T(E) \subset E$.
- E est **globalement invariante** par T si et seulement si $T(E) = E$.

Remarques :

- On peut encore transposer la définition dans le plan complexe.
- E peut être globalement invariant sans contenir de point invariant (cf. cas des translations).

2 Translations

Définition et propriété

Soit $\vec{u}(b)$ un vecteur d'affixe a, on appelle translation de vecteur $\vec{u}$ la transformation qui à tout point M associe l'unique point M' tel que $\overrightarrow{MM'} = \vec{u}$.
Son écriture complexe est $t_b(z) = z + b$.
t_b est une translation du plan complexe de vecteur b.

Notation : on notera $T_{\vec{u}}$ la translation de vecteur $\vec{u}$.

Remarque : $T_{\vec{0}}$ est l'identité du plan.

Propriété : caractérisation des translations

Soient T une transformation de P d'écriture complexe f.
T est une translation si et seulement si $\forall M_1, M_2 \in P,\ \overrightarrow{T(M_1)T(M_2)} = \overrightarrow{M_1M_2}$;
autrement dit, f est une translation si et seulement si $\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = z_2 - z_1$.

Propriété

Toute translation est une isométrie, donc une bijection.

Propriété

La composée de deux translations est une translation.
Plus précisément, soient $\vec{u}(b)$ et $\vec{v}(c)$ deux vecteurs, $T_{\vec{u}} \circ T_{\vec{v}} = T_{\vec{u}+\vec{v}}$.
Les transformations complexes associées vérifient : $t_b \circ t_c = t_{b+c}$.

Corollaire

Soient $\vec{u}(b)$ et $\vec{v}(c)$ deux vecteurs,

- Deux translations commutent : $T_{\vec{u}} \circ T_{\vec{v}} = T_{\vec{v}} \circ T_{\vec{u}}$, c.a.d. $t_b \circ t_c = t_c \circ t_b$.
- $T_{\vec{u}}^{-1} = T_{-\vec{u}}$ c.a.d. $t_b^{-1} = t_{-b}$.

Propriété : point invariant

Une translation de vecteur non nul n'admet pas de point invariant.

Propriété : droite globalement invariante

Soit $\vec{u}$ un vecteur **non nul**, une droite D est globalement invariante par la translation $T_{\vec{u}}$ si et seulement si $\vec{u}$ est un vecteur directeur de D.

Remarque : on peut encore transposer la propriété dans le plan complexe.

Démonstration

- Vérifions qu'il s'agit d'une **condition suffisante** : supposons que la droite D admet pour vecteur directeur $\vec{u}$.
  Considérons un point M quelconque de D et $M' = T_{\vec{u}}(M)$. Par définition de la translation, $\overrightarrow{MM'} = \vec{u}$, donc par définition du vecteur directeur, $M' \in D$.
- Vérifions qu'il s'agit d'une **condition nécessaire** : supposons que la droite D est globalement invariante par $T_{\vec{u}}$.
  Considérons un point M quelconque de D et $M' = T_{\vec{u}}(M)$. Par hypothèse $M' \in D$ et est distinct de M puisque $\vec{u}$ est non nul, donc $\overrightarrow{MM'} = \vec{u}$ est un vecteur directeur de D.

3 Homothéties

Définition et propriété

Soient $\Omega(\omega)$ un point, $k \neq 0$ un réel, on appelle homothétie de centre Ω et rapport k la transformation qui à tout point M associe l'unique point M' tel que $\overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$.
Son écriture complexe est $h_{\omega,k}(z) = \omega + k(z - \omega)$. $h_{\omega,k}$ est une homothétie du plan complexe de centre ω et rapport k.

Notation : on notera $H_{\Omega,k}$ l'homothétie de centre Ω et rapport k.

Remarque : toute homothétie de rapport 1 est l'identité du plan.

Définition

On appelle homothétie-translation une transformation qui est une homothétie ou une translation.

Théorème : caractérisation des homothéties-translations

Soient T une transformation d'écriture complexe f.
T (ou f) est une homothétie-translation si et seulement si f s'écrit $f(z) = az + b$ où $a \in \mathbb{R}^*$ et $b \in \mathbb{C}$.
T (ou f) est une homothétie si de plus $a = 1 \Rightarrow b = 0$.

Remarque : ne pas oublier $a \neq 0$.

Démonstration

(LHS) $\Rightarrow$ (RHS) : L'écriture complexe d'une translation est de la forme $f(z) = z + b$, c'est bien la forme $f(z) = az + b$ avec $a = 1$.
L'écriture complexe d'une homothétie de rapport a (réel non nul par définition) est de la forme $f(z) = \omega + a(z - \omega) = az + (1 - a)\omega$, c'est bien la forme $f(z) = az + b$ avec $b = (1 - a)\omega$ et a réel non nul.
De plus si $a = 1$, on a bien $b = (1 - a)\omega = 0$.

(RHS) $\Rightarrow$ (LHS) : Supposons que T est une transformation d'écriture complexe $f(z) = az + b$ avec $b \in \mathbb{C}$ et a réel non nul.
Compte tenu de ce qui précède, on distingue deux cas :

Cas $a = 1$: $f(z) = z + b$ est la translation complexe de vecteur b.
Si de plus $b = 0$, c'est l'identité qui est aussi une homothétie.

Cas $a \neq 1$: on pose $\omega = \dfrac{b}{1-a}$.
Soit $z \in \mathbb{C}$, $f(z) = az + b = \omega - \omega + a(z - \omega + \omega) + b = \omega + a(z - \omega) + b - \omega + a\omega = \omega + a(z - \omega)$
car $b - \omega + a\omega = b + (a-1)\omega = b + (a-1)\dfrac{b}{1-a} = 0$.
Donc f est l'homothétie complexe de centre ω et de rapport a.

Propriété : caractérisation des homothéties

Soient T une transformation de P d'écriture complexe f et $k \neq 1$.
T est une homothétie de rapport k si et seulement si

$$\forall M_1, M_2 \in P,\ \overrightarrow{T(M_1)T(M_2)} = k\,\overrightarrow{M_1M_2}.$$

autrement dit, f est une homothétie de rapport k si et seulement si

$$\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = k(z_2 - z_1).$$

Remarque : ne pas oublier $k \neq 1$.

Démonstration
Comme l'égalité $\overrightarrow{T(M)T(M')} = k\,\overrightarrow{MM'}$ s'écrit avec les affixes $f(z') - f(z) = k(z' - z)$, les deux formulations sont équivalentes.

On montre le résultat dans le plan complexe.

- (LHS) $\Rightarrow$ (RHS) : soit T une homothétie de centre $\Omega(\omega)$ et de rapport k.
  $\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = \big(\omega + k(z_2 - \omega)\big) - \big(\omega + k(z_1 - \omega)\big) = k(z_2 - z_1)$. (CQFD)
- (RHS) $\Rightarrow$ (LHS) : soit T une transformation dont l'écriture complexe f vérifie
  $\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = k(z_2 - z_1)$.
  Soit $z \in \mathbb{C}$, on en déduit $f(z) - f(0) = k(z - 0)$ c'est-à-dire $f(z) = kz + f(0)$.
  Comme $k \neq 1$, f est une homothétie, d'après la démonstration du théorème de caractérisation des homothéties-translations.

Remarque : une homothétie de rapport k multiplie les distances par $|k|$.

Propriété

Toute homothétie est bijective.

Propriété

La composée de deux homothéties **de même centre** est une homothétie.
Plus précisément, soient $\Omega(\omega)$ un point, k, k' des réels **non nuls**, $\quad H_{\Omega,k} \circ H_{\Omega,k'} = H_{\Omega,kk'}$.
Les transformations complexes associées vérifient : $\quad h_{\omega,k} \circ h_{\omega,k'} = h_{\omega,kk'}$.

Remarque : cette propriété ne se généralise pas si les homothéties n'ont pas le même centre.

Corollaire

Soient $\Omega(\omega)$ un point, k, k' des réels **non nuls**,

- Deux homothéties de même centre commutent : $H_{\Omega,k} \circ H_{\Omega,k'} = H_{\Omega,k'} \circ H_{\Omega,k}$.
  c.a.d. $h_{\omega,k} \circ h_{\omega,k'} = h_{\omega,k'} \circ h_{\omega,k}$.
  Remarque : faux si les homothéties n'ont pas le même centre.
- $H_{\Omega,k}^{-1} = H_{\Omega,\frac{1}{k}}$ $\quad$ c.a.d. $h_{\omega,k}^{-1} = h_{\omega,\frac{1}{k}}$.

Propriété

La composée de deux homothéties-translations est une homothétie-translation.

Démonstration
Soient T et T' des homothéties-translations d'écriture complexe $f(z) = az + b$ et $f'(z) = a'z + b'$ (a et a' sont des réels non nuls).

$f \circ f'(z) = f(a'z + b') = a(a'z + b') + b = aa'z + (ab' + b)$.
Comme $aa' \neq 0$, on retrouve bien la forme d'une homothétie translation du plan complexe.

Remarque : la formule obtenue montre que le produit n'est pas en général commutatif.

Propriété : composée de deux homothéties

Soient deux points $\Omega(\omega)$ et $\Omega'(\omega')$, k, k' des réels **non nuls**, $H_{\Omega,k} \circ H_{\Omega',k'}$ est

- Si $kk' = 1$: une translation de vecteur colinéaire à $\overrightarrow{\Omega\Omega'}$.
  Le vecteur est nul si $\Omega = \Omega'$ ou $k = k' = 1$. C'est alors l'identité qui aussi une homothétie.
- Si $kk' \neq 1$: une homothétie de rapport kk' dont le centre est sur la droite $(\Omega\Omega')$.

Démonstration
En reprenant les notations de l'énoncé, les écritures complexes de $H_{\Omega,k}$ et $H_{\Omega',k'}$ sont $f(z) = \omega + k(z - \omega) = kz + (1 - k)\omega$ et $f'(z) = k'z + (1 - k')\omega'$.
D'après la démonstration précédente, $f \circ f'(z) = kk'z + (kb' + b)$ avec $b = (1 - k)\omega$ et $b' = (1 - k')\omega'$ donc $f \circ f'(z) = kk'z + k(1 - k')\omega' + (1 - k)\omega = a''z + b''$, en posant :

$$\begin{cases} a'' = kk' \\ b'' = k(1 - k')\omega' + (1 - k)\omega \end{cases}$$

a'' est réel donc d'après la démonstration du théorème de caractérisation des homothéties-translations, on distingue deux cas :

Cas $a'' = 1$: $f \circ f'$ est une translation de vecteur
$b'' = k(1 - k')\omega' + (1 - k)\omega = (k - 1)\omega' + (1 - k)\omega = (k - 1)(\omega' - \omega)$.
$k - 1 \in \mathbb{R}$, donc le vecteur $\vec{u}(b'')$ est colinéaire à $\overrightarrow{OO'}$.
De plus $b'' = 0 \Leftrightarrow (k - 1 = 0$ ou $\omega' - \omega) \Leftrightarrow k = k' = 1$ ou $\Omega = \Omega'$ (CQFD).

Cas $a'' \neq 1$: $f \circ f'$ est une homothétie de rapport $a'' = kk'$.
Son centre est $\omega'' = \dfrac{b''}{1 - a''} = \dfrac{k(1 - k')\omega' + (1 - k)\omega}{1 - kk'}$.
En notant $\alpha' = k(1 - k')$ et $\alpha = 1 - k$, on a $\alpha' + \alpha = k(1 - k') + 1 - k = 1 - kk'$ donc $\omega'' = \dfrac{\alpha'\omega' + \alpha\omega}{\alpha' + \alpha}$.
Comme α et α' sont réels, $\Omega''(\omega'')$ est le barycentre de $(\Omega', \alpha'))$ et (Ω, α).
Par conséquent Ω'' est sur la droite $(\Omega\Omega')$.

Propriété : point invariant

Toute homothétie de rapport $k \neq 1$ n'admet pas d'autre point invariant que son centre.

Propriété : droite globalement invariante

Soient Ω un point, $k \notin \{0, 1\}$ un réel, une droite D est globalement invariante par l'homothétie $H_{\Omega,k}$ si et seulement si $\Omega \in D$.

Démonstration

- Vérifions qu'il s'agit d'une **condition suffisante** : supposons que la droite D passe par le point Ω.
  Considérons un point M quelconque de D et $M' = H_{\Omega,k}(M)$. Par définition de l'homothétie $\overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$, donc $M' \in D$.
- Vérifions qu'il s'agit d'une **condition nécessaire** : supposons que la droite D est globalement invariante par $H_{\Omega,k}$.
  Considérons un point M de D distinct de Ω et $M' = H_{\Omega,k}(M)$. Par hypothèse $M' \in D$ et est distinct de M puisque $k \neq 1$ et $M \neq \Omega$. On en déduit que $D = (MM')$. Mais par définition de l'homothétie $\Omega \in (MM')$, donc D passe par Ω.

4 Rotations

Définition et propriété

Soit $\Omega(\omega)$ un point et θ un réel, on appelle rotation de centre Ω d'angle θ la transformation de point invariant Ω qui à tout point $M \neq \Omega$ associe l'unique point M' tel que

$$\begin{cases} \Omega M = \Omega M' \\ (\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}) \equiv \theta\,[2\pi] \end{cases}$$

Son écriture complexe est $r_{\omega,\theta}(z) = \omega + e^{i\theta}(z - \omega)$.
$r_{\omega,\theta}$ est appelée rotation du plan complexe de centre ω et d'angle θ.

Notation : on notera $R_{\Omega,\theta}$ la rotation de centre Ω d'angle θ.

Justification : M' est bien unique.
En effet, considérons $M(z) \neq \Omega$, et notons $M'(z')$ un point vérifiant la définition.
Posons $Z = \dfrac{z' - \omega}{z - \omega}$, bien défini car $z \neq \omega$.
$\Omega M = \Omega M' \Leftrightarrow |z' - \omega| = |z - \omega| \Leftrightarrow |Z| = 1$.
$\overrightarrow{\Omega M}, \overrightarrow{\Omega M'} \equiv \theta\,[2\pi] \Leftrightarrow \arg Z \equiv \theta\,[2\pi]$.
donc $Z = e^{i\theta}$ c.a.d. $z' - \omega = e^{i\theta}(z - \omega)$.
Cette égalité reste vraie pour $M = \Omega$.

Conclusion : M' est unique et $R_{\Omega,\theta}$ a pour écriture complexe $f(z) = \omega + e^{i\theta}(z - \omega)$.

Remarque : toute rotation d'angle nul est l'identité du plan.

Propriété : caractérisation des rotations-translations

Soient T une transformation d'écriture complexe f.
T (ou f) est une rotation ou une translation si et seulement si f s'écrit $f(z) = az + b$ avec a complexe de module 1 et $b \in \mathbb{C}$.
T (ou f) est une rotation si de plus $a = 1 \Rightarrow b = 0$

Démonstration

(LHS) $\Rightarrow$ (RHS) : Une translation complexe a bien cette écriture avec $a = 1$ et b quelconque.
Une rotation complexe d'angle θ et de centre ω est de la forme
$f(z) = \omega + e^{i\theta}(z - \omega) = e^{i\theta}z + \omega(1 - e^{i\theta})$.
En posant $\begin{cases} a = e^{i\theta} \\ b = \omega(1 - e^{i\theta}) \end{cases}$, on peut écrire $f(z) = az + b$.
On a bien $|a| = 1$.
De plus, $a = 1$ équivaut à $\theta \equiv 0[2\pi]$ et implique $b = 0$. f est alors l'identité, c.a.d. une rotation d'angle nul.

(RHS) $\Rightarrow$ (LHS) : Soit T une transformation d'écriture complexe $f(z) = az + b$ avec a complexe de module 1 et $b \in \mathbb{C}$.

Cas $a = 1$: $f(z) = z + b$ est la translation complexe de vecteur b.
Si de plus $b = 0$, c'est l'identité qui est aussi une rotation.

Cas $a \neq 1$: Comme $|a| = 1$, il existe θ réel tel que $a = e^{i\theta}$. On pose $\omega = \dfrac{b}{1 - a}$.
On a $f(z) = e^{i\theta}z + \omega(1 - e^{i\theta}) = \omega + e^{i\theta}(z - \omega)$.
f est donc la rotation de centre ω et d'angle θ (CQFD).

Propriété : caractérisation des rotations

Soient T une transformation de P d'écriture complexe f et $\theta \not\equiv 0[2\pi]$ un réel.
T est une rotation d'angle θ si et seulement si

$$\forall M_1, M_2 \in P,\ \begin{cases} M_1'M_2' = M_1M_2 \\ \text{si } M_1 \neq M_2,\ (\overrightarrow{M_1'M_2'}, \overrightarrow{M_1M_2}) \equiv \theta\,[2\pi] \end{cases} \quad \text{en notant } \begin{cases} M_1' = T(M_1) \\ M_2' = T(M_2) \end{cases}.$$

autrement dit, f est une rotation d'angle θ si et seulement si

$$\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = e^{i\theta}(z_2 - z_1).$$

Démonstration
On montre le résultat dans le plan complexe.

- (LHS) $\Rightarrow$ (RHS) : soit f une rotation de centre ω et de rapport $e^{i\theta}$.
  $\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = \big(\omega + e^{i\theta}(z_2 - \omega)\big) - \big(\omega + e^{i\theta}(z_1 - \omega)\big) = e^{i\theta}(z_2 - z_1)$. (CQFD)
- (RHS) $\Rightarrow$ (LHS) : soit f une transformation complexe qui vérifie
  $\forall z_1, z_2 \in \mathbb{C},\ f(z_2) - f(z_1) = e^{i\theta}(z_2 - z_1)$.
  Soit $z \in \mathbb{C}$, on en déduit $f(z) - f(0) = e^{i\theta}(z - 0)$ c'est-à-dire $f(z) = e^{i\theta}z + f(0)$.
  Comme $\theta \not\equiv 0[2\pi]$ on a $e^{i\theta} \neq 1$, et d'après la démonstration du théorème précédent, f a bien la forme d'une rotation complexe.

Propriété

Toute rotation est une isométrie, donc une bijection.

Propriété

La composée de deux rotations **de même centre** est une rotation.
Plus précisément, soient $\Omega(\omega)$ un point, θ, θ' des réels , $\quad R_{\Omega,\theta} \circ R_{\Omega,\theta'} = R_{\Omega,\theta+\theta'}$.
Les transformations complexes associées vérifient : $\quad r_{\omega,\theta} \circ r_{\omega,\theta'} = r_{\omega,\theta+\theta'}$.

Remarque : cette propriété ne se généralise pas si les rotations n'ont pas le même centre.

Corollaire

Soient $\Omega(\omega)$ un point, θ, θ' des réels,

- Deux rotations de même centre commutent : $R_{\Omega,\theta} \circ R_{\Omega,\theta'} = R_{\Omega,\theta'} \circ R_{\Omega,\theta}$.
  c.a.d. $r_{\omega,\theta} \circ r_{\omega,\theta'} = r_{\omega,\theta'} \circ r_{\omega,\theta}$.
  Remarque : faux si les rotations n'ont pas le même centre.
- $R_{\Omega,\theta}^{-1} = R_{\Omega,-th}$ $\quad$ c.a.d. $r_{\omega,\theta}^{-1} = r_{\omega,-\theta}$.

Propriété : composée de deux rotations

Soient deux points $\Omega(\omega)$ et $\Omega'(\omega')$, θ, θ' des réels, $R_{\Omega,\theta} \circ R_{\Omega',\theta'}$ est

- Si $\theta \equiv -\theta'\,[2\pi]$: une translation.
  Le vecteur est nul si $\Omega = \Omega'$ ou $\theta \equiv \theta' \equiv 0[2\pi]$. C'est alors l'identité qui aussi une rotation.
- Si $\theta + \theta' \not\equiv 0\,[2\pi]$: une rotation d'angle $\theta + \theta'$.

Démonstration
En reprenant les notations de l'énoncé, $r_{\omega,\theta} = \omega + e^{i\theta}(z - \omega) = e^{i\theta}z + (1 - e^{i\theta})\omega$ et $r_{\omega',\theta'} = (z) = e^{i\theta'}z + (1 - e^{i\theta'})\omega'$.
Par un calcul simple, on a $r_{\omega,\theta} \circ r_{\omega,\theta'}(z) = e^{i\theta}e^{i\theta'}z + e^{i\theta}(1 - e^{i\theta'})\omega' + (1 - e^{i\theta})\omega = a''z + b''$,
en posant : $\begin{cases} a'' = e^{i(\theta+\theta')} \\ b'' = e^{i\theta}(1 - e^{i\theta'})\omega' + (1 - e^{i\theta})\omega \end{cases}$

$|a''| = 1$ donc d'après le théorème de caractérisation des rotations complexes, on distingue deux cas :

Cas $\theta \equiv -\theta' \,[2\pi]$: alors $a'' = 1$ donc la composée est une translation. De plus

$$\begin{aligned} b'' &= e^{i\theta}(1 - e^{-i\theta})\omega' + (1 - e^{i\theta})\omega \\ &= (e^{i\theta} - 1)\omega' + (1 - e^{i\theta})\omega \\ &= (e^{i\theta} - 1)(\omega' - \omega) \end{aligned}$$

$b'' = 0 \Leftrightarrow (e^{i\theta} - 1 = 0 \text{ ou } \omega' - \omega = 0) \Leftrightarrow \theta \equiv 0\,[2\pi] \text{ ou } \Omega = \Omega'$ (CQFD).

Cas $\theta + \theta' \not\equiv 0\,[2\pi]$: alors $a'' \neq 1$ donc la composée est une rotation d'angle $\theta + \theta'$.
Son centre est $\omega'' = \dfrac{b''}{1 - a''} = \dfrac{e^{i\theta}(1 - e^{i\theta'})\omega' + (1 - e^{i\theta})\omega}{1 - e^{i(\theta+\theta')}}$.

Propriété : point invariant

Toute rotation d'angle $\theta \not\equiv 0\,[2\pi]$ n'admet pas d'autre point invariant que son centre.

Propriété : droite globalement invariante

Soient Ω un point, θ un réel tel que $\theta \not\equiv 0\,[\pi]$.
Aucune droite n'est globalement invariante par la rotation $R_{\Omega,\theta}$.

Démonstration par l'absurde :
Soit D une droite globalement invariante et M un point de D distinct de Ω.
Considérons les points $M' = R_{\Omega,\theta}(M)$ et $M'' = R_{\Omega,\theta}(M')$.
D est globalement invariante donc M, M' et M'' sont sur D (1).
$M \neq \Omega$ donc M n'est pas invariant et $M' \neq M$.
On peut donc affirmer $(\overrightarrow{M'M''}, \overrightarrow{MM'}) \equiv \theta\,[2\pi]$.
Comme $\theta \not\equiv 0\,[\pi]$, M, M' et M'' ne sont pas alignés, contradictoire avec (1).

Chapitre V

Systèmes d'équations linéaires

1 Définitions

1.2 Système d'équations linéaires

Définition

Un système d'équations linéaires à n équations et p inconnues $(x_1, \ldots, x_p)$ peut s'écrire

$$(S)\begin{cases} a_{1,1}\,x_1 & + & \ldots & + & a_{1,p}\,x_p & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{n,1}\,x_1 & + & \ldots & + & a_{n,p}\,x_p & = & b_n \end{cases}$$

Les nombres $a_{i,j}$ et b_i sont appelés coefficients du système. Ce sont des nombres réels ou complexes.

1.3 Système homogène associé

Définition

On appelle **système homogène associé** au système (S) défini précédemment le système :

$$(SH)\begin{cases} a_{1,1}\,x_1 & + & \ldots & + & a_{1,p}\,x_p & = & 0 \\ \vdots & & & & \vdots & & \vdots \\ a_{n,1}\,x_1 & + & \ldots & + & a_{n,p}\,x_p & = & 0 \end{cases}$$

1.4 Systèmes équivalents

Définition

Deux systèmes sont **équivalents** si et seulement si ils ont le même ensemble de solutions.

1.5 Système compatible

Définition

Un système est dit **compatible** si et seulement si il admet au moins une solution.

Propriété

Tout système homogène est **compatible**.

Démonstration : un système homogène a toujours pour solution évidente la solution nulle $(0, \ldots, 0)$.

1.6 Propriétés

Propriété 1

Soit $X = (x_1, \ldots, x_p)$ une solution du système (S) et Y une solution du système homogène associé, alors $X + Y$ est une solution de (S).

Démonstration immédiate.

Propriété 2

L'ensemble des solutions d'un système **homogène** à coefficients réels et à p inconnues est un sous espace vectoriel de $\mathbb{R}^p$, c'est-à-dire que c'est un sous ensemble de $\mathbb{R}^p$ contenant le vecteur nul $(0, \ldots, 0)$ et stable par combinaison linéaire.

Démonstration
On note (SH) le système.
$(0, \ldots, 0)$ est une solution évidente de (SH) car il est homogène.

on note $\mathcal{S}_h$ l'ensemble des solutions de (SH).

$\mathcal{S}_h$ est stable par combinaison linéaire signifie : Soient α et β dans K, $X = (x_1, \ldots, x_p)$ et $Y = (y_1, \ldots, y_p)$ dans $\mathcal{S}_h$ alors $\alpha X + \beta Y = (\alpha x_1 + \beta y_1, \ldots, \alpha x_p + \beta y_p) \in \mathcal{S}_h$.

En effet, pour tout $i \in [1, n]$, $\alpha X + \beta Y$ vérifie la i-ième équation de (SH) car :
$a_{i,1}(\alpha x_1 + \beta y_1) + \ldots + a_{i,p}(\alpha x_p + \beta y_p) = \alpha(a_{i,1}x_1 + \ldots + a_{i,p}x_p) + \beta(a_{i,1}y_1 + \ldots + a_{i,p}y_p) = \alpha.0 + \beta.0 = 0.$

Propriété 3

Si X_0 une solution particulière de (S) et $\mathcal{S}_h$ l'ensemble des solutions du système homogène associé à (S), alors l'ensemble $\mathcal{S}$ des solutions de (S) est $\mathcal{S} = X_0 + \mathcal{S}_h = \{X_0 + Y / Y \in \mathcal{S}_h\}$.

Démonstration
On note $\mathcal{S}$ l'ensemble des solutions de (S).

D'après la propriété 1, on a $X_0 + \mathcal{S}_h \subset \mathcal{S}$.

On montre que l'on a aussi $X_0 + \mathcal{S}_h \supset \mathcal{S}$.
En effet, soit Y une solution de S alors $Y - X_0$ est solution de (SH) donc $Y \in X_0 + \mathcal{S}_h$.

Ecriture matricielle

On appelle **matrice** un tableau de nombres (que l'on note entre deux grandes parenthèses). Les nombres figurant dans une matrice sous appelé **coefficients** de la matrice.

Pour alléger l'écriture, on peut écrire le système

$$(S)\begin{cases} a_{1,1}x_1 + \ldots + a_{1,p}x_p = b_1 \\ \vdots \qquad\qquad \vdots \quad \vdots \\ a_{n,1}x_1 + \ldots + a_{n,p}x_p = b_n \end{cases} \quad \text{sous la forme matricielle :} \quad (S)\left(\begin{array}{ccc|c} a_{1,1} & \ldots & a_{1,p} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{n,1} & \ldots & a_{n,p} & b_n \end{array}\right)$$

A gauche du trait vertical, on ne fait figurer que les coefficients des inconnues, à droite du trait les seconds membres. Cette écriture est très pratique mais n'a de sens que si on respecte scrupuleusement l'ordre des inconnues et des colonnes.

2 Méthode du Pivot de Gauss

2.2 Système échelonné

Définitions : pivot, système échelonné

- On appelle **pivot d'une ligne** le premier coefficient non nul de cette ligne.
- Un système est dit **échelonné** si et seulement si le pivot de chaque ligne est à droite (au sens strict) de celui de la ligne précédente.

Exemples : les pivots sont entourés.

$$\left(\begin{array}{cccc|c} 0 & \boxed{1} & 2 & 0 & 1 \\ 0 & 0 & \boxed{-2} & 0 & 2 \\ 0 & 0 & 0 & \boxed{-1} & -1 \end{array}\right) \qquad \left(\begin{array}{cccc|c} \boxed{3} & -3 & 2 & -1 & 1 \\ 0 & 0 & \boxed{2} & 3 & 2 \\ 0 & 0 & 0 & \boxed{1} & -4 \\ 0 & 0 & 0 & 0 & \boxed{1} \end{array}\right)$$

Ce dernier écrit en notation classique $\begin{cases} \boxed{3}x - 3y + 2z - t = 1 \\ \qquad\qquad \boxed{2}z + 3t = 2 \\ \qquad\qquad\qquad \boxed{1}t = -4 \\ \qquad\qquad\qquad 0 = \boxed{1} \end{cases}$

Définition : inconnues principales et secondaires

Dans un système échelonné, on appelle **inconnues principales** celles dont le coefficient sur une des lignes est un pivot, les autres inconnues sont appelées **secondaires**.

Exemple

$$\begin{cases} \boxed{-1}x + 2y + 3z + 2t = 3 \\ \qquad\qquad \boxed{2}z = 5 \end{cases}$$

Dans ce système échelonné, x et z sont les inconnues principales, y et t les inconnues secondaires.

2.3 Solutions d'un système échelonné

Propriété : existence (compatibilité)

Un système échelonné admet des solutions (est compatible) si et seulement si il n'y a pas de pivot sur la colonne des seconds membres.

Explication : si il y a un pivot sur la colonne des seconds membres, l'équation correspondante est $0 = 1$.

Exemple de système ***incompatible***

$$\begin{cases} \boxed{1}x + 2y + 3z = -1 \\ \qquad\quad \boxed{1}z = 2 \\ \qquad\qquad 0 = \boxed{1} \end{cases}$$

Propriété : unicité

Un système échelonné compatible admet une solution unique si et seulement si il n' a pas d'inconnue secondaire.

Explication : on a un système triangulaire dont tous les coefficients diagonaux sont non nuls.

Exemple

$$\begin{cases} \boxed{1}x \quad + 2z = 0 \\ \quad \boxed{1}y - z = 3 \\ \qquad \boxed{1}z = 2 \end{cases}$$

Propriété : solutions multiples

Un système échelonné compatible admet des solutions multiples si et seulement si il possède au moins une inconnue secondaire.
La dimension du sous-espace affine des solutions est égale au nombre d'inconnues secondaires.

Expression paramétrique des solutions multiples

Pour exprimer l'ensemble des solutions de manière paramétrique :
1) On remplace toutes les inconnues secondaires par des paramètres dont les valeurs sont quelconques.
2) On calcule les inconnues principales en fonction de ces paramètres.

Exemple

$$\begin{cases} \boxed{1}x + 2y + 3z + 2t = 3 \\ \boxed{z} = 2 \end{cases}$$

Propriété

Si le nombre d'équations est strictement inférieur au nombre d'inconnus, le système homogène associé a au moins une solution non nulle (c.a.d. il admet des solutions multiples).

Démonstration : on note n le nombre d'équations et p le nombre d'inconnues.

Si le système est échelonné, le système homogène associé a au moins la solution nulle.

De plus, on a au plus n pivots (1 par ligne non nulle) et p inconnues, si $n < p$, il y a plus d'inconnues que de pivots, donc il y a des inconnues secondaires, c.a.d. que le système admet des solutions multiples.

Si le système n'est pas échelonné, par la méthode du pivot de Gauss, on peut obtenir un système échelonné équivalent à n équations et p inconnues et le raisonnement précédent peut alors s'appliquer.

2.4 Opérations élémentaires

Définition

On appelle **opération élémentaire** une des trois opérations suivantes :
1) Permuter deux lignes.
2) Multiplier une ligne par un scalaire **non nul**.
3) Ajouter à une ligne L_i une **autre** ligne L_j ($j \neq i$) multipliée un scalaire λ quelconque ($L_i \to L_i + \lambda L_j$).

Théorème

Les opérations élémentaires transforment un système en un système équivalent.

Démonstration

1) Le système est évidemment équivalent si on permute deux lignes.
2) Appelons (S) le système initial et (S') le système obtenu en multipliant la ligne L_i par le scalaire $\lambda \neq 0$.
   Si $X = (x_1, \ldots, x_p)$ est solution de (S), alors X vérifie la ligne $L'_i = \lambda L_i$ de (S'), les autres lignes étant identiques dans S et S', X est solution de (S').
   Si $X = (x_1, \ldots, x_p)$ est solution de (S'), alors X vérifie la ligne $L_i = \frac{1}{\lambda} L'_i$ de (S) car $\lambda \neq 0$, les autres lignes étant identiques dans S' et S, X est solution de (S).
   Si λ est on nul, on a bien deux systèmes équivalents.
3) Appelons (S) le système initial et (S') le système dont seule la i-ème ligne est différente avec $L'_i = L_i + \lambda L_j$ ($j \neq i$ et λ scalaire quelconque).
   Si $X = (x_1, \ldots, x_p)$ est solution de (S), alors X vérifie la ligne $L'_i = L_i + \lambda L_j$ de (S'), les autres lignes étant identiques dans S et S', X est solution de (S').
   Si $X = (x_1, \ldots, x_p)$ est solution de (S'), alors X vérifie aussi $L'_i - \lambda L'_j = L'_i - \lambda L_j$ car $j \neq i$ et donc la ligne L_j est inchangée dans S'. Or $L'_i - \lambda L_j = L_i$, les autres lignes étant identiques dans S' et S, X est solution de (S).
   Si $j \neq i$, on a bien deux systèmes équivalents.

2.5 Regroupement d'opérations élémentaires

Théorème

On obtient un système équivalent en effectuant une des trois opérations suivantes :
1) Echanger l'ordre des lignes.
2) Multiplier les lignes par des scalaires **non nuls**.
3) Après avoir choisi une ligne L_i, remplacer une ou plusieurs **autres** lignes L_j $(j \neq i)$ par $L_j + \lambda_j L_i$ où les λ_j sont des scalaires quelconques. Attention, **il est essentiel de ne pas modifier la ligne** L_i.

Démonstration

Pour les opérations 1. et 2., on peut décomposer de manière évidente ces opérations en une succession d'opérations élémentaires, donc le système obtenu est équivalent.

Pour l'opérations 3., on peut aussi décomposer cette opération en une succession d'opérations élémentaires de type 3 parce que la ligne L_i est inchangée. Le système obtenu est donc équivalent.

Contre exemple

Le système $\begin{cases} x+y+z=3 \\ y+z=2 \\ z=1 \end{cases}$ admet une solution unique $(x,y,z)=(1,1,1)$.

Si on effectue en une seule étape les opérations $L_1 \to L_1 - L_2$ et $L_2 \to L_2 - L_3$ et $L_3 \to L_3 - L_1$, on obtient le système :

$\begin{cases} x=1 \\ y=1 \\ x+y=2 \end{cases}$ où z est une inconnue secondaire et dont l'ensemble des solutions est la droite passant par $(1,1,0)$ et de vecteur directeur $(0,0,1)$.

Ces deux systèmes ne sont pas équivalents !

2.6 Méthode du Pivot de Gauss

Description

Elle consiste transformer un système (S) donné en un système échelonné (S') équivalent à l'aide des opérations élémentaires.
On échelonne colonne par colonne de la gauche vers la droite.
Pour chaque colonne, on annule les coefficients sous le premier pivot (en descendant la colonne) par des opérations de type 3.
Les opérations de type 1 servent à réorganiser éventuellement le système pour gagner des étapes.
Les opérations de type 2 servent à ramener les pivots à 1 (simplification des calculs).
On peut en plus annuler les coefficients au dessus du pivot, ce qui évite de faire des substitutions pour résoudre le système échelonné (S').

Exemple 1

$$\begin{cases} x+y-z=0 \\ x+5y=3 \\ 2x+y-z=1 \end{cases}$$

Le système peut s'écrire en notation matricielle : $\left(\begin{array}{ccc|c} \boxed{1} & 1 & -1 & 0 \\ \boxed{1} & 5 & 0 & 3 \\ \boxed{2} & 1 & -1 & 1 \end{array}\right)$

En utilisant la méthode de Gauss, on obtient les systèmes équivalents suivants :

$$\left(\begin{array}{ccc|c} \boxed{1} & 1 & -1 & 0 \\ 0 & \boxed{4} & 1 & 3 \\ 0 & \boxed{-1} & 1 & 1 \end{array}\right) \begin{array}{l} L_1 \\ L_2 - L_1 \\ L_3 - 2L_1 \end{array} \qquad \left(\begin{array}{ccc|c} \boxed{1} & 1 & -1 & 0 \\ 0 & \boxed{1} & -1 & -1 \\ 0 & \boxed{4} & 1 & 3 \end{array}\right) \begin{array}{l} L_1 \\ -L_3 \\ L_2 \end{array}$$

$$\left(\begin{array}{ccc|c} \boxed{1} & 0 & 0 & 1 \\ 0 & \boxed{1} & -1 & -1 \\ 0 & 0 & \boxed{5} & 7 \end{array}\right) \begin{array}{l} L_1 - L_2 \\ L_2 \\ L_3 - 4L_2 \end{array} \qquad \left(\begin{array}{ccc|c} \boxed{1} & 0 & 0 & 1 \\ 0 & \boxed{1} & -1 & -1 \\ 0 & 0 & \boxed{1} & \frac{7}{5} \end{array}\right) \begin{array}{l} L_1 \\ L_2 \\ \frac{L_3}{5} \end{array}$$

Ce système échelonné est compatible et n'a pas d'inconnues secondaires, il admet donc une solution unique. On poursuit la résolution soit en continuant la méthode du pivot soit par substitution.

$$\left(\begin{array}{ccc|c} \boxed{1} & 0 & 0 & 1 \\ 0 & \boxed{1} & 0 & \frac{2}{5} \\ 0 & 0 & \boxed{1} & \frac{7}{5} \end{array}\right) \begin{array}{l} L_1 \\ L_2 + L_3 \\ L_3 \end{array}$$

Le système admet pour solution unique $(x, y, z) = (1, \frac{2}{5}, \frac{7}{5})$.

Exemple 2

$$\begin{cases} x + y + 3z + 2t = -2 \\ 2x + 3y + 4z + t = -1 \\ 3x + 7y + z - 6t = 6 \end{cases}$$

Le système peut s'écrire en notation matricielle : $\left(\begin{array}{cccc|c} \boxed{1} & 1 & 3 & 2 & -2 \\ \boxed{2} & 3 & 4 & 1 & -1 \\ \boxed{3} & 7 & 1 & -6 & 6 \end{array}\right)$

En utilisant la méthode de Gauss, on obtient les systèmes équivalents suivants :

$$\left(\begin{array}{cccc|c} \boxed{1} & 1 & 3 & 2 & -2 \\ 0 & \boxed{1} & -2 & -3 & 3 \\ 0 & \boxed{4} & -8 & -12 & 12 \end{array}\right) \begin{array}{l} L_1 \\ L_2 - 2L_1 \\ L_3 - 3L_1 \end{array} \qquad \left(\begin{array}{cccc|c} \boxed{1} & 1 & 3 & 2 & -2 \\ 0 & \boxed{1} & -2 & -3 & 3 \\ 0 & \boxed{1} & -2 & -3 & 3 \end{array}\right) \begin{array}{l} L_1 \\ L_2 \\ \frac{L_3}{4} \end{array}$$

$$\left(\begin{array}{cccc|c} \boxed{1} & 0 & 5 & 5 & -5 \\ 0 & \boxed{1} & -2 & -3 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{l} L_1 - L_2 \\ L_2 \\ L_3 - L_2 \end{array}$$

Ce système échelonné est compatible et a 2 inconnues secondaires z et t, donc il admet des solutions multiples, son ensemble de solutions est un espace affine de dimension 2.
Pour exprimer les solutions sous forme paramétrique, on pose $\lambda = z$ et $\mu = t$, les solutions vérifient

$$\begin{cases} x = -5 - 5\lambda - 5\mu \\ y = 3 + 2\lambda + 3\mu \\ z = \lambda \\ t = \mu \end{cases}$$

L'ensemble des solutions est $\{(-5 - 5\lambda - 5\mu, 3 + 2\lambda + 3\mu, \lambda, \mu) \mid \lambda, \mu \in \mathbb{R}\}$.

Exemple 3

$$\begin{cases} x + y - z = 0 \\ x + 5y - 2z = 3 \\ 2x - 2y - z = 1 \end{cases}$$ c.a.d. en notation matricielle : $\left(\begin{array}{ccc|c} \boxed{1} & 1 & -1 & 0 \\ \boxed{1} & 5 & -2 & 3 \\ \boxed{2} & -2 & -1 & 1 \end{array}\right)$

En utilisant la méthode de Gauss, on obtient les systèmes équivalents suivants :

$$\left(\begin{array}{ccc|c} \boxed{1} & 1 & -1 & 0 \\ 0 & \boxed{4} & -1 & 3 \\ 0 & \boxed{-4} & 1 & 1 \end{array}\right) \begin{array}{l} L_1 \\ L_2 - L_1 \\ L_3 - 2L_1 \end{array} \qquad \left(\begin{array}{ccc|c} \boxed{1} & 1 & -1 & 0 \\ 0 & \boxed{1} & \frac{1}{4} & \frac{3}{4} \\ 0 & 0 & 0 & \boxed{4} \end{array}\right) \begin{array}{l} L_1 \\ L_2/4 \\ L_3 + L_2 \end{array}$$

Le système a un pivot sur la colonne des seconds membres donc il est incompatible.

Chapitre VI

Notions élémentaires de géométrie affine

1 Généralités

1.2 Vecteurs

Vocabulaire

On désigne par $\mathcal{E}$ l'Espace (avec une majuscule), c.a.d. l'espace physique à trois dimensions.
Soient A, B des points de l'Espace, le vecteur $\overrightarrow{AB}$ est une grandeur qui mesure le déplacement de A vers B.

Propriété

Soient A, B, C, D des points de l'Espace, $\overrightarrow{AB} = \overrightarrow{DC}$ si et seulement si (A, B, C, D) est un parallélogramme.

Propriété

Soient A, B des points de l'Espace, $\overrightarrow{AB} = \vec{0}$ si et seulement si A et B sont confondus ($A = B$).

Propriété

Soient A, B des points de l'Espace, $\overrightarrow{AB} = -\overrightarrow{BA}$.

Relation de Chasles

Soient A, B, C, des points de l'Espace, $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

1.3 Espaces vectoriels

Définition : direction

Soit F l'Espace, un plan, une droite ou un singleton, on note $\vec{F} = \{\overrightarrow{AB} \mid A, B \in F\}$, l'ensemble des vecteurs formés avec des points de F.
$\vec{F}$ est appelé direction de F.

Remarque
La direction d'un singleton $\{A\}$ où A est un point est $\{\vec{0}\}$.

Propriété

Soit F l'Espace, un plan ou une droite, $\vec{F}$ est un sous-espace vectoriel de $\vec{\mathcal{E}}$, c'est-à-dire que :

- $\forall \vec{u}, \vec{v} \in \vec{F}$, $\vec{u} + \vec{v} \in \vec{F}$, c'est la stabilité par addition.
- $\forall \lambda \in \mathbb{R}$, $\forall \vec{u} \in \vec{F}$, $\lambda\,\vec{u} \in \vec{F}$, c'est la stabilité par multiplication par un scalaire (les réels).

Définition : dimension

- La dimension de l'espace $\mathcal{E}$ et de sa direction $\vec{\mathcal{E}}$ est 3.
- La dimension d'un plan P et de sa direction $\vec{P}$ est 2.
- La dimension d'une droite D et de sa direction $\vec{D}$ est 1.
- La dimension d'un singleton $\{A\}$ où A est un point est 0. Sa direction $\{\vec{0}\}$ est aussi de dimension nulle.

Propriété

Soit F et F' deux droites ou deux plans de $\mathcal{E}$ (F et F' sont de même dimension).
$F \parallel F'$ si et seulement si ils ont la même direction, c'est-à-dire $\vec{F} = \vec{F'}$.

Démonstration
Supposons $F \parallel F'$.

Soit $\vec{v} \in \vec{F}$, il existe $A, B \in F$ tels que $\vec{v} = \overrightarrow{AB}$.
Soit $C \in F'$. On construit le parallélogramme (A, B, D, C). On a $\vec{v} = \overrightarrow{AB} = \overrightarrow{CD}$ et de plus $D \in F'$ car F et F' sont de même dimension et parallèles.

Donc $\vec{v} \in \vec{F'}$. Il suit que $\vec{F} \subset \vec{F'}$.

On montre de même que $\vec{F'} \subset \vec{F}$ donc $\vec{F} = \vec{F'}$. (CQFD)

Inversement, supposons que $\vec{F} = \vec{F'}$.

Si F et F' sont des droites, on note $(\vec{u})$ une base de $\vec{F} = \vec{F'}$.
$\vec{u}$ est un vecteur directeur des droites F et F' donc ces droites sont parallèles. (CQFD)

Si F et F' sont des plans, on note $(\vec{u}, \vec{v})$ une base de $\vec{F} = \vec{F'}$.
On note A et A' des points respectivement de F et F', puis D_u et D'_u les droites de repères respectivement $(A, \vec{u})$ et $(A', \vec{u})$, et enfin D_v et D'_v les droites de repères respectivement $(A, \vec{v})$ et $(A', \vec{v})$.

On a $D_u \parallel D'_u$ et $D_v \parallel D'_v$ avec D_u et D_v sécantes et incluses dans F et D'_u et D'_v sécantes et incluses dans F' donc F et F' sont deux plans parallèles. (CQFD)

1.4 Repères et bases

Définition : repères et bases en dimension 3

On appelle repère de l'espace $\mathcal{E}$, un quadruplet (O, I, J, K) de points non coplanaires de $\mathcal{E}$, le premier point, (ici O), est appelé origine du repère.
Alors, pour tout point $M \in \mathcal{E}$, il existe un unique triplet $(x, y, z) \in \mathbb{R}^3$ tel que $\overrightarrow{OM} = x\overrightarrow{OI} + y\overrightarrow{OJ} + z\overrightarrow{OK}$ (*).
(x, y, z) sont appelées coordonnées de M dans le repère (O, I, J, K).
On peut aussi définir un repère de l'Espace par la donnée d'un quadruplet $(O, \vec{i}, \vec{j}, \vec{k})$ tels que les vecteurs $\vec{i}, \vec{j}, \vec{k}$ sont linéairement indépendants (cf. définition ci-dessous).
L'égalité (*) s'écrit alors : $\overrightarrow{OM} = x\vec{i} + y\vec{j} + z\vec{k}$.
$(\vec{i}, \vec{j}, \vec{k})$ est alors appelée base de l'espace vectoriel $\vec{\mathcal{E}}$.

Définition : indépendance linéaire

Soient $\vec{u_1}$, $\vec{u_2}$, ..., $\vec{u_p}$, des vecteurs de l'Espace, ces vecteurs sont dits linéairement indépendants si et seulement si :

$$\forall \alpha_1, \ldots, \alpha_n \in \mathbb{R}, \quad \alpha_1 u_1 + \cdots + \alpha_n u_n = \vec{0} \Rightarrow \begin{cases} \alpha_1 = 0 \\ \vdots \\ \alpha_n = 0 \end{cases}$$

Propriété : indépendance linéaire de deux vecteurs

Soient $\vec{u}$, $\vec{v}$ **deux** vecteurs de l'Espace, $(\vec{u}, \vec{v})$ sont linéairement indépendants si et seulement si ils ne sont pas colinéaires.

Démonstration

On montre la contraposée : $(\vec{u}, \vec{v})$ ne sont pas linéairement indépendants si et seulement si ils sont colinéaires.

Soient $(\vec{u}, \vec{v})$ non linéairement indépendants. Alors il existe α, β non tous deux nuls tels que $\alpha\vec{u} + \beta\vec{v} = \vec{0}$.

Supposons par exemple que ce soit β qui soit non nul, alors $\vec{v} = -\frac{\alpha}{\beta}\vec{u}$ donc $\vec{u}$ et $\vec{v}$ sont colinéaires. (CQFD)

Soient $(\vec{u}, \vec{v})$ colinéaires, alors il existe $k \in \mathbb{R}$ tel que $\vec{u} = k\vec{v}$ ou $\vec{v} = k\vec{u}$.

On a donc $\vec{u} - k\vec{v} = \vec{0}$ ou $k\vec{u} - \vec{v} = \vec{0}$.

Le couple $(\alpha, \beta) = (1, -k)$ ou le couple $(\alpha, \beta) = (k, -1)$ vérifie $\alpha\vec{u} + \beta\vec{v} = \vec{0}$ avec $(\alpha, \beta) \neq (0, 0)$.

Donc $\vec{u}, \vec{v}$ ne sont pas linéairement indépendants. (CQFD)

Propriété : indépendance linéaire d'un vecteur

Soient $\vec{u}$ un vecteur de l'Espace, $\vec{u}$ est linéairement indépendant si et seulement si il n'est pas nul.

Démonstration

On montre la contraposée : $\vec{u}$ n'est pas linéairement indépendant si et seulement si il est nul.

Si $\vec{u} = \vec{0}$ alors on a par exemple $1.\vec{u} = 1.\vec{0} = \vec{0}$ donc $\vec{u}$ ne vérifie pas la propriété d'indépendance linéaire. (CQFD)

Si $\vec{u}$ n'est pas linéairement indépendant alors il existe $\lambda \neq 0$ tel que $\lambda\vec{u} = \vec{0}$ ce qui implique $\vec{u} = 0$. (CQFD)

Définition : repères et bases en dimension 2

On appelle repère d'un plan P, un triplet (O, I, J) de points non alignés de P.
Alors, pour tout point $M \in P$, il existe un unique couple $(x, y) \in \mathbb{R}^2$ tel que $\overrightarrow{OM} = x\overrightarrow{OI} + y\overrightarrow{OJ}$ (*).
(x, y) sont appelées coordonnées de M dans le repère (O, I, J).
On peut aussi définir un repère de P par la donnée d'un triplet $(O, \vec{i}, \vec{j})$ tels que les vecteurs $\vec{i}, \vec{j} \in \vec{P}$ sont linéairement indépendants ce qui est équivalents, **pour deux vecteurs**, à $\vec{i}, \vec{j}$ sont non colinéaires.
L'égalité (*) s'écrit alors : $\overrightarrow{OM} = x\vec{i} + y\vec{j}$.
$(\vec{i}, \vec{j})$ est alors appelée base de l'espace vectoriel $\vec{P}$.

Définition : repères et bases en dimension 1

On appelle repère d'une droite D, un couple (O, I) de points distincts de D.
Alors, pour tout point $M \in D$, il existe un unique $x \in \mathbb{R}$ tel que $\overrightarrow{OM} = x\overrightarrow{OI}$ (*).
x est appelée coordonnée de M dans le repère (O, I).
On peut aussi définir un repère de P par la donnée d'un couple $(O, \vec{i})$ tels que le vecteur $\vec{i} \in \vec{D}$ est linéairement indépendant ce qui est équivalent, **pour un vecteur**, à $\vec{i}$ non nul.
L'égalité (*) s'écrit alors : $\overrightarrow{OM} = x\vec{i}$.
$(\vec{i})$ est alors appelée base de l'espace vectoriel $\vec{D}$.

2 Plan affine $\mathbb{R}^2$

2.2 Généralités

Dans le plan affine $\mathbb{R}^2$, on considère les couples comme des points.

Définition et propriété : vecteurs de $\overrightarrow{\mathbb{R}^2}$

Soient $A = (x_A, y_A)$ et $B = (x_B, y_B)$ deux points de $\mathbb{R}^2$, on définit le vecteur $\overrightarrow{AB}$ par :

$$\overrightarrow{AB} = (x_B - x_A\,,\, y_B - y_A).$$

On peut alors appliquer toutes les définitions et propriétés de la section 1 concernant les plans, on obtient donc la même géométrie que dans un plan de l'Espace.

2.3 Sous-espaces affines de $\mathbb{R}^2$

Propriété

Les sous-espaces de $\mathbb{R}^2$ sont :

- les espaces de dimension 0, c'est à dire les singletons $\{A\}$ avec $A \in \mathbb{R}^2$.
- les espaces de dimension 1, c'est à dire les droites de $\mathbb{R}^2$.
- le plan $\mathbb{R}^2$ lui-même de dimension 2.

2.4 Équation paramétrique d'une droite de $\mathbb{R}^2$

Propriété

Toute droite de $\mathbb{R}^2$ admet une équation paramétrique de la forme $\begin{cases} x = x_a + \lambda x_u \\ y = y_a + \lambda y_u \end{cases}$ $(\lambda \in \mathbb{R})$ telle que $(x_u, y_u) \neq (0, 0)$.
Inversement, toute partie de $\mathbb{R}^2$ ayant une telle équation paramétrique est une droite de vecteur directeur $\vec{u} = (x_u, y_u)$ passant par $A = (x_a, y_a)$.

Démonstration : On note $M = (x, y)$, $A = (x_a, y_a)$ et $u = (x_u, y_u)$ et D la droite passant par A et dirigée par $\vec{u}$. Ce résultat se déduit de l'équivalence :
$\exists \lambda \in \mathbb{R}, \begin{cases} x = x_a + \lambda x_u \\ y = y_a + \lambda y_u \end{cases} \Leftrightarrow \overrightarrow{AM}$ et $\vec{u}$ sont colinéaires $\Leftrightarrow$ $M \in D$.

2.5 Équation cartésienne d'une droite de $\mathbb{R}^2$

Propriété

Toute droite de $\mathbb{R}^2$ admet une équation de la forme $ax + by + c = 0$ avec $(a, b) \neq (0, 0)$.
Inversement, toute partie de $\mathbb{R}^2$ admettant une telle équation est une droite de vecteur directeur $\vec{u} = (-b, a)$ passant par $A = (\frac{-c}{a}, 0)$ si a est non nul, $A = (0, \frac{-c}{b})$ sinon.

Démonstration : Soit D une droite de $\mathbb{R}^2$. Soit $A = (x_a, y_a)$ un point de D et $\vec{u} = (x_u, y_u)$ un vecteur directeur.
$M = (x, y) \in D$ si et seulement si $\overrightarrow{AM}$ est colinéaire à $\vec{u}$, c'est-à-dire $(x - x_a, y - y_a)$ est proportionnel (x_u, y_u), qui équivaut, d'après les produits en croix à : $y_u(x - x_a) = x_u(y - y_a)$ ce qui s'écrit $y_u x - x_u y - y_u x_a + x_u y_a = 0$.
Comme $(x_u, y_u) \neq (0, 0)$, on a bien une équation de la forme attendue.

Inversement, soit $(a, b) \neq (0, 0)$ et F la partie d'équation $ax + by + c = 0$ (1). Supposons $a \neq 0$, (x, y) est solution de (1) si et seulement si il existe λ tel que $\begin{cases} x = \frac{-c - b\lambda}{a} \\ y = \lambda \end{cases}$. Il s'agit de l'équation paramétrique de la droite passant par $A = (\frac{-c}{a}, 0)$ et de vecteur directeur $(\frac{-b}{a}, 1)$ colinéaire à $\vec{u} = (-b, a) \neq 0$.

Si $a = 0$, nécessairement $b \neq 0$, par le même raisonnement on en déduit que $(x, y) \in F$ si et seulement si il existe $\lambda \in$ tel que $(x, y) = (0, \frac{-c}{b}) + \lambda(1, \frac{-a}{b})$. F est donc la droite passant par $A = (0, \frac{-c}{b})$ et de vecteur directeur $\vec{u} = (-b, a)$.

Propriété : équation cartésienne de la direction d'une droite

Soit D une droite de $\mathbb{R}^2$ d'équation cartésienne $ax + by + c = 0$ avec $(a, b) \neq (0, 0)$.
Sa direction $\vec{D}$ admet pour équation cartésienne $ax + by = 0$, c'est-à-dire l'équation cartésienne homogène associée à celle de D.

Démonstration
Soit $A = (x_A, y_A) \in D$ et $B = (x_B, y_B) \in D$. On a $ax_A + by_A + c = 0$ (1) et $ax_B + by_B + c = 0$ (2).

Alors $\overrightarrow{AB} = (x_B - x_A, y_B - y_A)$ vérifie $a(x_B - x_A) + b(y_B - y_A) = 0$ par soustraction des égalités (2) et (1).

Donc les vecteurs de $\vec{D}$ vérifie l'équation $ax + by = 0$.

Inversement, une fois choisi un point $A = (x_A, y_A) \in D$, tout vecteur $\vec{v} = (x, y)$ vérifiant $ax + by = 0$ peut s'écrire $\vec{v} = (x_B - x_A, y_B - y_A)$ avec $B = (x_A + x, y_A + y)$.

Comme $a(x_A + x) + b(y_A + y) = (ax_A + by_A) + (ax + by) = -c$, on a $B \in D$ et donc $\vec{v} \in \vec{D}$.

Théorème : équations de droites parallèles

Soit D et D' deux droites de $\mathbb{R}^2$ d'équations $ax + by + c = 0$ et $a'x + b'y + c' = 0$.
$D \parallel D' \Leftrightarrow ab' - a'b = 0$.

Démonstration : D et D' ont pour vecteur directeur respectivement $\vec{u} = (-b, a)$ et $\vec{u}' = (-b', a')$.

$D \parallel D'$ si et seulement si $\vec{u}$ et $\vec{u}'$ sont colinéaires, c.a.d. $(-b, a)$ et $(-b', a')$ sont proportionnels, c.a.d. $-ba' = -ab'$ (produit en croix), qui s'écrit aussi $ab' - a'b = 0$.

3 Espace affine $\mathbb{R}^3$

3.2 Généralités

Dans l'espace affine $\mathbb{R}^3$, on considère les triplets comme des points.

Définition et propriété : vecteurs de $\overrightarrow{\mathbb{R}^2}$

Soient $A = (x_A, y_A, z_A)$ et $B = (x_B, y_B, z_B)$ deux points de $\mathbb{R}^3$, on définit le vecteur $\overrightarrow{AB}$ par :

$$\overrightarrow{AB} = (x_B - x_A\,,\, y_B - y_A\,,\, z_B - z_A).$$

On peut alors appliquer toutes les définitions et propriétés de la section 1 concernant l'Espace, on obtient donc la même géométrie que dans l'Espace.

3.3 Sous-espaces affines de $\mathbb{R}^3$

Propriété

Les sous-espaces de $\mathbb{R}^3$ sont :

- les espaces de dimension 0, c'est à dire les singletons $\{A\}$ avec $A \in \mathbb{R}^3$.
- les espaces de dimension 1, c'est à dire les droites de $\mathbb{R}^3$.
- les espaces de dimension 2, c'est à dire les plans de $\mathbb{R}^3$.
- l'espace $\mathbb{R}^3$ lui-même de dimension 3.

3.4 Plans de $\mathbb{R}^3$

Propriété : équation paramétrique d'un plan de $\mathbb{R}^3$

Tout plan de $\mathbb{R}^3$ admet une équation paramétrique de la forme $\begin{cases} x = x_a + \lambda x_u + \mu x_v \\ y = y_a + \lambda y_u + \mu y_v \\ z = z_a + \lambda z_u + \mu z_v \end{cases}$ de paramètres $\lambda, \mu \in \mathbb{R}$ et où $\vec{u} = (x_u, y_u, z_u)$ et $\vec{v} = (x_v, y_v, z_v)$ sont non colinéaires.
Inversement, toute partie de $\mathbb{R}^3$ ayant une telle équation paramétrique est un plan de repère $(A, \vec{u}, \vec{v})$.

Démonstration : même méthode que pour les droites.

Propriété : équation cartésienne d'un plan de $\mathbb{R}^3$

Tout plan P de $\mathbb{R}^3$ admet une équation de la forme $ax + by + cz + d = 0$ avec $(a, b, c) \neq (0, 0, 0)$.
Inversement, toute partie de $\mathbb{R}^3$ admettant une telle équation est un plan P dont la direction $\vec{P}$ admet pour équation cartésienne $ax + by + cz = 0$, c.a.d. l'équation homogène associé à celle de P.

Démonstration
Soit P un plan de $\mathbb{R}^3$ et $(A, \vec{u}, \vec{v})$ un repère de P avec $A = (x_a, y_a, z_a)$, $\vec{u} = (x_u, y_u, z_u)$ et $\vec{v} = (x_v, y_v, z_v)$.

$$M = (x, y, z) \in P \Leftrightarrow \exists \lambda, \mu \in \mathbb{R}, \quad \begin{cases} x = x_a + \lambda x_u + \mu x_v \\ y = y_a + \lambda y_u + \mu y_v \\ z = z_a + \lambda z_u + \mu z_v \end{cases}$$

Donc $M = (x, y, z) \in P$ si et seulement si le système (S) : $\begin{cases} x = x_a + \lambda x_u + \mu x_v \\ y = y_a + \lambda y_u + \mu y_v \\ z = z_a + \lambda z_u + \mu z_v \end{cases}$ d'inconnues λ et μ admet au moins une solution.

On échelonne (S) par la méthode de Gauss. Il existe au moins une composante de $\vec{u}$ non nulle car $\vec{u} \neq \vec{0}$. Supposons que ce soit x_u.

$$\text{(S)} \Leftrightarrow \begin{cases} x_u\lambda + x_v\mu = x - x_a & L_1 \\ x_u y_u\lambda + x_u y_v\mu = x_u(y - y_a) & x_u L_2 \\ x_u z_u\lambda + x_u z_v\mu = x_u(z - z_a) & x_u L_3 \end{cases}$$

$$\Leftrightarrow \begin{cases} x_u\lambda + x_v\mu = x - x_a & L_1 \\ (x_u y_v - x_v y_u)\mu = x_u(y - y_a) - y_u(x - x_a) & L_2 - y_u L_1 \\ (x_u z_v - x_v z_u)\mu = x_u(z - z_a) - z_u(x - x_a) & L_3 - z_u L_1 \end{cases}$$

Ce système est compatible si et seulement si les deux dernières équations sont proportionnelles, c.a.d. avec les produits en croix :

$$\big(x_u y_v - x_v y_u\big)\big(x_u(z - z_a) - z_u(x - x_a)\big) = \big(x_u z_v - x_v z_u\big)\big(x_u(y - y_a) - y_u(x - x_a)\big) \quad (1)$$

$$(1) \Leftrightarrow (y_u z_v - y_v z_u)x_u(x - x_a) - (x_u z_v - x_v z_u)x_u(y - y_a) + (x_u y_v - x_v y_u)x_u(z - z_a) = 0$$

$$(1) \Leftrightarrow (y_u z_v - y_v z_u)(x - x_a) - (x_u z_v - x_v z_u)(y - y_a) + (x_u y_v - x_v y_u)(z - z_a) = 0 \quad \text{car } x_u \neq 0.$$

Finalement (1) s'écrit $ax+by+cz+d = 0$ avec $\begin{cases} a = y_u z_v - y_v z_u \\ b = -x_u z_v + x_v z_u \\ c = x_u y_v - x_v y_u \\ d = -x_a(y_u z_v - y_v z_u) + y_a(x_u z_v - x_v z_u) - z_a(x_u y_v - x_v y_u) \end{cases}$

De plus, si on avait $(a, b, c) = (0, 0, 0)$, $\vec{u}$ et $\vec{v}$ seraient colinéaires (produits en croix) ce qui est contradictoire avec $(A, \vec{u}, \vec{v})$ est un repère de P.

Conclusion : P admet une équation de la forme $ax + by + cz + d = 0$ avec $(a, b, c) \neq (0, 0, 0)$.

Inversement, soit F une partie de $\mathbb{R}^3$ qui admet une équation de la forme $ax + by + cz + d = 0$ avec a, b et c non tous nuls.
Supposons par exemple que $a \neq 0$.
$M = (x, y, z) \in F \Leftrightarrow ax + by + cz + d = 0 \Leftrightarrow x = -\frac{b}{a}y - \frac{c}{a}z - \frac{d}{a}$.

On obtient donc l'expression paramétrique $F = \{(-\frac{d}{a} - \frac{b}{a}\lambda - \frac{c}{a}\mu, \lambda, \mu) \mid \lambda, \mu \in \mathbb{R}\}$.

On pose $A = (\frac{-d}{a}, 0, 0)$, $\vec{u} = (-\frac{b}{a}, 1, 0)$ et $\vec{v} = (-\frac{c}{a}, 0, 1)$.

$\vec{u}$ et $\vec{v}$ ne sont pas colinéaires (composantes non proportionnelles par les produits en croix) donc F est un plan de repère $(a, \vec{u}, \vec{v})$.

Enfin, soient $M = (x, y, z)$ et $M' = (x', y', z')$ des points de F, $\overrightarrow{MM'} = (x - x', y - y', z - z')$ vérifie $a(x - x') + b(y - y') + c(z - z') = 0$ donc la direction $\vec{F}$ de F admet pour équation $ax + by + cz = 0$.

Conclusion : L'ensemble d'équation $ax+by+cz+d = 0$ avec $(a, b, c) \neq (0, 0, 0)$ est un plan dont la direction a pour équation $ax + by + cz = 0$.

Théorème : équations cartésienne de plans parallèles

Soit P et P' des plans de $\mathbb{R}^3$ d'équations $ax + by + cz + d = 0$ et $a'x + b'y + c'z + d' = 0$.
$P \parallel P' \Leftrightarrow (a, b, c)$ et (a', b', c') sont proportionnels.

Démonstration :
Les directions de P et P' ont pour équations $ax + by + cz = 0$ et $a'x + b'y + c'z = 0$.
Donc $P \parallel P'$ si et seulement si ils ont la même direction, autrement dit $ax+by+cz = 0$ et $a'x+b'y+c'z = 0$ sont équivalentes, c'est-à-dire les coefficients de ces deux équations sont proportionnels. (CQFD)

3.5 Droites de $\mathbb{R}^3$

Propriété : équation paramétrique d'une droite de $\mathbb{R}^3$

Toute droite de $\mathbb{R}^3$ admet une équation paramétrique de la forme $\begin{cases} x = x_a + \lambda x_u \\ y = y_a + \lambda y_u \\ z = z_a + \lambda z_u \end{cases}$ de paramètre $\lambda \in \mathbb{R}$ et où $(x_u, y_u, z_u) \neq (0, 0, 0)$.
Inversement, toute partie de $\mathbb{R}^3$ ayant une telle équation paramétrique est une droite de vecteur directeur $\vec{u} = (x_u, y_u, z_u)$ passant par $A = (x_a, y_a, z_a)$.

Démonstration : identique à celle dans $\mathbb{R}^2$.

Propriété : équation cartésienne d'une droite de $\mathbb{R}^3$

Toute droite de $\mathbb{R}^3$ admet une équation cartésienne de la forme (S) : $\begin{cases} ax + by + cz + d = 0 \\ a'x + b'y + c'z + d' = 0 \end{cases}$ avec (a, b, c) et (a', b', c') non proportionnels.
Inversement, toute partie de $\mathbb{R}^3$ admettant une telle équation est une droite D dont la direction $\vec{D}$ admet pour équation le système homogène associé à (S).

Démonstration : Soit D une droite de $\mathbb{R}^3$. Soit $A = (x_a, y_a, z_a)$ un point de D et $\vec{u} = (x_u, y_u, z_u)$ un vecteur directeur. $(x_u, y_u, z_u) \neq (0, 0, 0)$, supposons par exemple que $x_u \neq 0$.
$M = (x, y, z) \in D$ si et seulement si $\overrightarrow{AM}$ est colinéaire à $\vec{u}$,
c'est-à-dire $(x - x_a, y - y_a, z - z_a)$ est proportionnel (x_u, y_u, z_u),
qui équivaut, d'après les produits en croix à : $\begin{cases} y_u(x - x_a) = x_u(y - y_a) \\ z_u(x - x_a) = x_u(z - z_a) \end{cases}$
c.a.d. $\begin{cases} y_u x - x_u y + x_u y_a - y_u x_a = 0 \\ z_u x - x_u z + x_u z_a - z_u x_a = 0 \end{cases}$.

Comme $x_u \neq 0$, $(y_u, -x_u, 0)$ $(z_u, 0, -x_u)$ ne sont pas proportionnels, on a bien une équation de la forme attendue.

Inversement, si une partie F admet une telle équation, $F = P \cap P'$ où P et P' sont les plans d'équations $ax + by + cz + d = 0$ et $a'x + b'y + c'z + d' = 0$. Comme (a, b, c) et (a', b', c') ne sont pas proportionnels, P et P' ne sont pas parallèles donc leur intersection F est une droite.

Chapitre VII

Ordre sur $\mathbb{R}$

1 Ordre sur $\mathbb{R}$ et opérations

Dans cette section, a, b, c, d, x et y sont des réels.

1.2 Compatibilité de l'ordre avec la structure de corps de $\mathbb{R}$, c.a.d avec l'addition et la multiplication des réels

Propriété : $\mathbb{R}$ est un corps ordonné

1) si $x \leqslant y$ alors $x + a \leqslant y + a$.

2) si $x \leqslant y$ et a positif alors $x\,a \leqslant y\,a$.

Remarque : toutes les autres propriétés concernant les opérations sur des inégalités s'en déduisent.
On peut même remplacer l'axiome 2 par l'axiome plus élémentaire 2bis :
si x et y sont positifs alors $x\,y$ est positif.

1.3 Addition sur des encadrements

- Addition d'un réel à un encadrement :
  Si $\quad a \leqslant x \leqslant b \quad$ alors $\quad a + c \leqslant x + c \leqslant b + c$
- Addition membre à membre de deux encadrements :
  Si $\quad a \leqslant x \leqslant b \quad$ et $\quad c \leqslant y \leqslant d \quad$ alors $\quad a + c \leqslant x + y \leqslant b + d$

1.4 Multiplication sur des encadrements

Multiplication d'un encadrement par un réel positif

Si $\quad a \leqslant x \leqslant b \quad$ et $\quad c$ positif $\quad$ alors $\quad c\,a \leqslant c\,x \leqslant c\,b$

Exemple : $-1 \leqslant x \leqslant 2 \;\Rightarrow\; -3 \leqslant 3x \leqslant 6$

Multiplication d'un encadrement par un réel négatif

Si $\quad a \leqslant x \leqslant b \quad$ et $\quad c$ négatif $\quad$ alors $\quad c\,b \leqslant c\,x \leqslant c\,a$

On se ramène au cas où c est positif avec $-c \geqslant 0$.
Exemple : $-1 \leqslant x \leqslant 2 \;\Rightarrow\; -4 \leqslant -2x \leqslant 2$

Multiplication membre à membre de deux encadrements positifs

Si $\quad 0 \leqslant a \leqslant x \leqslant b \quad$ et $\quad 0 \leqslant c \leqslant y \leqslant d \quad$ alors $\quad 0 \leqslant a\,c \leqslant x\,y \leqslant b\,d$

Exemple : $(\frac{1}{2} \leqslant x \leqslant 2 \text{ et } 3 \leqslant y \leqslant 5) \Rightarrow \frac{3}{2} \leqslant x\,y \leqslant 10$

Multiplication membre à membre d'un encadrement positif et d'un encadrement négatif

Si $0 \leqslant a \leqslant x \leqslant b$ et $c \leqslant y \leqslant d \leqslant 0$ alors $b\,c \leqslant x\,y \leqslant a\,d \leqslant 0$

On se ramène au cas de deux encadrements positifs avec $0 \leqslant -d \leqslant -y \leqslant -c$.
Exemple : $(\frac{1}{2} \leqslant x \leqslant 2 \text{ et } -7 \leqslant y \leqslant -5) \Rightarrow -14 \leqslant x\,y \leqslant -\frac{5}{2}$

Multiplication membre à membre de deux encadrements négatifs

Si $a \leqslant x \leqslant b \leqslant 0$ et $c \leqslant y \leqslant d \leqslant 0$ alors $0 \leqslant b\,d \leqslant x\,y \leqslant a\,c$

On se ramène au cas de deux encadrements positifs avec $0 \leqslant -b \leqslant -x \leqslant -a$ et $0 \leqslant -d \leqslant -y \leqslant -c$.

Exemple : $(-5 \leqslant x \leqslant -\frac{1}{3} \text{ et } -3 \leqslant y \leqslant -2) \Rightarrow \frac{2}{3} \leqslant x\,y \leqslant 15$

Remarque : pour un quotient $\dfrac{x}{y}$, il faut d'abord encadrer $\dfrac{1}{y}$ en utilisant le sens de variation de la fonction $t \mapsto \dfrac{1}{t}$ sur $]-\infty, 0[$ ou sur $]0, +\infty[$, puis on encadre le produit $x\,\dfrac{1}{y}$

1.5 Valeur absolue d'un réel

Définitions

Pour tout réel x, la **valeur absolue** de x, notée $\lvert x\rvert$ est définie par $\lvert x\rvert = \max(x, -x)$.

Propriété : distance à 0

Soient des réels x, a et $m \geqslant 0$: $\quad \lvert x-a\rvert \leqslant m \Leftrightarrow a-m \leqslant x \leqslant a+m \Leftrightarrow x \in [a-m, a+m]$.

Remarque : $|x|$ représente la distance de x à 0 et $|x-a|$ la distance de a à x.

On a les propriétés classiques des distances, en particulier l'**inégalité triangulaire**.

Propriété : inégalité triangulaire

Pour tout x et y dans $\mathbb{R}$, $\lvert x+y\rvert \leqslant \lvert x\rvert + \lvert y\rvert$

Corollaire de l'inégalité triangulaire

Pour tout x et y dans $\mathbb{R}$, $\big\lvert \lvert x\rvert - \lvert y\rvert \big\rvert \leqslant \lvert x-y\rvert$

2 Majorants et minorants

Définitions

Soit A une partie **non vide** de $\mathbb{R}$:

- A est **majorée** si et seulement s'il existe un réel M tel que $\forall x \in A,\ x \leqslant M$.
  On dit alors que M **est un majorant de** A.
- A est **minorée** si et seulement s'il existe un réel m tel que $\forall x \in A,\ m \leqslant x$.
  On dit alors que m **est un minorant de** A.
- A **borné** $\Leftrightarrow$ (A majorée) et (A minorée).

Propriété

A est **bornée** si et seulement si $\lvert A\rvert = \{\lvert x\rvert / x \in A\}$ est majorée.

Remarque : A est bornée signifie que la distance entre 0 et tout élément x de A est majorée.

Exemple
Montrer que $A = \left\{\frac{1-n}{1+n} / n \in \mathbb{N}\right\}$ est bornée.

Démonstration
On note $u_n = \frac{1-n}{1+n}$ pour tout $n \in \mathbb{N}$. la question revient à montrer que la suite $(u_n)_{n\in\mathbb{N}}$ est bornée. Pour cela, on peut montrer que la suite converge car c'est une condition suffisante pour qu'elle soit bornée.

On peut aussi le montrer directement.
Considérons $n > 0$, on a $u_n = -\dfrac{1-\frac{1}{n}}{1+\frac{1}{n}}$.
Or $1 < 1+\frac{1}{n} \leqslant 2$ donc $\frac{1}{2} \leq \frac{1}{1+\frac{1}{n}} < 1$ (I_1). De plus $0 \leqslant 1-\frac{1}{n} < 1$ (I_2).
Les inégalités I_1 et I_2 impliquent $0 \leqslant \dfrac{1-\frac{1}{n}}{1+\frac{1}{n}} < 1$ donc que $-1 < u_n \leqslant 0$.
Enfin, $u_0 = 1$ donc A est majoré par 1 et minorée par -1.

3 Plus grand élément, plus petit élément

Définitions

Soit A une partie **non vide** de $\mathbb{R}$:

- A admet un **plus grand élément** si et seulement s'il existe un **majorant de A qui appartient à A**, autrement dit s'il existe un réel $a \in A$ tel que $\forall x \in A,\ x \leqslant a$.
  a est alors **unique** et s'appelle **le plus grand élément de A**, notée $\max(A)$.
- A admet un **plus petit élément** si et seulement s'il existe un **minorant de A qui appartient à A**, autrement dit s'il existe un réel $b \in A$ tel que $\forall x \in A,\ x \geqslant b$.
  b est alors **unique** et s'appelle **le plus petit élément de A**, notée $\min(A)$.

Démonstration de l'unicité
Supposons par exemple que a et a' sont des plus grand élément de A. Comme a et a' appartiennent à A, a majore a', c'est-à-dire $a \geqslant a'$, et inversement, donc $a = a'$.

Exemple
$A = \{\frac{1-n}{1+n} / n \in \mathbb{N}\}$ admet-il un plus grand élément, un plus petit élément ?
Démonstration
On a montré précédemment que $1 = \frac{1-0}{1+0} \in A$ et 1 majore A donc $\max(A) = 1$.
On montre que A n'admet pas de plus petit élément, autrement dit que $\min(A)$ n'existe pas. Pour cela on montre qu'aucun élément de A ne minore A en utilisant que $\left(\frac{1-n}{1+n}\right)$ est une suite décroissante.

Soit $x \in A$ quelconque, il existe n tel que $x = \frac{1-n}{1+n}$.
On pose $x' = \frac{1-(n+1)}{1+(n+1)}$, on a $x' \in A$.
$x' - x = \frac{-n}{2+n} - \frac{1-n}{1+n} = \frac{-n(1+n)-(1-n)(2+n)}{(1+n)(2+n)} = \frac{-n-n^2-2-n+2n+n^2}{(1+n)(2+n)} = \frac{-2}{(1+n)(2+n)}$.
Donc $x' < x$ ce qui prouve que x ne minore pas A.

Théorème : parties finies de $\mathbb{R}$

Toute partie finie de $\mathbb{R}$ (c'est-à-dire de cardinal fini) admet **un plus grand et un plus petit élément**.

Comme il y a un nombre fini d'éléments, il est toujours possible de les comparer deux à deux et de déterminer ainsi le plus petit et le plus grand.

4 Borne sup et borne inf

Définitions

Soit A une partie **non vide** de $\mathbb{R}$:

- A admet une **borne supérieure** si et seulement s'il existe **un plus petit des majorants** de A, autrement dit,
  s'il existe un majorant S de A tel que tout majorant M de A vérifie $S \leqslant M$.
  S est alors **unique** et s'appelle **borne supérieure** de A, **notée** $\sup(A)$.
- A admet une **borne inférieure** si et seulement s'il existe **un plus grand des minorants** de A, autrement dit,
  s'il existe un minorant s de A tel que tout minorant m de A vérifie $s \geqslant m$.
  s est alors **unique** et s'appelle **borne inférieure** de A, **notée** $\inf(A)$.

L'unicité découle de l'unicité du max *et du* min.

Remarque : pour un intervalle, les bornes correspondent aux définitions ci-dessus. Par exemple pour $A =]1, 3]$, 1 est le plus grand des minorants de A et 3 est le plus petit des majorants de A.

Propriété caractéristique

Soit A une partie non vide de $\mathbb{R}$, s et S des réels :

- $S = \sup(A) \Leftrightarrow \begin{cases} S \text{ majore } A \\ \text{Pour tout } \varepsilon > 0, \text{ il existe } x \in A \text{ tel que } S - \varepsilon < x \end{cases}$
- $s = \inf(A) \Leftrightarrow \begin{cases} s \text{ minore } A \\ \text{Pour tout } \varepsilon > 0, \text{ il existe } x \in A \text{ tel que } x < s + \varepsilon \end{cases}$

Démonstration : cette formulation signifie que tout nombre strictement inférieur à S n'est pas un majorant de A ce qui est bien équivalent à (S est le plus petit des majorants de A).

Corollaire

Soit A une partie non vide de $\mathbb{R}$, m et M des réels :

- si M majore A et $M \in A$, autrement dit si $M = \max(A)$, alors A admet une borne supérieure et $\sup(A) = M$.
- si m minore A et $m \in A$, autrement dit si $m = \min(A)$, alors A admet une borne inférieure et $\inf(A) = m$.

Démonstration : il suffit d'appliquer la propriété caractéristique précédente.
Par exemple si M majore A et $M \in A$ alors $\forall \varepsilon > 0$, $x = M$ vérifie $x \in A$ et $S - \varepsilon < x$.

Exemple
Montrer que $A = \{\frac{1-n}{1+n} / n \in \mathbb{N}\}$ admet une borne supérieur et une borne inférieure, donner leur valeur.

On montre d'abord que $\sup(A) = 1$. D'après la propriété précédente, cela découle de $\max(A) = 1$.

On montre ensuite que $\inf(A) = -1$.
On note que $\lim \frac{1-n}{1+n} = -1$ mais que $-1 \notin A$.
D'après la question précédente, -1 minore A.
Soit $\varepsilon > 0$. On veut montrer que $-1 + \varepsilon$ n'est pas un minorant de A, c'est-à-dire qu'il existe $n \in \mathbb{N}$ tel que $u_n < -1 + \varepsilon$ qui s'écrit $\dfrac{1-n}{1+n} < -1 + \varepsilon$.

Or $\dfrac{1-n}{1+n} < -1 + \varepsilon \Leftrightarrow \dfrac{1-n}{1+n} + 1 = \dfrac{2}{1+n} < \varepsilon \Leftrightarrow 1 + n > \dfrac{2}{\varepsilon}$.

On choisit un entier n_0 tel que $n_0 > \frac{2}{\varepsilon} - 1$, on a $u_{n_0} < -1 + \varepsilon$. (CQFD)

Conclusion : -1 est le plus grand des minorants de A, c'est-à-dire $\inf(A) = -1$.

Théorème fondamental : complétude de $\mathbb{R}$

Toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure.
Toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure.

Remarque : cette propriété n'est pas vraie dans $\mathbb{Q}$. Par exemple $\{x \in \mathbb{Q}/x < \sqrt{2}\}$ est majorée dans $\mathbb{Q}$ (par exemple par 2) mais n'admet pas de borne supérieure dans $\mathbb{Q}$. Cela se comprend intuitivement car la borne supérieure dans $\mathbb{R}$ est $\sqrt{2} \notin \mathbb{Q}$.

Démonstration de l'incomplétude de $\mathbb{Q}$:
L'ensemble $A := \{r \in \mathbb{Q}/r^2 < 2\}$ n'est pas vide, est majoré dans $\mathbb{Q}$ mais n'admet pas de borne supérieure dans $\mathbb{Q}$.

1) A **contient le rationnel 1** donc il n'est pas vide.

2) A **est majoré** par le rationnel 2.
Par l'absurde, supposons l'existence de $x \in A$ tel que $x > 2$. Alors $x^2 > 4$ ce qui contredit $x \in A$.

3) Montrons d'abord que A **n'a pas de maximum**.
Par l'absurde : supposons $r \in A$ qui majore A. Comme $1 \in A$, nécessairement $r \geqslant 1$ donc $r > 0$.
On note $\varepsilon = 2 - r^2$. On a $\varepsilon > 0$.
Pour tout $n \in \mathbb{N}^*$, on note $r_n = r + \dfrac{1}{n}$. On a $r_n > r$ pour tout n. On va choisir n pour avoir $r_n \in A$.
$r_n^2 < 2 \Leftrightarrow r^2 + \dfrac{2r}{n} + \dfrac{1}{n^2} < 2 \Leftrightarrow \dfrac{2r}{n} + \dfrac{1}{n^2} < 2 - r^2 = \varepsilon$. (1)
On choisit un entier $n_0 > \dfrac{4r}{\varepsilon} > 0$, alors pour tout entier $n \geqslant n_0$, $n > \dfrac{4r}{\varepsilon}$ donc $\dfrac{2r}{n} < \dfrac{\varepsilon}{2}$. (2)
On choisit un entier $n_1 \geqslant n_0 \geqslant 1$ tel que $n_1 > \dfrac{2}{\varepsilon}$. Alors $n_1^2 \geqslant n_1 > \dfrac{2}{\varepsilon}$ donc $\dfrac{1}{n_1^2} < \dfrac{\varepsilon}{2}$. (3)
D'après les inégalités (2) et (3), on a $\dfrac{2r}{n_1} + \dfrac{1}{n_1^2} < \dfrac{\varepsilon}{2} + \dfrac{\varepsilon}{2} = \varepsilon$ c.a.d. l'inégalité (1).
Il suit que $r_{n_1} \in A$ puisque c'est un rationnel qui vérifie $r_{n_1}^2 < 2$. Comme il majore strictement r, cela contredit que r est le maximum de A. (CQFD)

4) A **n'admet pas de borne supérieure dans** $\mathbb{Q}$. On montre par l'absurde que l'ensemble des majorants de A n'a pas de minimum.
Supposons qu'il existe un rationnel r qui soit le minimum des majorants rationnels de A.
Comme A n'a pas de maximum, le majorant $r \notin A$ donc $r^2 \geqslant 2$. De plus $r \geqslant 1 > 0$ car $1 \in A$.
En outre, il n'y pas de solution rationnelle à l'équation $x^2 = 2$ (démonstration vue au lycée), donc $r^2 > 2$.
On note $\varepsilon = r^2 - 2$. On a $\varepsilon > 0$.
On fait un raisonnement semblable au précédent avec la suite de rationnels $r'_n = r - \dfrac{1}{n}$.
${r'_n}^2 > 2 \Leftrightarrow r^2 - \dfrac{2r}{n} + \dfrac{1}{n^2} > 2 \Leftrightarrow \dfrac{2r}{n} - \dfrac{1}{n^2} < r^2 - 2 = \varepsilon$. (1)
On choisit un entier $n_0 > \dfrac{2r}{\varepsilon} > 0$, alors pour tout entier $n \geqslant n_0$, $n > \dfrac{2r}{\varepsilon}$ donc $\dfrac{2r}{n} < \varepsilon$ et a frotiori $\dfrac{2r}{n} - \dfrac{1}{n^2} < \varepsilon$ c.a.d. l'inégalité (1).
On choisit un entier $n_1 \geqslant n_0$ tel que $n_1 > \dfrac{1}{r} > 0$, on a alors $r'_{n_1} = r - \dfrac{1}{n_1} > 0$.
On a donc $r'_{n_1} > 0$ et ${r'_n}^2 > 2$. On en déduit que r'_{n_1} majore A. Par l'absurde : supposons $x \in A$ qui vérifie $x > r'_{n_1} > 0$ alors $x^2 > {r'}^2_{n_1} > 2$ ce qui contredit $x \in A$.
Finalement r'_{n_1} est un majorant de A strictement inférieur à r, ce qui contredit $r = \sup(A)$.

5 Partie entière d'un réel

Propriété axiomatique de $\mathbb{N}$

Toute ensemble d'entiers non vide et majoré admet un plus grand élément.

Remarque : c'est un des axiomes qui définissent $\mathbb{N}$.

Définition

Pour tout réel x, on appelle partie entière de x notée $\mathrm{E}(x)$ ou $\lfloor x \rfloor$, le plus grand entier $n \leqslant x$, autrement dit $\mathrm{E}(x) = \max\{n \in \mathbb{Z} \,|\, n \leqslant x\}$.

Justification : Pour tout $x \in \mathbb{R}$, l'ensemble $\{n \in \mathbb{Z} \,|\, n \leqslant x\}$ est un ensemble d'entiers non vide et majoré.

Théorème

- Pour tout réel x, la partie entière de x est l'unique entier n tel que $n \leqslant x < n+1$.
- Pour tout réel x, la partie entière de x est l'unique entier n tel que $x - 1 < n \leqslant x$.

6 Intervalles de $\mathbb{R}$

Définition d'un segment

Soit $x \leqslant y$ des réels, on définit le segment $[x, y]$ par $[x, y] := \{a \in \mathbb{R} | x \leqslant a \leqslant y\}$

Définition d'un intervalle

Une partie I de $\mathbb{R}$ est un intervalle si et seulement si $\forall x, y \in I$ tels que $x < y, [x, y] \subset I$.

Remarques :

- Cette propriété s'appelle la **convexité**. Elle implique ici que I est "d'un seul tenant".
- L'ensemble vide vérifie cette propriété donc $\emptyset$ est un intervalle.

Définition d'un intervalle ouvert

Soit I un intervalle de $\mathbb{R}$, I est ouvert si et seulement si pour tout $x \in I$, il existe un intervalle ouvert centré sur x inclus dans I, autrement dit :
Pour tout $x \in I$, $\exists \varepsilon > 0$ tel que $]x - \varepsilon, x + \varepsilon[\subset I$.

Remarque : cette propriété caractérise plus généralement les sous-ensembles ouverts de $\mathbb{R}$, concept fondamentale de l'Analyse.

Exemple : l'intervalle $]1, 3]$ ne vérifie pas cette propriété en 3.
En effet, pour tout $\varepsilon > 0$, $3 + \frac{\varepsilon}{2} \in]x - \varepsilon, x + \varepsilon[$ mais $3 + \frac{\varepsilon}{2} \notin]1, 3]$ donc $]x - \varepsilon, x + \varepsilon[$ n'est pas inclus dans $]1, 3]$.

7 Voisinage

Définition

Soient x un réel et A une partie de $\mathbb{R}$, on dit que A est un voisinage de x si et seulement si :
$\exists \varepsilon > 0$ tel que $]x - \varepsilon, x + \varepsilon[\subset A$.

Remarques :

- Un voisinage de x contient x.
- Un intervalle ouvert est un voisinage de chacun de ses points.

Exemple : l'intervalle $]1, 3]$ n'est pas un voisinage de 3 mais c'est un voisinage de tous ses autres points.

8 Densité dans $\mathbb{R}$

Définition

Soit A une partie de $\mathbb{R}$. On dit que A est dense dans $\mathbb{R}$ si et seulement si, pour tous $x < y$ dans $\mathbb{R}$, il existe $a \in A$ tel que $x < a < y$.

Définition

On appelle rationnel tout élément de $\mathbb{Q}$, c'est-à-dire tout réel x qui peut s'écrire $x = \frac{n}{q}$ avec $n \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. On appelle irrationnel tout élément de $\mathbb{R} - \mathbb{Q}$ (le complémentaire de $\mathbb{Q}$ dans $\mathbb{R}$), c'est-à-dire tout réel qui ne peut pas s'écrire comme une fraction d'entiers.

Propriété

$\sqrt{2}$ est irrationnel donc $\mathbb{Q} \subset \mathbb{R}$ est une inclusion stricte.

Théorème

$\mathbb{Q}$ est dense dans $\mathbb{R}$, c'est-à-dire qu'il y a toujours un rationnel entre deux réels distincts.

Démonstration

Soit $x < y$ deux réels.

Considérons la suite de rationnels (r_n) définie par $\forall n \in \mathbb{N}^*, r_n = \dfrac{\mathrm{E}(nx) + 1}{n}$.

Soit $n \in \mathbb{N}^*$, on a l'encadrement, $nx - 1 < \mathrm{E}(nx) \leqslant nx$ donc $nx < \mathrm{E}(nx) + 1 \leqslant nx + 1$ et finalement $x < r_n \leqslant x + \frac{1}{n}$ (1).

En prenant un entier $n_0 > \frac{1}{y-x}$, par exemple $n_0 = \mathrm{E}(\frac{1}{y-x}) + 1$, l'encadrement (1) donne
$x < r_{n_0} \leqslant x + \frac{1}{n_0} < x + (y - x) = y$.

r_{n_0} est un rationnel de l'intervalle $]x, y[$.

Théorème

$\mathbb{R} - \mathbb{Q}$ est dense dans $\mathbb{R}$, c'est-à-dire qu'il y a toujours un irrationnel entre deux réels distincts.

Démonstration

Soit $x < y$ deux réels.

On applique le théorème précédent à $]x - \sqrt{2}, y - \sqrt{2}[$: il existe un rationnel r tel que
$x - \sqrt{2} < r < y - \sqrt{2}$.

On pose $t = \sqrt{2} + r$. On a $x < t < y$ et t est irrationnel, sinon $\sqrt{2} = t - r$ serait rationnel car la différence de deux rationnels est un rationnel (CQFD).

Chapitre VIII

Suites numériques

1 Généralités

1.2 Définition

Une **suite** réelle (resp. complexe) est une **application** $u : \mathbb{N} \to \mathbb{R}$ (resp. $\mathbb{N} \to \mathbb{C}$).
Pour tout entier, l'image $u(n)$, notée u_n, est appelée **terme de rang** n (ou d'indice n) de la suite u.
La suite peut débuter au rang $n_0 \in \mathbb{N}$, l'ensemble de départ de u est alors $\{n \in \mathbb{N}/n \geqslant n_0\}$.
La suite est notée u, $(u_n)_{n\in\mathbb{N}}$, $(u_n)_{n\geqslant n_0}$ si elle commence au rang n_0, ou simplement (u_n).

Dans ce cours, certaines parties ne concernent que les suites réelles et d'autres les suites réelles et complexes. Cela sera précisé à chaque fois au début de la section.

Remarque : dans le souci d'alléger l'écriture, nous omettrons parfois de préciser que n est un entier.

1.3 Suites extraites

Soient $(u_n)_{n\in\mathbb{N}}$ une suite et $\varphi : \mathbb{N} \to \mathbb{N}$ une application strictement croissante, la suite $(u_{\varphi(n)})_{n\in\mathbb{N}}$ est appelée **suite extraite** de (u_n).
NB : φ est strictement croissante si et seulement si $\forall n \in \mathbb{N}$, $\varphi(n+1) > \varphi(n)$.

Remarque
φ sélectionne certains termes en conservant l'ordre des rangs.

A contrario, $(u_4, u_3, u_8, u_7, u_{12}, u_{11}, etc.)$ n'est pas une suite extraite de la suite $(u_n)_{n\in\mathbb{N}}$ car l'ordre des rangs n'a pas été respecté : $\varphi(1) = 3 < \varphi(0) = 4$ ce qui suffit pour conclure. Mais on a aussi $\varphi(3) = 7 < \varphi(2) = 8$, etc..

Exemples classiques
$(u_{2n})_{n\in\mathbb{N}}$ est la **suite extraite des termes de rangs pairs** ($\varphi : n \mapsto 2n$).

$(u_{2n+1})_{n\in\mathbb{N}}$ est la **suite extraite des termes de rangs impairs** ($\varphi : n \mapsto 2n+1$).

1.4 Rappels sur les suites réelles

Definition : suite positive

Une suite réelle est **positive** (resp. **négative**) si tous ses termes sont positifs (resp. négatifs).

Definition : suite majorée, minorée, bornée

Une suite réelle est **majorée** (resp. **minorée**, **bornée**) si l'ensemble $u(\mathbb{N}) = \{u(n), n \in \mathbb{N}\}$ est majoré (resp. minoré, borné).

Definition : suite monotone

- Une suite réelle est **croissante** si deux termes quelconques sont dans le même ordre que leurs rangs : $\forall n,\, n' \in \mathbb{N}, \quad n \leqslant n' \;\Rightarrow\; u_n \leqslant u_{n'}$.
- Une suite réelle est **décroissante** si deux termes quelconques sont dans l'ordre inverse de leurs rangs : $\forall n,\, n' \in \mathbb{N}, \quad n \leqslant n' \;\Rightarrow\; u_n \geqslant u_{n'}$.
- Une suite réelle est **monotone** si elle est croissante ou décroissante : $\big(\forall n,\, n' \in \mathbb{N}, \quad n \leqslant n' \;\Rightarrow\; u_n \leqslant u_{n'}\big)$ OU $\big(\forall n,\, n' \in \mathbb{N}, \quad n \leqslant n' \;\Rightarrow\; u_n \leqslant u_{n'}\big)$.
- Ces définitions s'étendent au sens strict (strictement croissante, strictement décroissante, strictement monotone) en passant au sens strict toutes les inégalités.
  Par exemple, une suite réelle est **strictement croissante** si : $\forall n,\, n' \in \mathbb{N}, \quad n < n' \;\Rightarrow\; u_n < u_{n'}$.

Caractérisation d'une suite monotone

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle :

- (u_n) **croissante** $\Leftrightarrow \quad \forall n \in \mathbb{N},\, u_{n+1} \geqslant u_n$.
- (u_n) **décroissante** $\Leftrightarrow \quad \forall n \in \mathbb{N},\, u_{n+1} \leqslant u_n$.
- La croissance ou la décroissance est stricte si l'inégalité est stricte pour tout n.

Démonstration pour la croissance
$LHS \;\Rightarrow\; RHS$: si u est croissante, pour tout n, $n+1 \geqslant n$ donc $u_{n+1} \geqslant u_n$.
$RHS \;\Rightarrow\; LHS$: soient n et n' quelconques tels que $n \leqslant n'$, on a
$u_n \leqslant u_{n+1} \leqslant \ldots \leqslant u_{n'-1} \leqslant u_{n'}$ donc $u_n \leqslant u_{n'}$.

Caractérisation d'une suite monotone strictement positive

Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle **strictement positive** :

- (u_n) **croissante** $\Leftrightarrow \quad \forall n \in \mathbb{N},\, \frac{u_{n+1}}{u_n} \geqslant 1$.
- (u_n) **décroissante** $\Leftrightarrow \quad \forall n \in \mathbb{N},\, \frac{u_{n+1}}{u_n} \leqslant 1$.
- La croissante ou la décroissance est stricte si l'inégalité est stricte.

Démonstration pour la croissance
Pour tout n, comme u_n est strictement positif, $u_{n+1} \geqslant u_n \;\Leftrightarrow\; \frac{u_{n+1}}{u_n} \geqslant 1$.

1.5 Premières propriétés des suites complexes

Nous ne disposons pas de relation d'ordre sur $\mathbb{C}$ compatible avec la structure de corps (cf. chap précédent) mais nous disposons du module qui joue le même rôle que la valeur absolue dans $\mathbb{R}$.

Que reste-t-il des définitions de la section précédente ?

Opérations sur les suites complexes

- **somme** : $u + v = (u_n + v_n)$.
- **produit** : $u\,v = (u_n\, v_n)$
- **multiplication par un scalaire** : $\lambda u = (\lambda u_n)$ où $\lambda \in \mathbb{C}$.

Definition : suite bornée

Une suite complexe (u_n) est **bornée** si et seulement si l'ensemble $\{|u(n)|, n \in \mathbb{N})\}$ est majoré, autrement dit (u_n) est bornée si et seulement si la suite réelle $(|u_n|)$ est majorée.

Remarque
Si (u_n) est une suite réelle, cette définition est bien équivalente à celle donnée précédemment.

Théorème

Si une suite complexe (u_n) est **bornée à partir d'un certain rang** alors elle est **bornée**.

Démonstration qui vaut a fortiori pour le cas des suites réelles.
Si (u_n) est bornée à partir d'un certain rang noté N, il existe un majorant M pour $\{|u_n|/n \geqslant N\}$.
D'autre part, l'ensemble $\{|u_0|, \ldots, |u_{N-1}|\}$ est fini, donc il admet un plus grand élément M'.
On note $M'' = \max(M', M)$. $(|u_n|)$ est majorée par M'' donc (u_n) est bornée.

2 Suite convergente

La section 2 s'applique aux suites complexes (les suites réelles sont un cas particulier).

2.2 Exemples de suites à étudier

Dans les exempmles suivants, la suite (u_n) est-elle convergente ? Admet-elle une limite infinie ? Ou n'admet-elle aucune limite ?

Exemple 1
$u_n = \sqrt[n]{n}$ pour tout entier $n \geqslant 1$.

Exemple 2 : série harmonique
$u_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k}$ pour tout entier $n \geqslant 1$.

Exemple 3
$u_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k^2}$ pour tout entier $n \geqslant 1$.

Exemple 4 : exponentielle
$u_n = \displaystyle\sum_{k=0}^{n} \frac{x^k}{k!}$ pour tout entier n, avec $x \in \mathbb{C}$.

Exemple 5 : moyenne de Césaro
$u_n = \frac{v_0+v_1+\ldots v_n}{n+1}$ pour tout entier n, où (v_n) est une suite complexe.
v_n est la moyenne arithmétique des n+1 premiers termes de (u_n).

Exemple 6 : suite définie par une récurrence $u_{n+1} = f(u_n)$ où f est une fonction homographique
$u_0 = \frac{1}{2}$ puis pour tout entier n, $u_{n+1} = \dfrac{4u_n + 5}{u_n + 3}$. On peut s'intéresser aussi au cas $u_0 = i$.

Exemple 7 : approximation d'une racine carrée par la méthode d'Héron d'Alexandrie
$u_0 = 1$ puis pour tout entier n, $u_{n+1} = \dfrac{u_n + \frac{a}{u_n}}{2}$ où a est un réel.

Exemple 8 : suite définie par une récurrence de la forme $u_{n+1} = f(u_n)$
$u_0 = 0$ puis pour tout entier n, $u_{n+1} = \cos(u_n)$.

Exemple 9 : suite de Fibonacci
$u_0 = 0$, $u_1 = 1$ puis pour tout entier n, $u_{n+2} = u_n + u_{n+1}$. On s'intéresse aussi à la suite (v_n) définie par $v_n = \dfrac{u_{n+1}}{u_n}$ pour tout entier $n \geqslant 1$.

Exemple 10 : suite de Syracuse
$u_0 = p$ quelconque dans $\mathbb{N}$, puis pour tout n, $u_{n+1} = u_n/2$ si u_n est pair et $u_{n+1} = 3u_n + 1$ si u_n est impair.

Exemple 11
Pour tout entier $n \geqslant 1$, on considère le polynôme $P_n(x) = x^n + x^{n-1} + \cdots + x - 1$.
Comme $P_n(0) = -1$ et $P_n(1) = n - 1 \geqslant 0$, P_n étant continu, le théorème des valeurs intermédiaires permet d'affirmer qu'il existe au moins une racine de P_n dans $[0, 1]$. En dérivant P_n, on montre facilement que P_n est strictement croissant sur $\mathbb{R}^+$. Il suit que P_n admet une racine unique dans $[0, 1]$ que l'on note u_n.

On a défini ainsi une suite (u_n) que l'on veut étudier.

2.3 Définitions

Definition : suite convergente

Soit $l \in \mathbb{C}$, la suite (u_n) **converge vers** l si et seulement si :
Pour tout réel $\varepsilon > 0$, il existe un entier N tel que $(\forall n \geqslant N,\ |u_n - l| < \varepsilon)$
Autrement dit, aussi petit que soit $\varepsilon > 0$, à partir d'un certain rang N, tous les termes de (u_n) sont à une distance de l inférieure à ε.
On dit aussi que (u_n) admet pour limite l.

Remarque : pour les suites réelles, la seule différence dans la définition est que $l \in \mathbb{R}$.

Exemple 1

Montrer que la suite $(u_n)_{n\in\mathbb{N}}$ définie pour tout n par $u_n = \dfrac{1-n}{1+n}$ converge vers -1.

Démonstration
Soit une réel $\varepsilon > 0$, on cherche N tel que $(\forall n \geqslant N,\ |u_n + 1| < \varepsilon)$.

Il faut trouver une majoration simple de $|u_n + 1|$ qui permette de conclure à l'existence de N.

On calcule $u_n + 1 = \frac{1-n}{1+n} + 1 = \frac{(1-n)+(1+n)}{1+n} = \frac{2}{1+n}$. Donc $|u_n + 1| = \frac{2}{1+n}$ pour tout n.

On en déduit que $\frac{2}{1+n} < \varepsilon \ \Rightarrow\ |u_n + 1| < \varepsilon$. Or $\frac{2}{1+n} < \varepsilon \ \Leftrightarrow\ \frac{2}{\varepsilon} - 1 < n$.

En choisissant $N \in \mathbb{N}$ tel que $N > \frac{2}{\varepsilon} - 1$, ce qui est toujours possible (par exemple $N = \lfloor \frac{2}{\varepsilon} - 1 \rfloor + 1$), on a :

Pour tout $n \geqslant N$, $n > \frac{2}{\varepsilon} - 1$ donc $|u_n + 1| < \varepsilon$.

On a fait ce raisonnement pour $\varepsilon > 0$ quelconque, on a donc démontré que (u_n) converge vers -1.

Exemple 2

Montrer que la suite $(v_n)_{n\in\mathbb{N}}$ définie pour tout n par $v_n = \dfrac{2\,e^{i\,n}}{3+n}$ converge vers 0.

Démonstration
Soit une réel $\varepsilon > 0$, on cherche N tel que $(\forall n \geqslant N,\ |v_n - 0| < \varepsilon)$.

Il faut trouver une majoration simple de $|v_n|$ qui permette de conclure à l'existence de N.

On calcule $|v_n - 0| = \frac{2}{3+n}$. Or $\frac{2}{3+n} < \varepsilon \ \Leftrightarrow\ \frac{2}{\varepsilon} - 3 < n$.

Donc $n > \frac{2}{\varepsilon} - 3 \ \Rightarrow\ |v_n| < \varepsilon$.

En choisissant $N \in \mathbb{N}$ tel que $N > \frac{2}{\varepsilon} - 3$, (par exemple $N = \lfloor \frac{2}{\varepsilon} - 3 \rfloor + 1$), on a :

Pour tout $n \geqslant N$, $n > \frac{2}{\varepsilon} - 3$ donc $|v_n| < \varepsilon$. (CQFD)

Propriété : unicité de la limite

Si une suite (u_n) est convergente, alors sa **limite est unique** et on la note $\lim u_n$.

Démonstration
Supposons (u_n) admette pour limite l et l'. Par définition, pour tout réel $\varepsilon > 0$, il existe deux entiers N et N' tels que $(\forall n \geqslant N,\ |u_n - l| < \varepsilon)$ et $(\forall n \geqslant N',\ |u_n - l'| < \varepsilon)$.

On pose $N_1 = \max(N, N')$. D'après l'inégalité triangulaire, pour tout $n \geqslant N_1$,
$|l - l'| = |(l - u_n) + (u_n - l')| \leqslant |u_n - l| + |u_n - l'| < 2\varepsilon$.

On peut ensuite raisonner par l'absurde ne supposant $l \neq l'$ ou bien continuer ainsi :

Comme 2ε est quelconque dans $]0, +\infty[$, on en déduit que $|l - l'|$ est un minorant de $]0, +\infty[$,
donc $|l - l'| \leqslant 0$.

On en conclut que $|l - l'| = 0$ qui implique $l = l'$.

Définition : suite divergente

On dit que (u_n) est **divergente** si et seulement si elle n'est pas convergente.

2.4 Convergence des suites extraites d'une suite convergente

Théorème

Si la suite (u_n) est convergente vers l, alors **toutes ses suites extraites convergent vers** l.

Par contraposée, si une suite extraite ne converge pas, ou si deux suites extraites, par exemple (u_{2n}) et (u_{2n+1}), n'admettent pas la même limite, alors (u_n) ne converge pas.

Exercice : démontrer ce théorème.

Théorème

(u_n) converge si et seulement si les suites extraites (u_{2n}) et (u_{2n+1}) converge vers la même limite l.

Exercice : démontrer ce théorème.

2.5 Propriétés immédiates

Théorème

Soit $l \in \mathbb{C}$, $\lim u_n = l \ \Leftrightarrow\ \lim(u_n - l) = 0 \ \Leftrightarrow\ \lim|u_n - l| = 0$.

En particulier $\lim u_n = 0 \ \Leftrightarrow\ \lim|u_n| = 0$.

Démonstration
Les définitions de $\lim u_n = l$, $\lim(u_n - l) = 0$ et $\lim|u_n - l| = 0$ sont identiques.

Théorème

Si (u_n) est **convergente** alors elle est **bornée**.

Démonstration
On note $\lim(u_n) = l$. En appliquant la définition de $\lim(u_n) = l$ avec $\varepsilon = 1$, on sait qu'il existe N tel que $\forall n \geqslant N$, $|u_n - l| < 1$, i.e. $l - 1 < u_n < l + 1$.

Donc (u_n) est bornée à partir d'un certain rang, ce qui implique qu'elle est bornée (cf. page 57).

Théorème

Soit $l \in \mathbb{C}$, $\lim u_n = l \ \Rightarrow\ \lim|u_n| = |l|$ (la réciproque est fausse)

Démonstration
D'après l'inégalité triangulaire, pour tout $n \in \mathbb{N}$, $||u_n| - |l|| \leqslant |u_n - l|$.

Donc pour tout $\varepsilon > 0$, $|u_n - l| < \varepsilon \Rightarrow ||u_n| - |l|| < \varepsilon$, d'où, en revenant aux définitions,
$\lim u_n = l \Rightarrow \lim |u_n| = |l|$.

3 Limite infinie

La section 3 s'applique uniquement aux suites réelles.

3.2 Définitions

Définition : limite $+\infty$

La suite (u_n) **admet pour limite** $+\infty$ si et seulement si :
Pour tout réel $A > 0$, il existe un entier N tel que $(\forall n \geqslant N,\ u_n > A)$

Autrement dit, aussi proche de $+\infty$ que soit $A > 0$, à partir d'un certain rang N, tous les termes de (u_n) sont supérieurs à A.

Définition : limite $-\infty$

La suite (u_n) **admet pour limite** $-\infty$ si et seulement si :
Pour tout réel $A < 0$, il existe un entier N tel que $(\forall n \geqslant N,\ u_n < A)$

Autrement dit, aussi proche de $-\infty$ que soit $A < 0$, à partir d'un certain rang N, tous les termes de (u_n) sont inférieurs à A.

NB : (u_n) admet pour limite $-\infty$ équivaut à $(-u_n)$ admet pour limite $+\infty$.

Exemple
Montrer que la suite $(a_n)_{n\in\mathbb{N}}$ définie pour tout n par $a_n = \frac{1+n}{2+\cos n}$ admet pour limite $+\infty$.

Démonstration
Soit une réel $A > 0$, on cherche N tel que $(\forall n \geqslant N,\ u_n > A)$.

Il faut trouver un encadrement simple de u_n qui permette de conclure à l'existence de N.

Pour tout $n \in \mathbb{N}$, $1 \leqslant 2 + \cos n \leqslant 3$ donc $\frac{1}{3} \leqslant \frac{1}{2+\cos n} \leqslant 1$ et $u_n \geqslant \frac{1+n}{3}$.

On en déduit que $\frac{1+n}{3} > A \Rightarrow u_n > A$. Or $\frac{1+n}{3} > A \Leftrightarrow n > 3A - 1$.

Donc en choisissant $N \in \mathbb{N}$ tel que $N > 3A - 1$, ce qui est toujours possible (d'après la propriété d'Archimède), on a pour tout $n \geqslant N$, $n > 3A - 1$ donc $u_n > A$.

On a fait ce raisonnement pour $A > 0$ quelconque, on a donc démontré que (u_n) tend vers $+\infty$.

Propriété : unicité de la limite

Si une suite admet une limite infinie, cette **limite est unique** et on la note $\lim u_n$.

Démonstration pour $+\infty$

- Supposons que (u_n) admette pour limite $+\infty$ et une limite réelle l. Si (u_n) converge, elle est bornée, notons M un majorant de (u_n). Par définition de $\lim u_n = +\infty$, il existe N tel que $\forall n \geqslant N,\ u_n > M$. En particulier $u_N > M$ contradictoire avec M majore (u_n).
- Supposons que (u_n) admette pour limite $+\infty$ et $-\infty$.
  Par définition de $\lim u_n = +\infty$, il existe N tel que $\forall n \geqslant N,\ u_n > 0$.
  Par définition de $\lim u_n = -\infty$, il existe N' tel que $\forall n \geqslant N',\ u_n < 0$.
  Posons $N" = \max(N, N')$. On a donc $u_{N''} < 0 < u_{N''}$ qui est une contradiction.

Corollaire

Si $\lim u_n$ est infinie alors (u_n) diverge.
NB : la réciproque est fausse.

Démonstration
D'après le théorème précédent, (u_n) ne peut pas avoir en même temps une limite finie et une limite infinie.

Théorème

Si $\lim u_n$ est infinie alors (u_n) n'est pas bornée.
NB : la réciproque est fausse.

Démonstration pour $+\infty$
Par l'absurde : supposons (u_n) bornée et $\lim u_n = +\infty$.

Notons $M \in \mathbb{R}^+$ un majorant de la suite $(|u_n|)$. Par définition, de $\lim u_n = +\infty$, il existe N tel que pour $n \geqslant N$, $u_n > M$. On en déduit en particulier que $|u_N| > M$ ce qui est contradictoire M majorant de $(|u_n|)$.

3.3 Suites extraites

Théorème

Soit $a = +\infty$ ou $a = -\infty$. Si la suite (u_n) **admet pour limite** a, alors **toutes ses suites extraites admettent une limite** et cette limite est a.

Remarque : on utilise couramment la contraposée.

Démonstration en revenant à la définition d'une limite infinie.

4 Théorèmes fondamentaux sur les limites de suites

4.2 Opérations sur des suites convergentes

La section 4.1 s'applique aux suites complexes (les suites réelles sont un cas particulier).

Théorème

Soient (u_n) et (v_n) deux suites convergentes.

1) Si $\lim u_n = l$ et $\lambda \in \mathbb{C}$ alors $\lim \lambda u_n = \lambda l$.

2) Si $\lim u_n = l$ et $\lim v_n = l'$ alors $\lim u_n + v_n = l + l'$ et $\lim u_n v_n = l\, l'$.

3) Si $\lim u_n = l$ et $l \neq 0$ alors $\lim \dfrac{1}{u_n} = \dfrac{1}{l}$.

Démonstrations
Il faut revenir aux définitions et procéder par découpage. Montrons par exemple que $\lim u_n v_n = l\, l'$.

Soit n quelconque, d'après l'inégalité triangulaire
$|u_n v_n - l\, l'| = |v_n(u_n - l) + l(v_n - l')| \leqslant |v_n||u_n - l| + |l||v_n - l'|$.

(v_n) est convergente donc bornée, on note M un majorant de $(|v_n|)$.

Soit $\varepsilon > 0$ quelconque, il existe N tel que pour tout $n > N$, $|u_n - l| < \frac{\varepsilon}{2M}$.

Si $l = 0$ alors pour tout $n > N$, $|u_n v_n - l\, l'| \leqslant \frac{\varepsilon}{2} < \varepsilon$ (CQFD).
Si $l \neq 0$, il existe N_1 tel que pour tout $n > N_1$, $|v_n - l'| < \frac{\varepsilon}{2|l|}$.

On pose $N_2 = \max(N, N_1)$, pour tout $n > N_2$, on a $|u_n v_n - l\, l'| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ (CQFD).

4.3 Opérations et limite infinie

La section 4.2 s'applique uniquement aux suites réelles.

Théorème : inverse d'une suite convergeant vers 0

Soient (u_n) une suite réelle.
Si $\lim u_n = 0$ et pour tout n à partir d'un certain rang $u_n > 0$, alors $\lim \dfrac{1}{u_n} = +\infty$.
Idem avec $u_n < 0$ et $-\infty$.

Théorème : opérations avec une suite de limite infinie

Soient (u_n) et (v_n) deux suites réelles avec $\lim u_n = +\infty$.

1) $\lim \frac{1}{u_n} = 0$.
2) si (v_n) est minorée alors $\lim u_n + v_n = +\infty$.
3) si (v_n) est minorée par un réel strictement positif alors $\lim u_n\, v_n = +\infty$.
4) si (v_n) est majorée par un réel strictement négatif alors $\lim u_n\, v_n = -\infty$.

On peut traduire ces propriétés pour $-\infty$ en utilisant $\lim u_n = -\infty \Leftrightarrow \lim -u_n = +\infty$.

Démonstrations
Montrons par exemple que si (v_n) est minorée par $a > 0$ alors $\lim u_n\, v_n = +\infty$.

Soit $A > 0$ quelconque, il existe N tel que pour tout $n > N$, $u_n > \frac{A}{a} > 0$.
De plus $\forall n \in \mathbb{N}$, $v_n > a > 0$ donc, pour tout $n > N$, $u_n\, v_n > A$ (CQFD).

4.4 Limites et encadrements

La section 4.3 s'applique uniquement aux suites réelles.

Lemme

Soient (u_n) une suite réelle positive ou nulle à partir d'un certain rang.
Si u_n admet une limite, alors $\lim u_n \geqslant 0$.

Remarque : on ne peut pas avoir mieux que l'inégalité au sens large $\lim u_n \geqslant 0$, même si $u_n > 0$ pour tout n. Exemple : $\lim \frac{1}{n}$.

Démonstration
On note $\lim u_n = l$ et on montre par l'absurde que $l \geqslant 0$.

Supposons $l < 0$. D'après la définition de $\lim u_n = l$ avec $\varepsilon = -\dfrac{l}{2} > 0$, il existe un rang à partir duquel les termes u_n vérifient tous $l - \varepsilon = \dfrac{3l}{2} < u_n < l + \varepsilon = \dfrac{l}{2} < 0$ ce qui est contradictoire avec (u_n) est positive ou nulle à partir d'un certain rang.

Théorème du passage à la limite

Soient (u_n) et (v_n) deux suites réelles telles que $u_n \leqslant v_n$ pour tout n à partir d'un certain rang.

1) Si $\lim u_n = +\infty$ alors $\lim v_n = +\infty$.
2) Si $\lim v_n = -\infty$ alors $\lim u_n = -\infty$.
3) Si (u_n) et (v_n) sont convergentes alors $\lim u_n \leqslant \lim v_n$.

Remarque pour le 3) : en passant à la limite une inégalité au sens stricte, on n'obtient qu'une inégalité au sens large.

Démonstration

1) Soit un réel quelconque $A > 0$, d'après la définition de $\lim u_n = +\infty$, il existe N tel que pour tout $n \geqslant N$, $u_n > A$.
   Comme il existe N_1 tel que pour tout $n \geqslant N_1$ on a $u_n \leqslant v_n$, on en déduit que pour tout $n \geqslant N_2 = \max(N, N_1)$, $v_n > A$ (CQFD).
2) On applique le résultat précédent pour $(-u_n)$ et $(-v_n)$.
3) $(v_n - u_n)$ est positive ou nulle à partir d'un certain rang et convergente donc $0 \leqslant \lim(u_n - v_n) = \lim u_n - \lim v_n$. on en déduit $\lim u_n \leqslant \lim v_n$.

Théorème des gendarmes

Soient (u_n), (v_n) et (w_n) des suites réelles telles que $u_n \leqslant v_n \leqslant w_n$ pour tout n à partir d'un certain rang.
Si (u_n) et (w_n) **convergent vers une même limite** l alors (v_n) converge aussi vers l.

Démonstration
Soit $\varepsilon > 0$ quelconque.
La définition de $\lim u_n = l$ et $\lim w_n = l$ implique qu'il existe N tel que
pour tout $n \geqslant N$, $\quad l - \varepsilon < u_n < l + \varepsilon \quad$ et $\quad l - \varepsilon < w_n < l + \varepsilon$.
Donc pour tout $n \geqslant N$, on a $l - \varepsilon < u_n \leqslant v_n \leqslant w_n < l + \varepsilon$ qui implique $|v_n - l| < \varepsilon$ (CQFD).

Corrolaire pour des suites réelles ou complexes

Soient (u_n) et (v_n) des suites complexes telles que $\lim u_n = 0$ et (v_n) est bornée alors $\lim u_n\, v_n = 0$.

Démonstration
On note M un majorant de $(|v_n|)$. Pour tout n, $0 \leqslant |u_n\, v_n| \leqslant M|u_n|$. Or $\lim M|u_n| = 0$ d'où $\lim |u_n\, v_n| = 0$ par application du théorème du gendarme. Il suit que $\lim u_n\, v_n = 0$.

4.5 Limite et suites monotones

La section 4.4 s'applique uniquement aux suites réelles.

Théorème de la limite monotone

1) Soit (u_n) une suite réelle **croissante** :
   - si (u_n) est **majorée** alors (u_n) est **convergente** et sa limite est $\sup\{u_n,\ n \in \mathbb{N}\}$,
   - si (u_n) n'est **pas majorée**, alors $\lim u_n = +\infty$.
2) Soit (v_n) une suite réelle **décroissante** :
   - si (v_n) est **minorée** alors (v_n) est **convergente** et sa limite est $\inf\{v_n,\ n \in \mathbb{N}\}$,
   - si (v_n) n'est **pas minorée**, alors $\lim v_n = -\infty$.

Démonstration

1) **Cas** (u_n) **majorée** : $\{u_n,\ n \in \mathbb{N}\}$ est une partie majorée de $\mathbb{R}$, donc elle admet une borne supérieure que l'on note l.
   Soit $\varepsilon > 0$ quelconque, d'après la propriété de la borne supérieure, il existe N tel que $l - \varepsilon < u_N \leqslant l$.
   Comme (u_n) est croissante et que l majore (u_n), on en déduit que pour tout $n \geqslant N$, $l - \varepsilon < u_n \leqslant l$ ce qui implique $|u_n - l| < \varepsilon$ (CQFD).

   Cas (u_n) **non majorée** : Soit $A > 0$ quelconque. A ne majore pas (u_n) donc il existe N tel que $u_N > A$.
   Comme (u_n) est croissante on en déduit que pour tout $n \geqslant N$, $u_n > A$ (CQFD).
2) Le résultat pour une suite décroissante (v_n) se déduit du 1) avec $(-v_n)$.

Exemples (à faire en TD)
- Montrer que la suite (u_n) définie pour tout $n \in \mathbb{N}$ par $u_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ tend vers $+\infty$.
  Indication : montrer que $u_{2^p} \geqslant 1 + \frac{p}{2}$.

- Montrer que la suite (v_n) définie pour tout $n \in \mathbb{N}$ par $v_n = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2}$ converge.
  Indication : montrer que $v_n \leqslant 2 - \frac{1}{n}$.

Théorème : suites adjacentes

Soient (u_n) une suite réelle **croissante** et (v_n) une suite réelle **décroissante** telles que $\lim u_n - v_n = 0$, alors (u_n) **et** (v_n) **convergent vers une même limite** l, on dit qu'elles sont **adjacentes**.
De plus, pour tout n, on a l'encadrement $u_n \leqslant l \leqslant v_n$.

Démonstration
On montre d'abord par l'absurde que (u_n) est majorée et (v_n) est minorée.
En effet supposons que (u_n) n'est pas majorée, alors, d'après le théorème précédent, $u_n \to +\infty$ et comme $(v_n) = (u_n) + (v_n - u_n)$ et $u_n - v_n \to 0$, on a aussi $v_n \to +\infty$. Or (v_n) est décroissante donc (v_n) converge ou tend vers $-\infty$. On obtient une contradiction donc (u_n) est nécessairement majorée.
Comme (u_n) est croissante, il suit qu'elle converge.

On montre de la même manière que (v_n) est minorée. Comme elle décroit, il suit qu'elle converge.

(u_n) et (v_n) étant convergentes, $\lim u_n \ - \lim u_n = \lim u_n - v_n = 0$. On note l leur limite commune.

D'après le théorème précédent, $l = \sup\{u_n / n \in \mathbb{N}\}$ et $l = \inf\{v_n / n \in \mathbb{N}\}$, par conséquent l majore (u_n) et minore (v_n), donc pour tout n, $u_n \leqslant l \leqslant v_n$.

Théorème de Bolzano-Weierstrass

De toute suite réelle bornée, on peut extraire une suite convergente.
C.a.d, soit (u_n) une suite réelle bornée, il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(u_{\varphi(n)})$ converge.

Démonstration :
Soit (u_n) une suite réelle bornée.

Posons pour tout $n \in \mathbb{N}$, $s_n = \sup U_n$ où $U_n = \{u_k, k > n\}$, c.a.d. s_n est la borne sup des termes de rangs strictement supérieurs à n.

Pour tout n, U_n est une partie de $\mathbb{R}$ non vide et majorée donc s_n est bien défini.

Pour tout n, $U_{n+1} \subset U_n$ et s_n majore U_n, donc s_n majore aussi U_{n+1}, il suit que $s_n \geqslant s_{n+1}$ puisque s_{n+1} est le plus petit majorant de U_{n+1}.

On a montré que (s_n) est une suite décroissante.

(u_n) est bornée, donc elle admet un minorant m.
Pour tout n, m minore à fortiori U_n, de plus, par définition, s_n majore U_n. Comme U_n contient au moins un élément a, on a $m \leqslant a \leqslant s_n$.

On a montré que (s_n) est minorée par m.

D'après le théorème de la limite monotone, (s_n) est convergente. Bien sûr, ce n'est pas a priori une suite extraite de (u_n) mais on peut en construire une à partir de s_n.

On construit la suite extraite $(u_{\varphi(n)})$ par récurrence :

- on choisit $\varphi(0) = 0$ c.a.d. que u_0 est le premier terme de la suite extraite.

- soit n quelconque. Supposons construit $\varphi(n)$.

$s_{\varphi(n)} = \sup U_{\varphi(n)}$, donc, d'après la propriété de la borne sup avec $\varepsilon = \frac{1}{n}$,
il existe $x \in U_{\varphi(n)}$ tel que $s_{\varphi(n)} - \frac{1}{n} < x \leqslant s_{\varphi(n)}$

x est un élément de $U_{\varphi(n)}$ donc il existe $k > \varphi(n)$ tel que $u_k = x$. On pose $\varphi(n+1) = k$.

On a donc $\varphi(n+1) > \varphi(n)$ et (I) $s_{\varphi(n)} - \frac{1}{n} < u_{\varphi(n+1)} \leqslant s_{\varphi(n)}$.

Conclusion : on a construit une application $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante. Les suites $(s_{\varphi(n)})$ et $(u_{\varphi(n)})$ sont donc des suites extraites respectivement de (s_n) et (u_n).

On note l la limite de (s_n), la suite extraite $(s_{\varphi(n)})$ converge vers l, ainsi que $(s_{\varphi(n)} - \frac{1}{n})$.
D'après le théorème de passage à la limite sur l'encadrement (I) on en déduit que $(u_{\varphi(n)})$ converge vers l.