PSF 11 – Mathématiques

Notes de cours

Table des matières

Introduction

Vos modules de mathématiques durant votre première année à l'IPSA fonctionnent suivant le principe de la *classe inversée* : ils vous est demandé de découvrir les nouvelles notions de cours durant votre temps de travail personnel à l'aide de ressources écrites ou vidéo qui vous seront fournies, tandis que les heures de travaux dirigés seront essentiellement consacrées à la mise en application de ces notions sur des exercices-types puis des problèmes plus élaborés. L'intérêt de ce système est multiple. D'abord, cela vous permet d'acquérir les notions de cours suivant le planning de votre choix, et à votre rythme : vous pouvez passer rapidement sur les notions que vous comprenez immédiatement et consacrer plus de temps aux concepts qui vous semblent plus difficiles. Par ailleurs, en déplaçant ce temps d'acquisition du cours sur votre temps de travail personnel, l'intégralité de la séance TD pourra être dédiée aux réponses aux questions sur le cours et à la mise en pratique sur des exercices. Enfin, si vous prenez le temps d'essayer de comprendre par vous-mêmes les notions de cours avant chaque séance, vous retiendrez beaucoup mieux ces notions dans le temps et votre travail de révision s'en trouvera naturellement réduit à l'approche des semaines d'examens.

Toutefois pour que cette méthode de classe inversée soit efficace, il est impératif que vous fassiez la démarche d'avoir une attitude **active** lors de votre travail personnel du cours. La majorité du contenu à préparer pour les TD étant disponible sous forme de vidéos sur la plateforme IonisX, ce document est là principalement pour vous accompagner dans le visionnage de ces vidéos. Il vous aidera à identifier les définitions et résultats clés de chaque chapitre, et à organiser votre cours en sections et sous-sections thématiques. En supplément, voici quelques recommandations pour vous aider à tirer le meilleur de ce système.

1. N'hésitez pas à inclure un ou plusieurs créneaux dédiés spécifiquement au visionnage du cours dans votre planning de travail personnel.
2. N'hésitez pas à regarder à nouveau une vidéo de cours quelques jours après votre premier visionnage : en ayant compris et intégré l'essentiel du contenu, vous pourrez vous saisir de certaines remarques et subtilités à côté desquelles vous serez peut-être passé la première fois.
3. Libre à vous de choisir comment utiliser ce document : l'imprimer pour simplement compléter les trous, le réécrire complètement au propre sur le support de votre choix, … L'écriture favorisant souvent la mémorisation, la deuxième option peut être préférable mais n'est pas obligatoire.
4. Évitez autant que possible de recopier mécaniquement et de manière superficielle le contenu que vous visionnez. Vous pouvez mettre en pause la vidéo et travailler le cours à votre rythme, profitez-en pour faire l'effort de toujours chercher à comprendre ce que vous écrivez.
5. Lorsqu'une vidéo de cours propose un exemple, une application, une démonstration, … essayez d'anticiper et de faire par vous-même les prochaines étapes avant qu'elles ne soient affichées. Cela vous permettra de vérifier votre compréhension des notions qui vous ont été présentées juste avant et facilitera votre mémorisation du cours.
6. N'hésitez pas à compléter ce document avec des explications et remarques fournies par vos professeurs de TD ou issues votre expérience personnelle. Comparez régulièrement vos notes de cours avec celles de vos camarades afin qu'elles soient aussi complètes que possible.
7. Si après votre travail du cours des points restent incompris, n'hésitez pas à vous tourner vers vos camarades de classe, ou bien notez vos questions et posez-les à votre professeur dès le début de la prochaine séance de TD.
8. Les démonstrations marquées du symbole ● pourront être demandées en examen (oral ou écrit). Évitez à tout prix de les apprendre par cœur ! Apprenez simplement les étapes clés et faites vous confiance sur votre capacité à savoir mener le reste des calculs ou du raisonnement. Les autres démonstrations, bien que non exigibles, doivent tout de même être comprises.

Ma111

Chapitre I.

Calculs algébriques

Pas de mimo associé sur IonisX.

I.1. Puissances et racines

Définition 1. (Puissance entière positive) Pour tout $x \in \mathbb{R}$ et pour tout entier $n \geqslant 0$, on pose

$$x^n = \underbrace{x \times x \times \cdots \times x}_{n \text{ fois}}$$

avec la convention $x^0 = 1$.

Remarque. De manière plus rigoureuse, la notation x^n est définie par récurrence en posant

$$x^0 = 1 \qquad \text{et} \qquad \forall\, n \in \mathbb{N},\ x^{n+1} = x^n \times x.$$

Proposition 1. Soit $(x, y, a, b) \in \mathbb{R} \times \mathbb{R} \times \mathbb{N} \times \mathbb{N}$. Alors :

1. $x^a \times x^b = x^{a+b}$,
2. $(x^a)^b = x^{ab}$,
3. $(x \times y)^a = x^a \times y^a$,
4. $\left(\dfrac{x}{y}\right)^a = \dfrac{x^a}{y^a}$.

La convention $x^0 = 1$ n'a rien d'arbitraire, il s'agit de la valeur la plus naturelle à poser pour x^0 si l'on veut conserver les propriétés listées dans la Proposition 1. C'est ce qu'illustre la figure ci-dessous, qui donne également une idée de comment définir la puissance négative d'un réel : pour x^{-1} par exemple, il faut donner une valeur telle que $x^{-1} \times x$ soit égal à $x^{-1+1} = x^0 = 1$.

x^{-2}	x^{-1}	x^0	x^1	x^2	x^3	x^4
?	?	1	x	$x \times x$	$x \times x \times x$	$\cdots$

$\times x$ $\times x$ $\times x$ $\times x$ $\times x$

Définition 2. (Puissance entière négative) Pour tout $x \in \mathbb{R}^*$ et pour tout entier $n \geqslant 0$, on pose

$$x^{-n} = \frac{1}{x^n}.$$

Définition 3. (Racine n-ième) Soient $n \geqslant 2$ un entier et soit $x \in \mathbb{R}$. Une racine n-ième de x est un nombre $r \in \mathbb{R}$ tel que

$$r^n = x.$$

Proposition 2. Soit $n \geqslant 2$ un entier. On distingue deux cas.

1. Si n est pair, alors :
   - un réel $x > 0$ admet deux racines n-ièmes opposées dans $\mathbb{R}$, on note $\sqrt[n]{x}$ celle qui est positive,
   - $x = 0$ admet une seule racine n-ième qui est zéro lui-même, on note $\sqrt[n]{0} = 0$,
   - un réel $x < 0$ n'admet pas de racine n-ième dans $\mathbb{R}$.
2. Si n est impair, alors tout réel $x \in \mathbb{R}$ admet exactement une racine n-ième dans $\mathbb{R}$, notée $\sqrt[n]{x}$.

Pour $n = 2$, on retrouve le concept de racine carrée, notée simplement $\sqrt{x}$ au lieu de $\sqrt[2]{x}$.

Exemple.
- 9 admet deux racines carrées dans $\mathbb{R}$: 3 et -3. La notation $\sqrt{9}$ désigne le nombre 3.
- 16 admet deux racines quatrièmes dans $\mathbb{R}$: 2 et -2. La notation $\sqrt[4]{16}$ désigne le nombre 2.
- 125 admet une seule racine cubique ($n = 3$) dans $\mathbb{R}$, il s'agit de 5. On note donc $\sqrt[3]{125} = 5$.
- -8 admet une seule racine cubique dans $\mathbb{R}$, il s'agit de -2. On note donc $\sqrt[3]{-8} = -2$.

Proposition 3. Soient x, y deux réels et n, m deux entiers supérieurs ou égaux à 2. Alors :

1. $\sqrt[n]{x \times y} = \sqrt[n]{x} \times \sqrt[n]{y}$,
2. $\sqrt[n]{\dfrac{x}{y}} = \dfrac{\sqrt[n]{x}}{\sqrt[n]{y}}$,
3. $\sqrt[m]{\sqrt[n]{x}} = \sqrt[mn]{x}$,
4. $\sqrt[m]{x^n} = \left(\sqrt[m]{x}\right)^n$.

Le concept de racine n-ième permet de définir $x^{\frac{1}{n}}$. En effet, pour que la proposition 1 reste valide, il faut notamment choisir un nombre tel que :

$$\left(x^{\frac{1}{n}}\right)^n = x^{\frac{n}{n}} = x^1 = x.$$

On définit donc $x^{\frac{1}{n}}$ comme étant $\sqrt[n]{x}$.

Définition 4. (Puissance rationnelle) Soient $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. On pose

$$x^{\frac{p}{q}} = \sqrt[q]{x^p}.$$

(ce qui est équivalent à poser $x^{\frac{p}{q}} = (\sqrt[q]{x})^p$ d'après la proposition précédente.)

Remarque. Notez qu'avec cette nouvelle notation, les propriétés listées dans la proposition 3 ne sont que des réécritures de propriétés déjà listées dans la proposition 1. Il n'est donc pas nécessaire d'apprendre par cœur la proposition 3, il vaut mieux savoir retrouver ces relations à l'aide des propriétés des puissances lorsqu'elles interviennent dans un calcul.

Enfin, pour aller plus loin on peut chercher à donner plus généralement du sens à x^a lorsque a est irrationnel. Cette généralisation est plus subtile, il faut utiliser les fonctions exponentielle et logarithme dont on rappelle les définitions et propriétés dans la section suivante.

Définition 5. (Puissance réelle) Pour tout $x \in \mathbb{R}_+^*$ et pour tout $a \in \mathbb{R}$, on pose

$$x^a = \exp(a \ln(x)).$$

Proposition 4. La proposition 1 reste vraie pour toutes les généralisations de x^a décrites dans cette section (c'est-à-dire pas seulement pour $a \in \mathbb{N}$, mais aussi pour $n \in \mathbb{R}$ réel quelconque).

I.2. Exponentielle et logarithme népérien

Définition 6. La fonction **exponentielle**, notée $\exp$, est définie comme l'unique fonction dérivable de $\mathbb{R}$ dans $\mathbb{R}$ telle que

$$\exp(0) = 1 \qquad \text{et} \qquad \exp' = \exp\,.$$

Proposition 5. Pour tout $(x, y) \in \mathbb{R} \times \mathbb{R}$ et pour tout $n \in \mathbb{R}$,

1. $\exp(-x) = \dfrac{1}{\exp(x)}$,
2. $\exp(x + y) = \exp(x)\exp(y)$,
3. $\exp(x - y) = \dfrac{\exp(x)}{\exp(y)}$,
4. $\exp(nx) = (\exp(x))^n$.

Définition 7. On note e le nombre $\exp(1) \approx 2{,}7$. Plus généralement, pour tout $x \in \mathbb{R}$ on notera e^x pour $\exp(x)$.

L'avantage de cette nouvelle notation est que la proposition 5 n'est pas à apprendre par cœur, car elle peut être vue comme un cas particulier de la proposition 1.

Définition 8. La fonction **logarithme népérien**, notée $\ln$, peut-être définie de deux manières en apparence très différentes, mais qui s'avèrent être équivalentes.

1. C'est la fonction définie sur $\mathbb{R}_+^*$ définie par
$$\forall\, x \in \mathbb{R}_+^*, \quad \ln(x) = \int_1^x \frac{1}{t} \mathrm{d}t.$$
2. C'est la *réciproque* de la fonction exponentielle, c'est-à-dire l'unique fonction de $\mathbb{R}_+^*$ dans $\mathbb{R}$ telle que :
$$\forall (x, y) \in \mathbb{R} \times \mathbb{R}_+^*, \quad (\exp(x) = y \iff x = \ln(y)).$$

Quelques propriétés découlant de ces définitions :

Proposition 6.

1. $\ln(1) = 0$ et $\ln(e) = 1$,
2. Pour tout $x \in \mathbb{R}$, $\ln(e^x) = x$,
3. Pour tout $x \in \mathbb{R}_+^*$, $e^{\ln(x)} = x$.

Quelques propriétés à mettre en relation avec la proposition 5 :

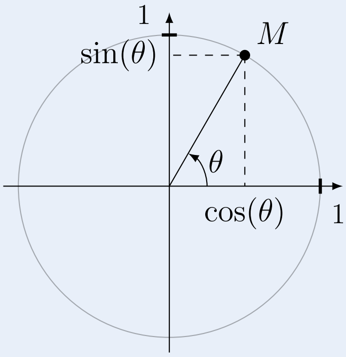
Proposition 7. Pour tout $(x, y) \in \mathbb{R}_+^* \times \mathbb{R}_+^*$ et pour tout $n \in \mathbb{N}$,

1. $\ln\left(\dfrac{1}{x}\right) = -\ln(x)$,
2. $\ln(xy) = \ln(x) + \ln(y)$,
3. $\ln\left(\dfrac{x}{y}\right) = \ln(x) - \ln(y)$,
4. $\ln(x^n) = n\ln(x)$.

Pour aller plus loin : vidéo *Logarithme et exponentielle* sur IonisX (Ma12, module 16).

I.3. Trigonométrie

Définition 9.



Dans le plan euclidien, notons $\mathscr{C}$ le cercle de centre O et de rayon 1.

Soit $\theta \in \mathbb{R}$. On note M le point sur $\mathscr{C}$ tel que l'angle orienté entre la demi-droite $[Ox)$ et $\overrightarrow{OM}$ soit égal à θ.

- Le **cosinus** de θ, noté $\cos(\theta)$, est l'abscisse du point M.
- Le **sinus** de θ, noté $\sin(\theta)$, est l'ordonnée du point M.

De plus, pour tout θ différent de $\frac{\pi}{2}$ modulo π, on définit la **tangente** de θ, notée $\tan(\theta)$, comme le rapport :

$$\tan(\theta) = \frac{\sin(\theta)}{\cos(\theta)}.$$

Proposition 8. Pour tout $(x, a, b) \in \mathbb{R}^3$,

1. $\cos^2(x) + \sin^2(x) = 1$,
2. $\cos(-x) = \cos(x)$,
3. $\cos(x + \frac{\pi}{2}) = -\sin(x)$,
4. $\cos(x + \pi) = -\cos(x)$,
5. $\cos(x + 2\pi) = \cos(x)$,
6. $\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b)$,
7. $\cos(a - b) = \cos(a)\cos(b) + \sin(a)\sin(b)$,
8. $\cos(2a) = \cos^2(a) - \sin^2(a)$,
9. $\sin(-x) = -\sin(x)$,
10. $\sin(x + \frac{\pi}{2}) = \cos(x)$,
11. $\sin(x + \pi) = -\sin(x)$,
12. $\sin(x + 2\pi) = \sin(x)$,
13. $\sin(a + b) = \sin(a)\cos(b) + \sin(b)\cos(a)$,
14. $\sin(a - b) = \sin(a)\cos(b) - \sin(b)\cos(a)$,
15. $\sin(2a) = 2\sin(a)\cos(a)$.

Remarque. Les propriétés 6 et 13 sont parfois appelées *formules d'addition*, et les propriétés 8 et 15 *formules de duplication*. Des formules analogues existent pour la tangente mais ne sont pas à connaître.

De plus, une grande partie des propriétés listées ci-dessus découlent en réalité des formules d'addition. Il peut être intéressant d'essayer de poser les calculs pour s'en convaincre.

I.4. Symboles somme et produit

I.4.1. Définition et propriétés

Définition 10. Soient deux entiers $p \leqslant q$.

- Les notations
$$\sum_{k=p}^{q} u_k, \qquad \textstyle\sum_{k=p}^{q} u_k \qquad \text{et} \qquad \displaystyle\sum_{p \leqslant k \leqslant q} u_k$$
désignent la somme $u_p + u_{p+1} + \cdots + u_q$.
- Les notations
$$\prod_{k=p}^{q} u_k, \qquad \textstyle\prod_{k=p}^{q} u_k \qquad \text{et} \qquad \displaystyle\prod_{p \leqslant k \leqslant q} u_k$$
désignent le produit $u_p \times u_{p+1} \times \cdots \times u_q$.

Exemple.

- $\displaystyle\sum_{k=3}^{7} k = 3 + 4 + 5 + 6 + 7 = 25,$
- $\displaystyle\sum_{k=0}^{n} k^2 = 0^2 + 1^2 + 2^2 + \cdots + (n-1)^2 + n^2,$
- $\displaystyle\sum_{k=1}^{4} (2k+1) = (2 \times 1 + 1) + (2 \times 2 + 1) + (2 \times 3 + 1) + (2 \times 4 + 1) = 3 + 5 + 7 + 9 = 24,$
- $\displaystyle\prod_{k=1}^{4} (2k+1) = (2 \times 1 + 1) \times (2 \times 2 + 1) \times (2 \times 3 + 1) \times (2 \times 4 + 1) = 3 \times 5 \times 7 \times 9 = 945.$

Remarque. Par convention, on considère souvent que
$$\sum_{k=p}^{q} u_k = 0 \qquad \text{et} \qquad \prod_{k=p}^{q} u_k = 1$$
lorsque $q < p$ (on parle parfois de somme ou de produit *vide*).

Proposition 9. On a les propriétés de calcul suivantes :

1. $\displaystyle\left(\sum_{k=p}^{q} u_k\right) + \left(\sum_{k=q+1}^{r} u_k\right) = \sum_{k=p}^{r} u_k,$
2. $\displaystyle\sum_{k=p}^{q} (u_k + v_k) = \left(\sum_{k=p}^{q} u_k\right) + \left(\sum_{k=p}^{q} v_k\right),$
3. $\displaystyle\sum_{k=p}^{q} (u_k - v_k) = \left(\sum_{k=p}^{q} u_k\right) - \left(\sum_{k=p}^{q} v_k\right),$
5. $\displaystyle\left(\prod_{k=p}^{q} u_k\right) \times \left(\prod_{k=q+1}^{r} u_k\right) = \prod_{k=p}^{r} u_k,$
6. $\displaystyle\prod_{k=p}^{q} (u_k \times v_k) = \left(\prod_{k=p}^{q} u_k\right) \times \left(\prod_{k=p}^{q} v_k\right),$
7. $\displaystyle\prod_{k=p}^{q} \frac{u_k}{v_k} = \frac{\prod_{k=p}^{q} u_k}{\prod_{k=p}^{q} v_k},$

4. $\displaystyle\sum_{k=p}^{q} \lambda u_k = \lambda \sum_{k=p}^{q} u_k,$

8. $\displaystyle\prod_{k=p}^{q} u_k^{\lambda} = \left(\prod_{k=p}^{q} u_k\right)^{\lambda}.$

Remarque. Il faut éviter d'apprendre ces règles de calcul par cœur. Mieux vaut être capable de se convaincre qu'elles sont vraies en réécrivant au brouillon la somme ou le produit à l'aide de points de suspension.

Proposition 10. (Cas où le terme est constant) Pour tous entiers $p \leqslant q$, on a

$$\sum_{k=p}^{q} c = N \times c \qquad \text{et} \qquad \prod_{k=p}^{q} c = c^N$$

où $N = q - p + 1$ est le nombre de termes dans la somme ou le produit.

Exemple.

- $\displaystyle\sum_{k=5}^{15} 3 = \underbrace{3 + 3 + \cdots + 3}_{11 \text{ termes}} = 11 \times 3 = 33,$
- $\displaystyle\prod_{k=0}^{9} 2 = \underbrace{2 \times 2 \times \cdots \times 2}_{10 \text{ termes}} = 2^{10} = 1024.$

Proposition 11. (Somme de suites particulières)

- Si la suite (u_n) est arithmétique, alors

$$\sum_{k=p}^{q} u_k = N \times \frac{u_p + u_q}{2}$$

où $N = q - p + 1$ est le nombre de termes de la somme.

Cas particulier : pour tout $n \in \mathbb{N}^*$,

$$\sum_{k=0}^{n} k = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

- Si la suite (u_n) est géométrique de raison $q \neq 1$, alors

$$\sum_{k=p}^{q} u_k = u_p \times \frac{1 - q^N}{1 - q}$$

où $N = q - p + 1$ est le nombre de termes de la somme.

Cas particulier : pour tout $n \in \mathbb{N}^*$ et pour tout $q \neq 1$,

$$\sum_{k=0}^{n} q^k = \frac{1 - q^{n+1}}{1 - q}.$$

I.4.2. Changements d'indices

Proposition 12. (Changement d'indice) Soient $p \leqslant q$ deux entiers, et soit $d \in \mathbb{Z}$. On a :

$$\sum_{k=p}^{q} u_{k+d} = \sum_{k=p+d}^{q+d} u_k \qquad \text{et} \qquad \prod_{k=p}^{q} u_{k+d} = \prod_{k=p+d}^{q+d} u_k.$$

Remarque. La proposition ci-dessus ne doit pas être apprise par cœur, mais simplement suffisamment comprise pour être appliquée sans problème lors d'un calcul.

Exemple.

- $\displaystyle\sum_{k=0}^{4} u_{k+2} = u_{0+2} + u_{1+2} + u_{2+2} + u_{3+2} + u_{4+2} = u_2 + u_3 + u_4 + u_5 + u_6 = \sum_{k=2}^{6} u_k,$
- $\displaystyle\sum_{k=3}^{n+2} u_{k-1} = u_{3-1} + u_{4-1} + \cdots + u_{n+2-1} = u_2 + u_3 + \cdots + u_{n+1} = \sum_{k=2}^{n+1} u_k.$

Le changement d'indice est souvent très utile pour simplifier des sommes ou des produits, notamment dans le cas de phénomène dits de *télescopage* comme dans les deux exemples suivants.

Exemple. (Somme télescopique) Considérons la somme

$$S = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right).$$

Au brouillon on semble deviner un phénomène de télescopage :

$$S = \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n-2} - \frac{1}{n-1}\right) + \left(\frac{1}{n-1} - \frac{1}{n}\right) + \left(\frac{1}{n} - \frac{1}{n+1}\right)$$

c'est-à-dire qu'il semblerait que chaque terme en rouge se simplifie avec un terme en bleu dans l'expression ci-dessus. Démontrons-le rigoureusement.

Remarquons déjà que

$$S = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right) = \left(\sum_{k=1}^{n} \frac{1}{k} \right) - \left(\sum_{k=1}^{n} \frac{1}{k+1} \right).$$

Étudions séparément les deux sommes obtenues.

- Dans la première, on peut isoler le premier terme de la somme et on trouve :

$$\sum_{k=1}^{n} \frac{1}{k} = \frac{1}{1} + \sum_{k=2}^{n} \frac{1}{k}.$$

- Dans la seconde, on effectue un changement d'indice puis on isole le dernier terme :

$$\sum_{k=1}^{n} \frac{1}{k+1} = \sum_{k=2}^{n+1} \frac{1}{k} = \left(\sum_{k=2}^{n} \frac{1}{k} \right) + \frac{1}{n+1}.$$

Avec ces deux transformations, le télescopage apparaît clairement puisqu'on peut maintenant écrire :

$$S = \left(\frac{1}{1} + \sum_{k=2}^{n} \frac{1}{k}\right) - \left(\sum_{k=2}^{n} \frac{1}{k} + \frac{1}{n+1}\right) = 1 - \frac{1}{n+1}.$$

Exemple. (Produit télescopique) Considérons le produit

$$P = \prod_{k=2}^{n+1} \frac{k}{k-1}.$$

Comme dans l'exemple précédent, on conjecture au brouillon un télescopage :

$$P = \frac{2}{1} \times \frac{3}{2} \times \frac{4}{3} \times \cdots \times \frac{n-1}{n-2} \times \frac{n}{n-1} \times \frac{n+1}{n}.$$

Faisons apparaître ces simplifications à l'aide d'un calcul rigoureux. On a

$$P = \prod_{k=2}^{n+1} \frac{k}{k-1} = \frac{\displaystyle\prod_{k=2}^{n+1} k}{\displaystyle\prod_{k=2}^{n+1} (k-1)} = \frac{\left(\displaystyle\prod_{k=2}^{n} k\right) \times (n+1)}{1 \times \left(\displaystyle\prod_{k=3}^{n+1} (k-1)\right)}.$$

Or, un changement d'indice révèle que $\displaystyle\prod_{k=2}^{n} k = \prod_{k=3}^{n+1} (k-1)$. Ces deux termes se simplifient donc entre eux et on trouve $P = n+1$.

I.4.3. Formule du binôme de Newton

Vous connaissez déjà les identités remarquables

$$(a+b)^2 = a^2 + 2ab + b^2 \qquad \text{et} \qquad (a-b)^2 = a^2 - 2ab + b^2.$$

L'objectif de cette partie est d'arriver à une méthode systématique permettant de développer facilement $(a+b)^n$ et $(a-b)^n$ pour n'importe quelle valeur de $n \in \mathbb{N}^*$.

Définition 11. Soit $n \in \mathbb{N}^*$ un entier non-nul. On définit la **factorielle** de n, notée $n!$, par

$$n! = \prod_{k=1}^{n} k.$$

Par convention, on pose aussi $0! = 1$.

Exemple.

$$3! = 1 \times 2 \times 3 = 6, \qquad 5! = 1 \times 2 \times 3 \times 4 \times 5 = 120, \qquad 1! = 1.$$

Définition 12. Soient k, n deux entiers tels que $0 \leqslant k \leqslant n$. On définit le **coefficient binomial** « k parmi n », noté $\binom{n}{k}$ ou C_n^k, comme le nombre

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Exemple.

$$\binom{3}{1} = \frac{3!}{1! \times 2!} = \frac{6}{1 \times 2} = 3, \qquad \binom{5}{2} = \frac{5!}{2 \times 3!} = \frac{4 \times 5}{2} = 10, \qquad \binom{10}{0} = \frac{10!}{0! \times 10!} = 1.$$

Proposition 13. Pour tous entiers k, n tels que $0 \leqslant k \leqslant n$,

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{1} = \binom{n}{n-1} = n, \qquad \binom{n}{n-k} = \binom{n}{k}.$$

Remarque. En réalité, nous verrons plus tard dans l'année que le coefficient binomial « k parmi n » s'interprète comme le nombre de sous-ensembles formés de k éléments dans un ensemble de n éléments. Ceci permet de retrouver facilement les propriétés ci-dessus. En effet, dans l'ensemble $E = \{1, 2, \dots, n\}$:

- il y a 1 seul sous-ensemble à 0 élement (c'est l'ensemble vide) et un seul sous-ensemble à n élements (c'est E lui-même),
- il y a n sous-ensembles à 1 élément (ce sont $\{1\}, \{2\}, \dots, \{n\}$), et il y a n sous-ensembles à $n-1$ éléments (ce sont $E \setminus \{1\}, E \setminus \{2\}, \dots, E \setminus \{n\}$),
- choisir un sous-ensemble formé de k éléments, c'est équivalent à choisir les $n-k$ éléments qui ne seront pas dans ce sous-ensemble.

Proposition 14. (Formule du triangle de Pascal) Pour tous entiers k et n tels que $0 < k < n$, on a

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Démonstration. Partons du second membre qui, d'après la définition du coefficient binomial, est égal à :

$$\begin{aligned} \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!((n-1)-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!}. \end{aligned}$$

Réduisons ces deux fractions au même dénominateur. Pour cela il suffit de remarquer que $k! = (k-1)! \times k$ et $(n-k)! = (n-k-1)! \times (n-k)$. On obtient :

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)! \times k}{k!(n-k)!} + \frac{(n-1)! \times (n-k)}{k!(n-k)!}.$$

Il n'y a plus qu'à factoriser par $(n-1)!$ et on trouve bien :

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)! \times (k+n-k)}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Cette formule est d'une utilité capitale car elle permet de calculer très facilement les coefficients binomiaux $\binom{n}{k}$ pour les première valeurs de n, sans passer par des expressions faisant intervenir des factorielles.

Exemple. Calculons les coefficients binomiaux $\binom{n}{k}$ pour $0 \leqslant k \leqslant 5$.

- Pour $n = 0$ et $n = 1$, on sait déjà que
$$\binom{0}{0} = 1 \qquad \text{et} \qquad \binom{1}{0} = \binom{1}{1} = 1.$$
- Pour $n = 2$, on sait déjà que
$$\binom{2}{0} = \binom{2}{2} = 1$$
et la formule du triangle de Pascal nous indique que
$$\binom{2}{1} = \binom{1}{0} + \binom{1}{1} = 1 + 1 = 2.$$
- Pour $n = 3$, on sait déjà que
$$\binom{3}{0} = \binom{3}{3} = 1$$
et la formule du triangle de Pascal nous indique que
$$\binom{3}{1} = \binom{2}{0} + \binom{2}{1} = 1 + 2 = 3 \quad \text{et} \quad \binom{3}{2} = \binom{2}{1} + \binom{2}{2} = 2 + 1 = 3.$$
- On peut continuer à calculer ainsi les valeurs des coefficients binomiaux $\binom{n}{k}$ à partir de celles calculées pour les $\binom{n-1}{k}$. De manière schématique, cela veut dire que si on représente les coefficients binomiaux sur un triangle où chaque ligne correspond aux coefficients $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}$ pour une valeur de n fixée, alors chaque coefficient peut être obtenue en faisant la somme des deux coefficients placés au-dessus. Cette figure est appelée le **triangle de Pascal**.

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad \boxed{2 \; + \; 1} \\
1 \quad 3 \quad \boxed{3} \quad 1 \\
1 \quad \boxed{4 \; + \; 6} \quad 4 \quad 1 \\
1 \quad 5 \quad \boxed{10} \quad 10 \quad 5 \quad 1
\end{array}
$$

Proposition 15. (Formule du binôme de Newton) Soit $n \in \mathbb{N}$. Pour tout $(a, b) \in \mathbb{R}^2$,
$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Démonstration. Cette formule se démontre par récurrence sur n.

- **Initialisation.** Soit $n = 0$. Pour tout $(a, b) \in \mathbb{R}^2$, on a d'une part
$$(a+b)^n = (a+b)^0 = 1$$
et d'autre part
$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{0}{0} a^{0-0} b^0 = 1$$
donc la formule est vraie pour $n = 0$.
- **Hérédité.** Supposons la formule vraie pour un entier $n \in \mathbb{N}$ fixé. On a alors :
$$(a+b)^{n+1} = (a+b) \times (a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$
En développant le produit, on trouve
$$(a+b)^{n+1} = a \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k + b \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}.$$
Étudions séparément les deux sommes obtenues. Dans la première, on peut isoler le premier terme pour obtenir :
$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k = \binom{n}{0} a^{n-0+1} b^0 + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} b^k = a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} b^k.$$
Dans la seconde, on peut isoler le dernier terme et effectuer un changement d'indice, on trouve alors :
$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} = \binom{n}{n} a^{n-n} b^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} = b^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^{n+1-k} b^k.$$
Finalement, on obtient donc
$$(a+b)^{n+1} = \left(a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} b^k \right) + \left(b^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^{n+1-k} b^k \right)$$
soit encore en regroupant les deux sommes entre elles :
$$(a+b)^{n+1} = a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) a^{n+1-k} b^k.$$
On reconnaît alors la formule du triangle de Pascal, et on peut également remarquer que
$$a^{n+1} = \binom{n+1}{0} a^{n+1-0} b^0 \qquad \text{et} \qquad b^{n+1} = \binom{n+1}{n+1} a^{n+1-(n+1)} b^{n+1}$$
ce qui permet finalement d'écrire
$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.$$
Ainsi, la formule est vraie au rang $n+1$.

Exemple. En utilisant les coefficients binomiaux calculés précédemment, on trouve :

- pour $n = 2$, $(a+b)^2 = a^2 + 2ab + b^2$,
- pour $n = 3$, $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$,
- pour $n = 4$, $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

Remarque. Pour obtenir une expression pour $(a-b)^n$, il suffit de développer $(a+(-b))^n$ avec la formule précédente. Par exemple pour $n = 5$ on trouve

$$(a-b)^5 = a^5 + 5a^4 \times (-b) + 10a^3 \times (-b)^2 + 10a^2 \times (-b)^3 + 5a \times (-b)^4 + (-b)^5$$

soit, après simplifications,

$$(a-b)^5 = a^5 - 5a^4b + 10a^3b^2 - 10a^2b^3 + 5ab^4 - b^5.$$

Chapitre II.

Logique

▷ *MA11, module 1 — Logique*

Définition 1. Une **assertion** est une phrase soit ____, soit _____, pas les deux en même temps.

Exemple.

- « $2+2=4$ » est une assertion (qui est ____),
- « $2\times 3=7$ » est une assertion (qui est _____).
- « Pour tout $x\in\mathbb{R}$, on a $x^2\geqslant 0$ » (qui est ____),
- « Pour tout $z\in\mathbb{C}$, on a $|z|=1$ » (qui est fausse [1]).

Définition 2. Soient P et Q deux assertions.

- On définit l'assertion « P et Q » comme étant l'assertion qui est vraie si P est ____ et Q est ____, et fausse sinon.
- On définit l'assertion « P ou Q » comme étant l'assertion qui est vraie si l'une au moins des deux assertions P ou Q est ____, et fausse si les deux assertions P et Q sont _____.

P \ Q	V	F
V		
F		

Table de vérité de « P et Q »

P \ Q	V	F
V		
F		

Table de vérité de « P ou Q »

Définition 3. Soit P une assertion. On définit l'assertion « $\mathrm{non}\ P$ » comme l'assertion qui est vraie si P est _____, et fausse si P est ____. On l'appelle la **négation** de l'assertion P.

P	V	F
$\mathrm{non}\ P$	F	V

Exemple. La négation de l'assertion P : « $x\geqslant 1$ » est l'assertion $(\mathrm{non}\ P)$: « $x<1$ ».

1. L'ensemble $\mathbb{C}$ des nombres complexes et la notation $|z|$ seront vues dans le chapitre V.

Définition 4. (Implication) Soient P et Q deux assertions. On note « $P \implies Q$ » l'assertion

« ____________ ».

L'implication « $P \implies Q$ » se lit « P *implique* Q » ou « *si* P *alors* Q ».

P \ Q	V	F
V		
F		

Table de vérité de « $P \implies Q$ ».

Exemple.

1. Pour tout $x \in \mathbb{R}$, l'assertion
$$\text{« } 0 \leqslant x \leqslant 25 \implies \sqrt{x} \leqslant 5 \text{ »}$$
est ____ . En effet, on peut distinguer deux cas de figure :
   - si x est compris entre 0 et 5, alors l'assertion « $0 \leqslant x \leqslant 25$ » est ____ , or on sait de plus (par croissance de la fonction racine carrée) que l'assertion « $\sqrt{x} \leqslant 5$ » est également ____ ,
   - sinon, l'assertion « $0 \leqslant x \leqslant 25$ » est ____ et dans ce cas on peut immédiatement affirmer que l'implication est vraie.
2. De même, l'assertion
$$\text{« } x \in]-\infty, -4[\implies x^2 + 3x - 4 > 0 \text{ »}$$
est ____ pour n'importe quelle valeur de $x \in \mathbb{R}$.
3. En revanche, l'assertion
$$\text{« } \sin(\theta) = 0 \implies \theta = 0 \text{ »}$$
n'est pas toujours vraie. Par exemple, pour $\theta = \pi$, l'assertion « $\sin(\theta) = 0$ » est ____ mais l'assertion « $\theta = 0$ » est ____ , donc par définition l'implication est fausse.

Remarque. En particulier, notez bien que l'implication « $P \implies Q$ » est **vraie** dès lors que P est fausse.

Définition 5. (Équivalence) Soient P et Q deux assertions. On note « $P \iff Q$ » l'assertion

« __________________ ».

L'assertion « $P \iff Q$ » se lit « P *équivaut à* Q » ou « P *si et seulement si* Q ».

P \ Q	V	F
V		
F		

Table de vérité de « $P \iff Q$ ».

Exemple. L'assertion
$$\text{« } x \times x' = 0 \iff (x = 0 \text{ ou } x' = 0) \text{ »}$$
est vraie pour tous $x, x' \in \mathbb{R}$.

Proposition 1.
Soient P, Q, R des assertions.

1. $P \iff \text{non}(\text{non}(P))$,
2. $(P \text{ et } Q) \iff (Q \text{ et } P)$,
3. $\text{non}(P \text{ et } Q) \iff$ ____________ ,
4. $(P \text{ et } (Q \text{ ou } R)) \iff$ ____________ ,
5. ________ $\iff (\text{non}(Q) \Rightarrow \text{non}(P))$,
6. $(P \text{ ou } Q) \iff (Q \text{ ou } P)$,
7. $\text{non}(P \text{ ou } Q) \iff$ ____________ ,
8. $(P \text{ ou } (Q \text{ et } R)) \iff$ ____________ .

Définition 6. L'assertion « $\text{non}(Q) \implies \text{non}(P)$ » s'appelle la **contraposée** de l'implication « $P \implies Q$ ».

Démonstration. (Proposition 1.3) Commençons par construire la table de vérité de « $\text{non}(P \text{ et } Q)$ » :

P	Q	P et Q	$\text{non}(P \text{ et } Q)$
V	V	V	**F**
V	F	F	**V**
F	V	F	**V**
F	F	F	**V**

Construisons ensuite la table de vérité de « $(\text{non } P)$ ou $(\text{non } Q)$ » :

P	Q	$\text{non } P$	$\text{non } Q$	$(\text{non } P)$ ou $(\text{non } Q)$
V	V	F	F	**F**
V	F	F	V	**V**
F	V	V	F	**V**
F	F	V	V	**V**

On voit que dans chaque cas de figure, les assertions « $\text{non}(P \text{ et } Q)$ » et « $(\text{non } P)$ ou $(\text{non } Q)$ » ont même valeur de vérité (c'est-à-dire qu'elles sont soit toutes les deux vraies, soit toutes les deux fausses), on en déduit donc qu'elles sont équivalentes.

On a vu dans certains exemples plus haut qu'une assertion pouvait dépendre d'un paramètre. Par exemple l'assertion $P(x)$: « $x^2 \geqslant 1$ » est une assertion qui sera vraie ou fausse suivant la valeur de x. À partir d'assertions dépendant d'un paramètre, on peut construire de nouvelles assertions à l'aide des *quantificateurs* $\forall$ (*pour tout*) et $\exists$ (*il existe*).

Définition 7. Soit $P(x)$ une assertion dépendant d'un paramètre $x \in E$. On définit :

- l'assertion « $\forall x \in E, P(x)$ » comme l'assertion qui est vraie si les assertions $P(x)$ sont vraies pour ____ les éléments x de l'ensemble E, et fausse sinon,
- l'assertion « $\exists x \in E, P(x)$ » comme l'assertion qui est vraie si l'on peut trouver ________ élément x de l'ensemble E pour lequel $P(x)$ est vraie, et fausse sinon.

Exemple.

1. À partir de l'assertion « $x^2 \geqslant 1$ », on peut définir les assertions suivantes :
   - « $\forall x \in [1, +\infty[\,, x \geqslant 1$ » (qui est ____),
   - « $\forall x \in \mathbb{R}, x \geqslant 1$ » (qui est _____),
   - « $\exists x \in [1, +\infty[\,, x \geqslant 1$ » (qui est vraie),
   - « $\exists x \in \mathbb{R}, x \geqslant 1$ » (qui est vraie),
2. L'assertion « $\forall n \in \mathbb{N}, n(n+1)$ est divisible par 2 » est vraie.
3. L'assertion « $\exists x \in \mathbb{R}, x(x-1) < 0$ » est ____.
4. L'assertion « $\exists n \in \mathbb{N}, n^2 - n > n$ » est ____.
5. L'assertion « $\exists x \in \mathbb{R}, x^2 = -1$ » est _____.

Proposition 2. Soit $P(x)$ une assertion dépendant d'un paramètre $x \in E$. Alors :

- la négation de « $\forall x \in E, P(x)$ » est « ________________ »,
- la négation de« $\exists x \in E, P(x)$ » est « ________________ ».

Exemple.

1. La négation de « $\forall x \in [1, +\infty[\,, x^2 \geqslant 1$ » est « ________________ ».
2. La négation de « $\exists z \in \mathbb{C}, z^2 + z + 1 = 0$ » est « ________________ ».
3. La négation de « $\forall x \in \mathbb{R}, x + 1 \in \mathbb{Z}$ » est « ________________ ».
4. La négation de « $\forall x \in \mathbb{R}, \exists y > 0, x + y > 10$ » est « ____________________ ».

Remarque.

1. L'ordre des quantificateurs $\forall$ et $\exists$ est important. Par exemple :
   - « $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$ » est ____,
   - « $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x + y > 0$ » est _____.
2. L'assertion « $\exists x \in E, P(x)$ » est vraie dès lors que $P(x)$ est vraie pour *au moins* un élément $x \in E$, mais il peut y avoir plusieurs éléments x qui conviennent. Si on veut préciser qu'il n'existe qu'un seul $x \in E$ pour lequel $P(x)$ est vraie, on note
$$« \exists!\, x \in E,\ P(x) ».$$
3. Attention lorsque vous faites la négation d'inégalités. La négation d'une inégalité stricte donne une inégalité large (et vice-versa).
4. Les quantificateurs $\forall$ et $\exists$ ainsi que les symboles $\Rightarrow$ et $\Leftrightarrow$ ne sont **pas** des abréviations et ne doivent pas être utilisés comme telles !

5. Les symboles $\nexists$ et $\not\Longrightarrow$ sont à éviter car il peuvent créer des ambiguïtés. Il faut privilégier les autres symboles vus dans ce chapitre qui suffiront toujours à exprimer la même idée de manière non-ambigüe.

Chapitre III.

Ensembles et applications

III.1. Opérations générales sur les ensembles

▷ *MAI1, module 3 — Ensembles*

III.1.1. Définition d'un ensemble

La définition d'un *ensemble* à proprement parler est une question trop compliquée pour être exposée simplement en première année (voir par exemple le *paradoxe de* RUSSEL). Heureusement, vous connaissez déjà des exemples d'ensembles :

- l'ensemble des entiers naturels : ______________,
- l'ensemble des entiers relatifs : ______________________,
- l'ensemble des entiers rationnels : ________________________,
- l'ensemble des réels $\mathbb{R}$, contenant par exemple ___________,
- l'ensemble des nombres complexes[1] $\mathbb{C}$.

Pour ce module, il vous suffira de penser un *ensemble* comme une collection de plusieurs éléments.

Exemple.

- L'ensemble $\{0, 1\}$ formée des nombres 0 et 1.
- L'ensemble $\{rouge, noir\}$.
- L'ensemble $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (et plus généralement tous les ensembles évoqués plus haut).

Définition 1. On appelle **ensemble vide** l'ensemble ______________________. On le note __.

Définition 2. On note _____ si x est un élément de l'ensemble E. Dans le cas contraire, on note _____.

Dans l'exemple précédent, les ensembles ont été défini en énumérant simplement leurs éléments, mais on peut parfois aussi définir un ensemble via une propriété commune.

Exemple.

- L'ensemble
$$\{x \in \mathbb{R} \mid |x - 2| < 1\}$$
est l'ensemble formé de tous les réels $x \in \mathbb{R}$ tels que $|x - 2|$ est strictement inférieur à 1.
- L'ensemble
$$\{z \in \mathbb{C} \mid z^5 = 1\}$$

1. Si vous ne connaissez pas encore cet ensemble, pas de panique ! Il sera introduit plus tard dans ce module.

est l'ensemble formé de tous les nombres complexes qui, lorsqu'on les élèves à la puissance 5, donnent 1.

- L'ensemble
$$\{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\}$$
est l'ensemble de tous les réels compris (au sens large) entre 0 et 1. Autrement dit, c'est l'ensemble souvent noté plus simplement $[0, 1]$.

III.1.2. Appartenance et inclusion

Définition 3. Soit E et F deux ensembles. On dit que E est **inclus** dans F, et on note ______, si

______

(autrement dit si tout élément de E est un élément de F).

Dans ce cas, on dit aussi que E est un ______ de F ou encore que E est une ______ de F.

Définition 4. Soient E et F deux ensembles. On dit que E et F sont **égaux**, et on note $E = F$, si

______

Définition 5. Soit E un ensemble. L'**ensemble des parties** de E, noté ______, est l'ensemble qui contient ______.

Exemple. Si $E = \{1, 2, 3\}$, alors l'ensemble des parties de E est :

$$\mathcal{P}(\{1, 2, 3\}) = \{\qquad\qquad\qquad\qquad\}.$$

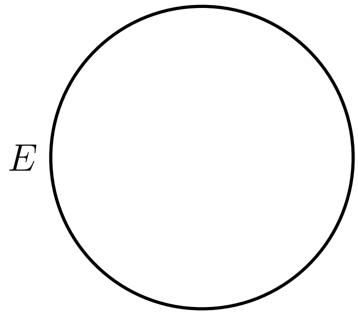
III.1.3. Complémentaire, union et intersection

Définition 6. Soit E un ensemble, et soit $A \subset E$ une partie de E. Le **complémentaire** de A dans E, noté ______, est l'ensemble

______

(autrement dit c'est l'ensemble formé de tous les éléments de E qui ______).

On peut aussi le noter $E \setminus A$, ou encore seulement $\complement A$, $\bar{A}$ ou A^c lorsqu'il n'y a pas d'ambiguïté sur l'ensemble E dont on parle.



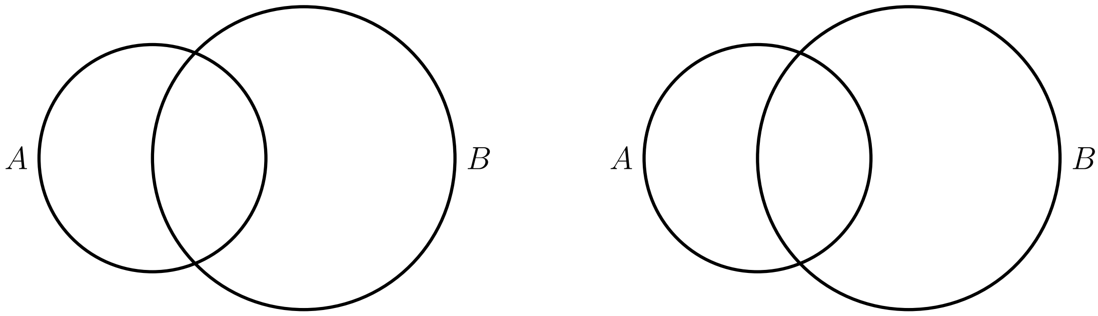
Définition 7. Soient A et B deux sous-ensembles d'un ensemble E.

- L'**union** de A et B, notée ______, est l'ensemble

  ____

- L'**intersection** de A et B, notée ______, est l'ensemble

  ______________________________ .



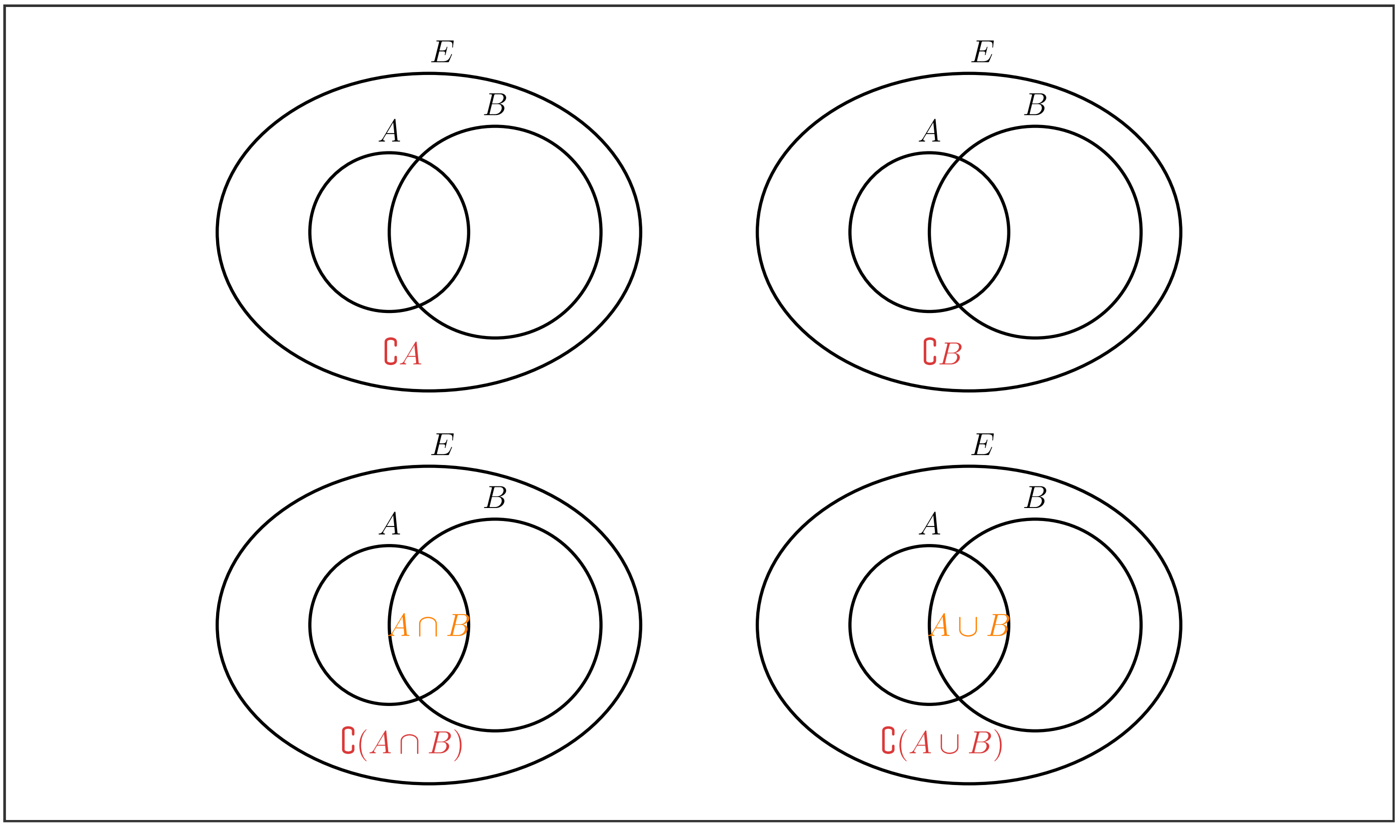
Proposition 1. Soient A, B, C trois sous-ensembles d'un ensemble E.

1. $A \cap (B \cap C) =$ ______________
2. $A \cup (B \cup C) =$ ______________
3. $A \cap (B \cup C) =$ ______________
4. $A \cup (B \cap C) =$ ______________

Remarque. Les propriétés 1 et 2 ci-dessus montrent que si on ne manipule que des unions d'ensembles (ou que des intersections), alors on peut écrire les expressions sans parenthèses car l'ordre des opérations n'a pas d'importance. En revanche, ce n'est plus vrai dès lors qu'on mélange des unions et des intersections !

Proposition 2. Soit A et B deux sous-ensembles d'un ensemble E.

1. $\complement(\complement A) =$ __
2. $A \subset B \iff$ __________
3. $\complement(A \cap B) =$ __________
4. $\complement(A \cup B) =$ __________



Démonstration. (Proposition 1.3.) Soit $x \in E$. On a :

$$\begin{aligned} x \in A \cap (B \cup C) &\Longleftrightarrow x \in A \text{ et } x \in (B \cup C) \\ &\Longleftrightarrow \underline{\hspace{6cm}} \\ &\Longleftrightarrow \underline{\hspace{8cm}} \\ &\Longleftrightarrow \underline{\hspace{6cm}} \\ &\Longleftrightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

On en déduit que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Démonstration. (Proposition 2.3.) Soit $x \in E$. On a :

$$\begin{aligned} x \in \complement(A \cap B) &\Longleftrightarrow \underline{\hspace{4cm}} \\ &\Longleftrightarrow \underline{\hspace{5cm}} \\ &\Longleftrightarrow \underline{\hspace{6cm}} \\ &\Longleftrightarrow \underline{\hspace{4cm}} \\ &\Longleftrightarrow \underline{\hspace{4cm}} \end{aligned}$$

On en déduit que $\underline{\hspace{5cm}}$.

III.1.4. Produit cartésien

Définition 8. Soient E et F deux ensembles. Le **produit cartésien** de E et F, noté ______, est l'ensemble

______________________ .

Exemple.

1. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R},\ y \in \mathbb{R}\}$
2. $[0, 1] \times \mathbb{R} = \{(x, y) \mid 0 \leqslant x \leqslant 1,\ y \in \mathbb{R}\}$
3. $[0, 1] \times [0, 1] \times [0, 1] = \{(x, y, z) \mid 0 \leqslant x, y, z \leqslant 1\}$

III.2. Applications et ensembles associés

▷ *MA11, module 4 — Applications : image directe, image réciproque et antécédents*

III.2.1. Définitions générales

Définition 9. Soient E et F deux ensembles. Une **application** (ou **fonction**) $f : E \to F$ est la donnée, pour chaque élément ______, d'un unique élément de __ noté ____.

On dit alors que E est l'**ensemble de départ** de l'application f, et F son **ensemble d'arrivée**.

On peut schématiser une application ...

... à l'aide de « patates » :

... à l'aide d'un graphe :

Remarque. *Pour pouvoir représenter $f : E \to F$ à l'aide d'un graphe, il faut que E et F soient des sous-ensembles de $\mathbb{R}$.*

Définition 10. Deux applications f et g de E dans F sont **égales** si

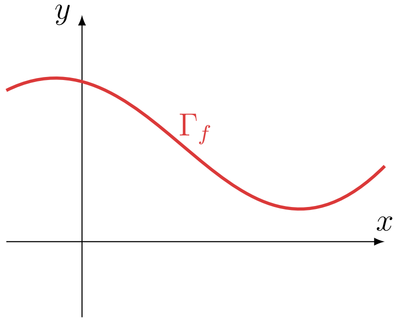
____

Définition 11. Soit $f : E \to F$ une application. Le **graphe** de l'application f est l'ensemble :

$$\Gamma_f = \underline{\qquad\qquad\qquad\qquad\qquad}.$$

C'est un sous-ensemble du produit cartésien ______.

Vous avez déjà rencontré la notion de graphe dans le cas d'une fonction $f : \mathbb{R} \to \mathbb{R}$:



III.2.2. Composition de fonctions

Définition 12. Soient $f : E \to F$ et $g : F \to G$ deux applications. L'application **composée** $g \circ f : E \to G$ est l'application définie par

$$\forall x \in E, \quad g \circ f(x) = \underline{\qquad\qquad}.$$

Exemple.

1. Si E est un ensemble, l'**identité** de E est l'application $\mathrm{id}_E : E \to E$ définie par ______.
2. Si f et g sont les fonctions définies par

$$f : \left| \begin{array}{ccc}]0;+\infty[& \to &]0;+\infty[\\ x & \longmapsto & \frac{1}{x} \end{array} \right. \qquad g : \left| \begin{array}{ccc}]0;+\infty[& \to & \mathbb{R} \\ x & \longmapsto & \frac{x-1}{x+1} \end{array} \right.$$

alors l'application $g \circ f :]0;+\infty[\to \mathbb{R}$ vérifie

$$\forall x \in]0;+\infty[, \quad g \circ f(x) =$$

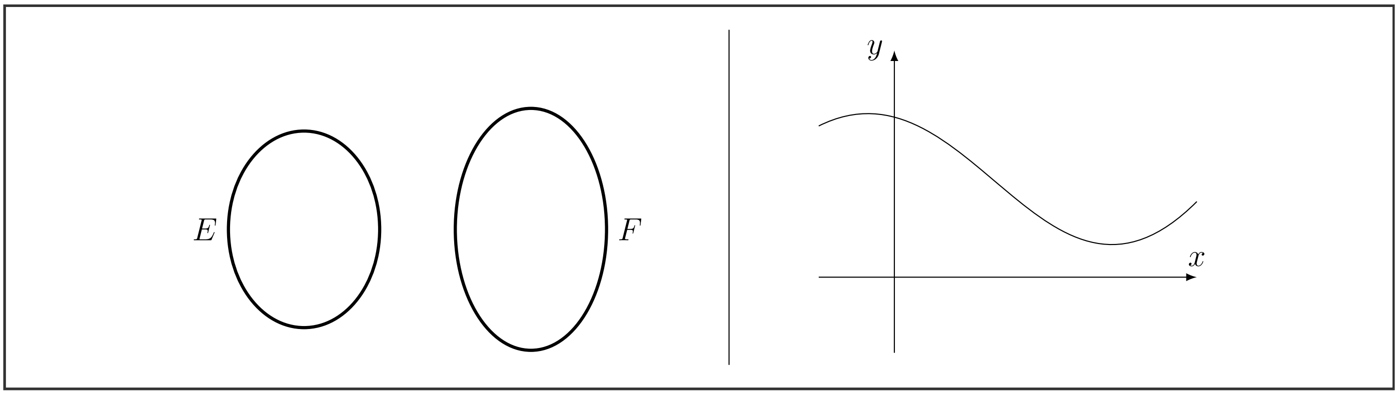
III.2.3. Image directe et image réciproque

Définition 13. Soit $f : E \to F$ une application, et soit $A \subset E$.

L'**image directe** de A par f, notée ______, est l'ensemble

$$\underline{\qquad\qquad\qquad\qquad\qquad}.$$

C'est un sous-ensemble de ____________.

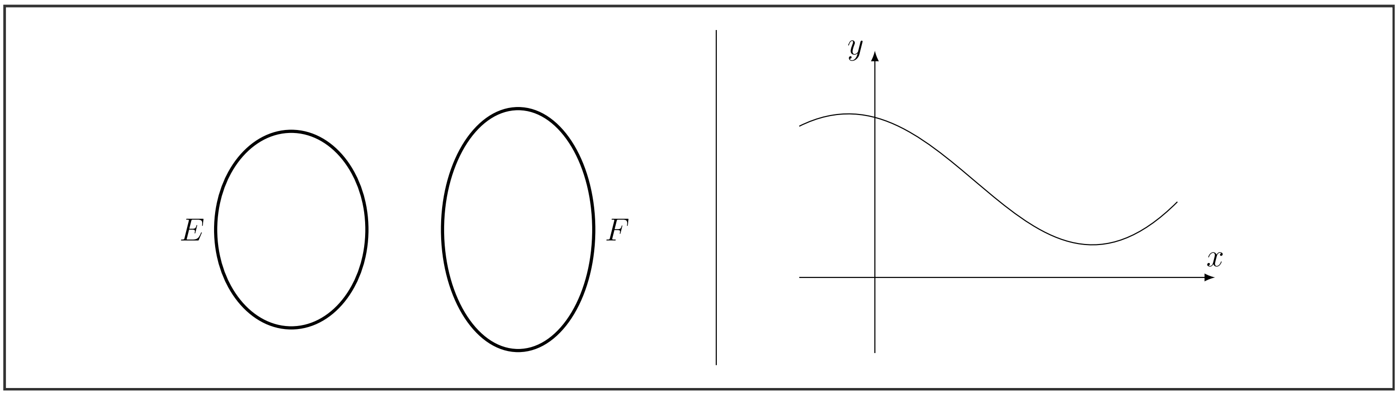


Définition 14. Soit $f : E \to F$ une application, et soit $B \subset F$.

L'**image réciproque** de B par f, notée ______, est l'ensemble

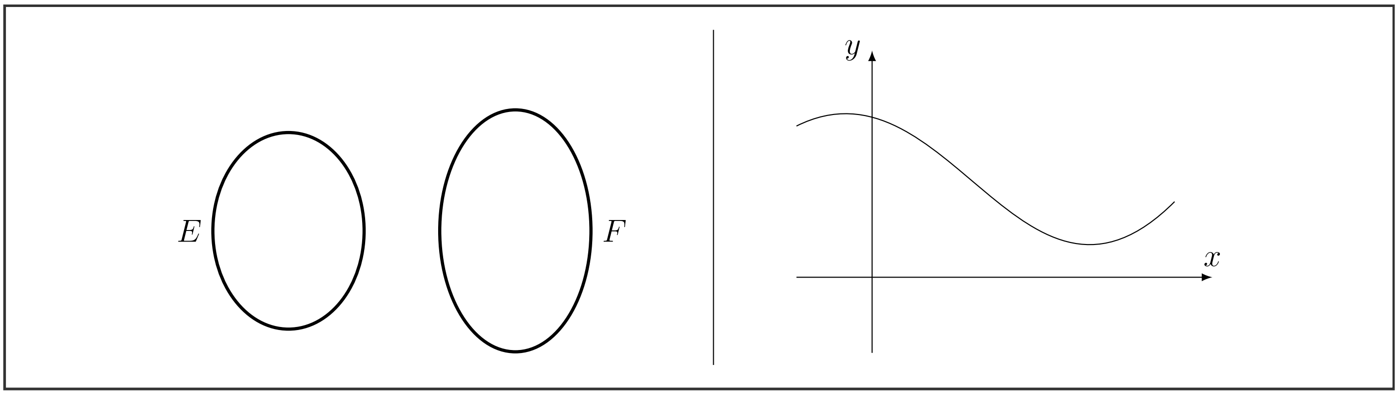
______________________ .

C'est un sous-ensemble de ________________ .



Définition 15. Soit $f : E \to F$ une application, et soit $y \in F$.

Un élément $x \in E$ tel que ______ est appelé un **antécédent** de y par f.



III.3. Injection, surjection et bijection

▷ *MAI1, module 5 — Injection, surjection et bijection*

III.3.1. Injection et surjection

Définition 16. Soit $f : E \to F$ une application. On dit que f est **injective** si

$$\forall\, (x, x') \in E^2, \quad (\underline{\hspace{3cm}} \implies \underline{\hspace{1.5cm}}).$$

Remarque. Par contraposée, f est injective signifie que, pour tout $(x, x') \in E^2$, si x est différent de x' alors ______________.

Définition 17. Soit $f : E \to F$ une application. On dit que f est **surjective** si

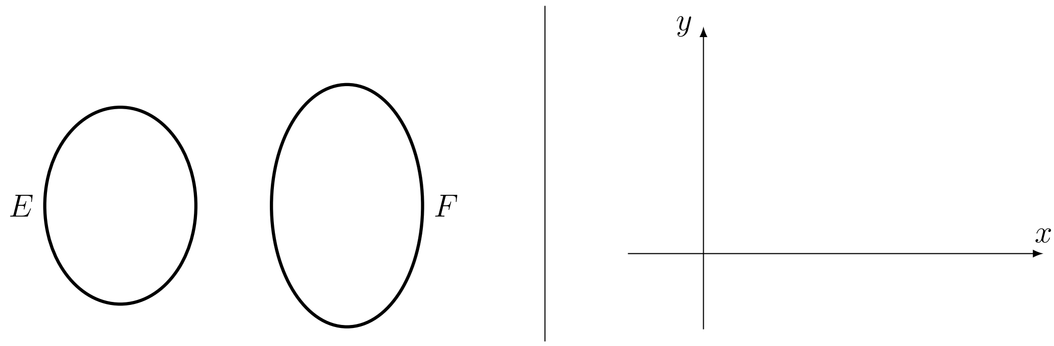
$$\forall \underline{\hspace{1.5cm}}, \quad \exists \underline{\hspace{1.5cm}}, \quad \underline{\hspace{2cm}}.$$

Remarque. En utilisant la notion d'image directe définie plus haut, on peut dire qu'une application $f : E \to F$ est surjective si et seulement si ________.

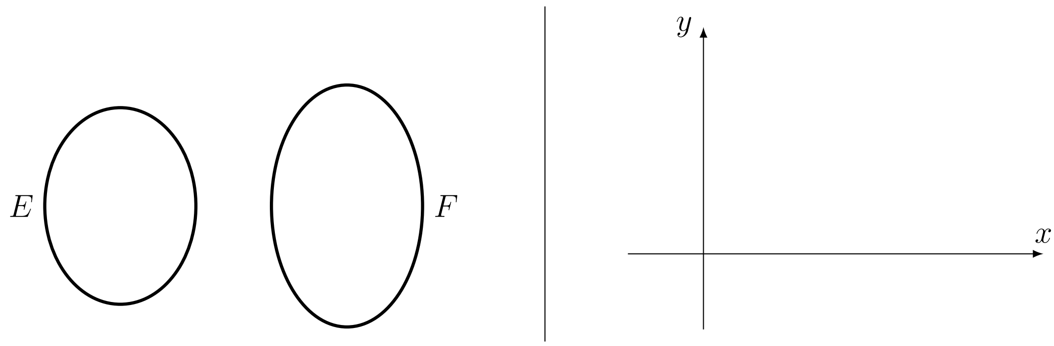
Remarque. Soit $f : E \to F$ une application. En utilisant le vocabulaire des antécédents :

- f est injective si et seulement si tout élément $y \in F$ possède ________ antécédent par f,
- f est surjective si et seulement si tout élément $y \in F$ possède ________ antécédent par f.

Exemples d'applications non-injectives :



Exemples d'applications non-surjectives :



Exemple. Soit $f_1 : \mathbb{N} \to \mathbb{Q}$ définie par

$$f_1(x) = \frac{1}{1+x}.$$

- La fonction f_1 est injective. En effet, soient $x, x' \in \mathbb{N}$ tels que $f_1(x) = f_1(x')$. On a donc

$$\frac{1}{1+x} = \frac{1}{1+x'}$$

donc $1 + x = 1 + x'$ et donc $x = x'$.

- La fonction f_1 n'est pas surjective. Comme on a toujours $f_1(x) \leqslant 1$ (*sauriez-vous le démontrer rigoureusement ?*), alors par exemple ____ n'a pas d'antécédent.

Exemple. Soit $f_2 : \mathbb{Z} \to \mathbb{N}$ définie par $f_2(x) = x^2$.

- La fonction f_2 n'est pas injective. En effet, si on prend $x =$ __ et $x' =$ _, alors on trouve $f(x) = f(x') =$ _ et pourtant $x \neq x'$.
- La fonction f_2 n'est pas surjective. Par exemple, l'élément $y =$ _ $\in \mathbb{N}$ n'a pas d'antécédent dans $\mathbb{Z}$ (les seuls nombres x tels que $x^2 = y$ sont __ et ___ et aucun des deux n'est entier).

III.3.2. Bijection

Définition 18. Soit $f : E \to F$ une application. On dit que f est **bijective** si f est à la fois ______ et ______.

Autrement dit, $f : E \to F$ est bijective si et seulement si

$$\forall \_\_\_\_, \quad \exists! \_\_\_\_, \quad \_\_\_\_\_\_.$$

Remarque. Soit $f : E \to F$ une application. En utilisant le vocabulaire des antécédents, f est bijective si et seulement si tout élément $y \in F$ possède ______ antécédent par f.

Proposition 3. Soit $f : E \to F$ une application.

1. L'application f est bijective si et seulement si il existe une application $g :$ _ $\to$ _ telle que $f \circ g =$ __ et $g \circ f =$ __.
2. Si f est bijective, alors cette application g est unique. On l'appelle la **bijection réciproque** (ou **inverse**) de f et on la note f^{-1}.
   De plus, cette application f^{-1} est elle-aussi bijective, et $(f^{-1})^{-1} =$ _.

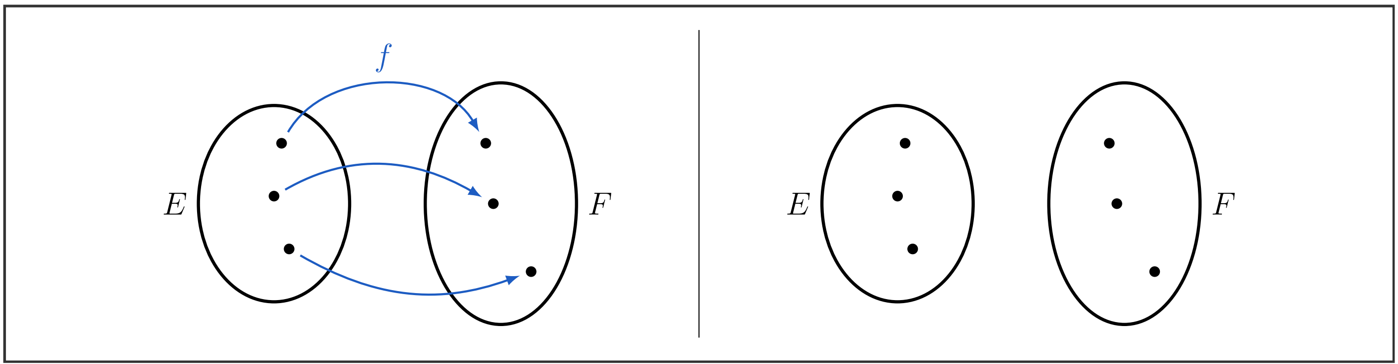
Remarque.

- La condition $f \circ g =$ __ est une égalité entre fonctions, et est donc équivalente à

  ____________.

- De même, la condition $g \circ f =$ ____ est équivalente à

  ______________________.



Exemple. Soit $f : \mathbb{R} \to]0;+\infty[$ définie par $f(x) = \exp(x)$. Sa bijection réciproque est l'application $g :]0;+\infty[\to \mathbb{R}$ définie par $g(y) = \ln(y)$. En effet, on a les égalités bien connues :

$$\forall\, y \in]0;+\infty[\,, \quad \exp(\ln(y)) = y \qquad \text{et} \qquad \forall\, x \in \mathbb{R}, \quad \ln(\exp(x)) = x.$$

Graphiquement, le graphe de f et le graphe de g sont ______________________.

Proposition 4. Soient $f : E \to F$ et $g : F \to G$ des applications. Si f et g sont bijectives, alors $g \circ f$ est bijective et

$$(g \circ f)^{-1} = \underline{\qquad\qquad}.$$

Démonstration. (Proposition 3)

1. On raisonne par double implication.
   - **Preuve du sens « $\Rightarrow$ ».**
     Supposons f bijective et construisons explicitement g. Soit $y \in F$. Comme f est bijective, elle est en particulier surjective et donc il existe un $x \in E$ tel que $y = f(x)$. On pose alors $g(y) = x$. On a donc $f(g(y)) = f(x) = y$. La fonction g ainsi construite vérifie donc $f \circ g = \mathrm{id}_F$.
     De plus, en composant (à droite) par f, on trouve donc $f \circ g \circ f = \mathrm{id}_F \circ f = f$, c'est-à-dire

     $$\forall\, x \in E, \quad f(g(f(x))) = f(x).$$

     Comme f est bijective, elle est en particulier injective et donc on peut en déduire que

     $$\forall\, x \in E, \quad g(f(x)) = x$$

     autrement dit que $g \circ f = \mathrm{id}_E$.
   - **Preuve du sens « $\Leftarrow$ ».**
     Supposons qu'une telle application g existe, et montrons qu'alors f est bijective.
     — **Surjectivité de f.** Soit $y \in F$. Posons $x = g(y) \in E$. On a alors :

     $$f(x) = f(g(y)) = f \circ g(y) = \mathrm{id}_F(y) = y$$

     en utilisant l'hypothèse que $f \circ g = \mathrm{id}_F$. Ceci prouve que x est un antécédent de y par f. Comme cette démonstration est valable pour tout élément $y \in F$, on en déduit que f est surjective.

— **Injectivité de f.** Soient $x, x' \in E$. Supposons que $f(x) = f(x')$. On en déduit que $g(f(x)) = g(f(x'))$, c'est-à-dire que
$$g \circ f(x) = g \circ f(x').$$
En utilisant l'hypothèse que $g \circ f = \mathrm{id}_E$, on trouve donc finalement que $x = x'$. Ainsi, f est injective.

Comme f est à la fois injective et surjective, elle est bijective.

2. *Cette démonstration n'apparaît pas dans les vidéos, mais on la donne pour la culture. Elle n'est pas compliquée d'un point de vue technique mais elle demande de bien comprendre les objets manipulés. N'hésitez donc pas à y revenir dessus plus tard, une fois que vous aurez bien compris la démonstration précédente et les notions en jeu.*

D'abord, pour montrer que l'application g est unique, on suppose qu'il existe deux telles applications g_1 et g_2 vérifiant les hypothèse données, et on montre que ce sont les mêmes. Pour tout $y \in F$, on a :
$$g_1(y) = g_1 \circ \mathrm{id}_F(y) = g_1 \circ f \circ g_2(y) = \mathrm{id}_E \circ g_2(y) = g_2(y)$$
(en utilisant les hypothèses $f \circ g_2 = \mathrm{id}_F$ et $g_1 \circ f = \mathrm{id}_E$, et en utilisant aussi implicitement le fait que la composition de fonctions est *associative*, c'est-à-dire que $g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2$). Ceci revient donc à dire que $g_1 = g_2$.

Ensuite, pour la seconde partie de l'énoncé, posons $h = f$. On a alors :
$$h \circ g = f \circ g = \mathrm{id}_F \qquad \text{et} \qquad g \circ h = g \circ f = \mathrm{id}_E\,.$$
Ces égalités découlent simplement des hypothèses vérifiées par g, mais en reprenant le point 1. de la proposition, cela prouve aussi que la fonction g (c'est-à-dire la fonction notée f^{-1}) est bijective, et que sa bijection réciproque est h (c'est-à-dire simplement la fonction f de départ).

III.4. Ensembles finis

▷ *MAI1, module 6 — Ensembles finis*

III.4.1. Définition d'un ensemble fini et cardinal

Définition 19. Un ensemble E est **fini** s'il existe $n \in \mathbb{N}$ et une bijection de E vers l'ensemble $\{1, 2, \ldots, , n\}$. Ce n est unique, s'appelle le **cardinal** de E (ou le *nombre d'éléments*) et est noté $\operatorname{Card} E$.

Exemple.

- $E = \{\text{rouge}, \text{noir}\}$ est en bijection avec $\{1, 2\}$ et donc $\operatorname{Card} E = 2$.
- $\mathbb{N}$ n'est pas un ensemble fini.

Remarque. Par définition, le cardinal de l'ensemble vide est 0.

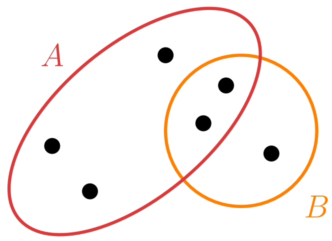
III.4.2. Propriétés du cardinal

Proposition 5. Si A est un ensemble fini et si $B \subset A$, alors :

1. B est aussi fini et $\operatorname{Card} B \leqslant \operatorname{Card} A$,
2. $\operatorname{Card}(A \setminus B) = \operatorname{Card}(A) - \operatorname{Card}(B)$.

Si A, B sont deux ensembles finis, alors :

1. si $A \cap B = \varnothing$, alors $\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B)$,
2. plus généralement, $\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B) - \operatorname{Card}(A \cap B)$.



III.4.3. Cardinal et applications

Proposition 6. Soient E, F deux ensembles finis et soit $f : E \to F$.

1. Si f est injective, alors $\operatorname{Card}(E) \leqslant \operatorname{Card}(F)$.
2. Si f est surjective, alors $\operatorname{Card}(E) \geqslant \operatorname{Card}(F)$.
3. Si f est bijective, alors $\operatorname{Card}(E) = \operatorname{Card}(F)$.

Proposition 7. Soient E, F deux ensembles finis et soit $f : E \to F$.

Si $\operatorname{Card}(E) = \operatorname{Card}(F)$, alors les assertions suivantes sont équivalentes :

1. f est injective,
2. f est surjective,
3. f est bijective.

Remarque. (Principe des tiroirs) Si dans k tiroirs l'on range $n > k$ paires de chaussettes, alors il existe un tiroir contenant (au moins) deux paires de chaussettes.

III.4.4. Cardinal et dénombrement

Proposition 8. Soient E et F deux ensembles finis. Le nombre d'applications différentes de E dans F est égal à

$$\operatorname{Card}(F)^{\operatorname{Card}(E)}.$$

Exemple. En particulier, si E est de cardinal n, le nombre d'applications de E dans lui-même est égal à n^n.

Par exemple si $E = \{1, 2, 3, 4, 5\}$, alors ce nombre est $5^5 = 3125$.

Proposition 9. Soit E un ensemble fini de cardinal n. Le nombre de bijections de E dans E est égal à

$$n! = 1 \times 2 \times 3 \times \cdots \times n.$$

Exemple. On reprend l'exemple de l'ensemble $E = \{1, 2, 3, 4, 5\}$.

Parmi les 3125 applications de E dans lui-même, il y en a $5! = 120$ qui sont bijectives.

Idée de la preuve.

- Pour l'image du premier élément, il y a n choix.
- Pour l'image du deuxième, il y a $n - 1$ choix.
- ...
- Pour l'image du k-ième il y a $n - k + 1$ choix.
- ...
- Pour l'image du n-ième il y a 1 choix.

Proposition 10. Soit E un ensemble de cardinal fini. Il y a $2^{\operatorname{Card} E}$ sous-ensembles de E, autrement dit

$$\operatorname{Card}(\mathcal{P}(E)) = 2^{\operatorname{Card} E}.$$

Exemple. Si $E = \{1, 2, 3, 4, 5\}$, alors il y a $2^5 = 32$ parties de E.

Plus précisément, $\mathcal{P}(E)$ contient :

- 1 ensemble à zéro élément : l'ensemble vide $\varnothing$,
- 5 singletons : $\{1\}, \{2\}, \ldots$
- 10 paires : $\{1, 2\}, \{1, 3\}, \ldots, \{2, 3\}, \ldots$
- 10 triplets : $\{1, 2, 3\}, \{1, 2, 4\}, \ldots$
- 5 ensembles à 4 éléments : $\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \ldots$
- 1 ensemble à 5 éléments : l'ensemble E tout entier.

Définition 20. Le nombre de parties à k éléments d'un ensemble à n éléments est noté

$$\binom{n}{k} \quad \text{ou} \quad C_n^k.$$

Exemple.

- Les parties à $k = 2$ éléments de $\{1,2,3\}$ sont $\{1,2\}$, $\{1,3\}$ et $\{2,3\}$, donc
$$\binom{3}{2} = 3.$$
- Pour $n = 5$ (voir exemple précédent) :
$$\binom{5}{0} = 1, \quad \binom{5}{1} = 5, \quad \binom{5}{2} = 10, \quad \binom{5}{3} = 10, \quad \binom{5}{4} = 5, \quad \binom{5}{5} = 1.$$

Proposition 11.
- Pour tout $k \in \mathbb{N}$,
$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{n} = 1.$$
- Pour tous $0 \leqslant k \leqslant n$,
$$\binom{n}{n-k} = \binom{n}{k}.$$
- Pour tout $n \in \mathbb{N}^*$,
$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n.$$

Proposition 12. Pour tout $0 < k \leqslant n$,
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Idée de la preuve. Soit E un ensemble tel que $\mathrm{Card}(E) = n$, soit $a \in E$ et $E' = E \setminus \{a\}$. Il y a deux sortes de parties $A \subset E$ ayant k éléments :
- celles qui ne contiennent pas a : ce sont donc des parties à k éléments dans E', qui possède $n-1$ éléments, il y en a donc $\binom{n-1}{k}$,
- celles qui contiennent a : elles sont de la forme $A = \{a\} \cup A'$ avec A' une partie à $k-1$ éléments dans E', il y en a $\binom{n-1}{k-1}$.

Bilan : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Relations utilisées :

$$\binom{n}{0} = 1 \qquad \binom{n}{n} = 1$$

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

Proposition 13. Pour tout $0 \leqslant k \leqslant n$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Idée de la preuve. On démontre par récurrence sur $n \in \mathbb{N}^*$ la propriété

$$P(n) : \text{« Pour tout } k \in [\![0, n]\!], \quad \binom{n}{k} = \frac{n!}{k!(n-k)!} \text{ ».}$$

- **Initialisation.** La propriété est vraie pour $n = 1$.
- **Hérédité.** Soit $n \geqslant 2$ un entier. Supposons $P(n-1)$ vraie et montrons que $P(n)$ est vraie.

  Pour $k = 0$, on a clairement
  $$\frac{n!}{0!(n-0)!} = 1 = \binom{n}{0}.$$
  Pour tout $0 < k \leqslant n$, on a (en utilisant l'hypothèse de récurrence) :
  $$\begin{aligned}\binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k} \\ &= \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!((n-1)-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{1}{n-k} + \frac{1}{k}\right) \\ &= \frac{n!}{k!(n-k)!}\end{aligned}$$

Théorème 1. (Formule du binôme de Newton) Pour tout $(a, b) \in \mathbb{R}^2$ et pour tout $n \in \mathbb{N}^*$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Exemple.

1. Pour $n = 2$, on retrouve $(a+b)^2 = a^2 + 2ab + b^2$.
2. Pour $n = 3$, on obtient $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
3. Pour $a = 1$ et $b = 1$, on retrouve l'égalité

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Chapitre IV.

Nombres réels

IV.1. Propriétés des nombres réels

▷ *MA12, module 1 — Nombres réels*

IV.1.1. Quelques considérations formelles

Proposition 1. $(\mathbb{R}, +, \times)$ est un *corps commutatif*.

Remarque. La notion de *corps commutatif* n'est **pas à connaître**. Sans rentrer dans les détails, cela signifie grossièrement que les opérations d'addition et de multiplication sur $\mathbb{R}$ vérifient les relations « naturelles » suivantes :

- $a + b = b + a$,
- $0 + a = a$,
- $a + b = 0 \iff a = -b$,
- $(a + b) + c = a + (b + c)$,
- $a \times (b + c) = a + (b + c)$,
- $a \times b = b \times a$,
- $1 \times a = a$ si $a \neq 0$,
- $ab = 1 \iff a = \frac{1}{b}$,
- $(a \times b) \times c = a \times (b \times c)$,
- $a \times b = 0 \iff (a = 0 \text{ ou } b = 0)$.

Proposition 2. La relation $\leqslant$ sur $\mathbb{R}$ vérifie les propriétés suivantes :

- elle est **réflexive**, c'est-à-dire que
$$\forall x \in \mathbb{R}, \quad x \leqslant x,$$
- elle est **antisymétrique**, c'est-à-dire que
$$\forall x, y \in E, \quad (x \leqslant y \text{ et } y \leqslant x) \implies x = y,$$
- elle est **transitive**, c'est-à-dire que
$$\forall x, y, z \in E, \quad (x \leqslant y \text{ et } y \leqslant z) \implies x \leqslant z.$$

Remarque. La proposition précédente se résume en disant que $\leqslant$ est une *relation d'ordre* sur $\mathbb{R}$. Ce vocabulaire n'est **pas à connaître**, mais en réalité vous avez déjà manipulé ces notions sans y avoir particulièrement mis de nom dessus. Par exemple, vous saviez déjà (sans le dire ainsi) que la relation $\subset$ sur l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E quelconque est elle aussi une relation d'ordre. En effet :

- $\forall A \in \mathcal{P}(E), \quad A \subset A$,
- $\forall A, B \in \mathcal{P}(E), \quad (A \subset B \text{ et } B \subset A) \implies A = B$,
- $\forall A, B, C \in \mathcal{P}(E), \quad (A \subset B \text{ et } B \subset C) \implies A \subset C$.

De plus la relation d'ordre $\leqslant$ sur $\mathbb{R}$ est *totale*, c'est-à-dire que deux éléments quelconques peuvent toujours être mis en relation dans un sens ou dans l'autre. Plus rigoureusement on a :

$$\forall\, x, y \in E, \quad (x \leqslant y \text{ ou } y \leqslant x).$$

Ce n'est pas le cas de la relation $\subset$ sur $\mathcal{P}(E)$: on peut en général trouver deux parties $A, B \in \mathcal{P}(E)$ telles qu'on n'ait ni $A \subset B$, ni $B \subset A$.

Proposition 3. La relation $\leqslant$ est « compatible » avec l'addition et la mulitiplication sur $\mathbb{R}$, c'est-à-dire que pour tous $a, b, c, d \in \mathbb{R}$ on a :

- $(a \leqslant b \text{ et } c \leqslant d) \implies a + c \leqslant b + d,$
- $(a \leqslant b \text{ et } c \geqslant 0) \implies a \times c \leqslant b \times c,$
- $(a \leqslant b \text{ et } c \leqslant 0) \implies a \times c \geqslant b \times c.$

Proposition 4. L'ensemble $\mathbb{R}$ est *archimédien*, c'est-à-dire que

$$\forall\, x \in \mathbb{R}, \quad \exists\, n \in \mathbb{N}, \quad n > x.$$

Remarque. Cette dernière notion théorique n'est pas à connaître non plus, mais elle est mentionnée ici car c'est elle qui justifie la définition qui suit.

IV.1.2. Partie entière

Proposition 5. Soit $x \in \mathbb{R}$. Il existe un unique entier, noté $E(x)$, appartenant à $\mathbb{Z}$ et tel que

$$\underline{\qquad\qquad\qquad\qquad}\,.$$

Ce nombre $E(x)$ est appelé la **partie entière** de x.

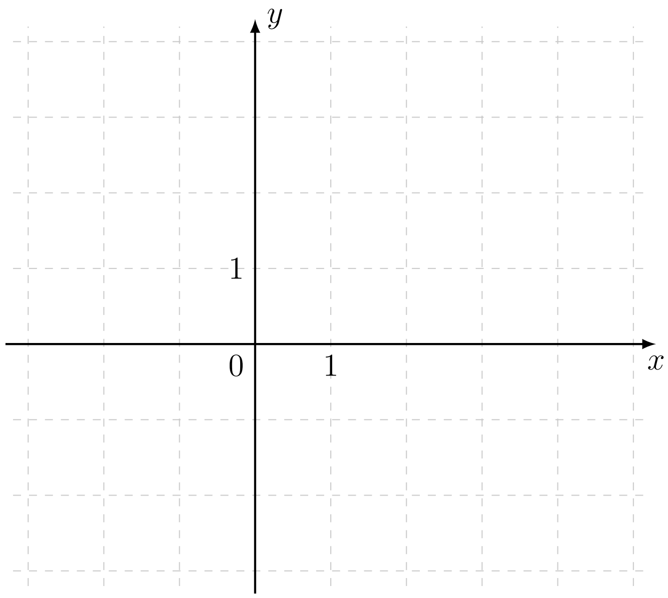
Remarque. La partie entière d'un nombre x est ainsi, par définition, le plus grand entier relatif inférieur ou égal à x. Il ne faut pas la confondre avec un arrondi ou une troncature. On a, par exemple :

- $E(2{,}853) = \underline{\quad}$
- $E(\pi) = \underline{\quad}$
- $E(-3{,}5) = \underline{\quad}$

La définition permet aussi d'établir des équivalences telle que

$$E(x) = 3 \iff \underline{\qquad\qquad}\,.$$

Vue comme une fonction $E : \mathbb{R} \to \mathbb{Z}$, la partie entière possède le graphe suivant :



Exemple. Calcul de la partie entière de $\sqrt{10}$:

- On sait que $3^2 = 9 < 10$. En appliquant la fonction racine carrée, qui est strictement croissante, on en déduit que $3 = \sqrt{3^2} < \sqrt{10}$.
- De même, sachant que $4^2 = 16 > 10$ et en appliquant un raisonnement similaire, on trouve que $4 = \sqrt{4^2} > \sqrt{10}$.

Finalement, on a trouvé que $3 < \sqrt{10} < 4$ donc on peut en déduire que $E(\sqrt{10}) = 3$.

Démonstration. (Existence et unicité de la partie entière)

- **Existence.** Soit $x \geqslant 0$. Comme $\mathbb{R}$ est archimédien, il existe $n \in \mathbb{N}$ tel que $n > x$. Considérons l'ensemble
$$K = \{k \in \mathbb{N} \mid k \leqslant x\}.$$
Cet ensemble est fini (car il est strictement inclus dans $[\![0, n]\!]$). Notons $k_{\max}$ son plus grand élément. On peut alors en déduire que :
  — $k_{\max} \leqslant x$ puisque, par définition, $k_{\max} \in K$,
  — $k_{\max} + 1 > x$ car, comme $k_{\max} + 1$ est strictement plus grand que $k_{\max} = \max K$, il n'appartient pas à K et donc n'est pas inférieur ou égal à x.

  On peut donc poser $E(x) = k_{\max}$ car on a bien $k_{\max} \leqslant x < k_{\max} + 1$.
  Remarque : on pourrait établir une démonstration analogue dans le cas où $x < 0$.
- **Unicité.** Soient $k, \ell \in \mathbb{Z}$ deux entiers tels que
$$k \leqslant x < k + 1 \quad \text{et} \quad \ell \leqslant x < \ell + 1.$$
Montrons qu'ils sont nécessairement égaux. On peut déjà remarquer que :
  — $k \leqslant x < \ell + 1$, d'où $k < \ell + 1$,
  — $\ell \leqslant x < k + 1$ d'où $\ell < k + 1$ et donc $\ell - 1 < k$.

  On trouve donc que $\ell - 1 < k < \ell + 1$. Or, il n'y a qu'un seul entier compris strictement entre les entiers $\ell - 1$ et $\ell + 1$: c'est ℓ. On en déduit que $k = \ell$.

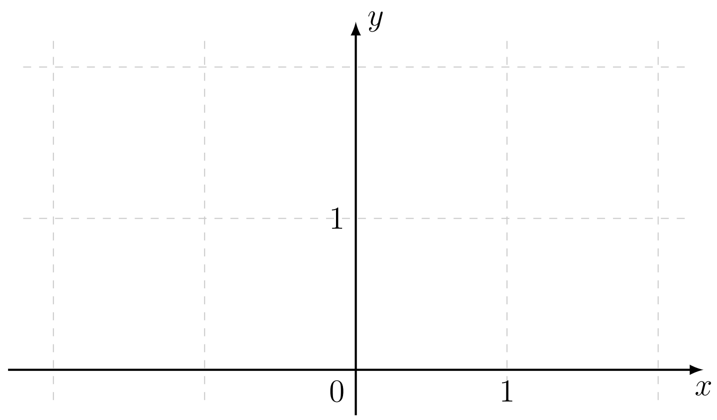
IV.1.3. Valeur absolue

Définition 1. Soit $x \in \mathbb{R}$. La **valeur absolue** de x, notée $|x|$, est le réel défini par

$$|x| = \begin{cases} \underline{\quad} & \text{si } \underline{\qquad} \\ \underline{\qquad} & \text{si } \underline{\qquad} \end{cases}$$

Remarque. Par définition même, la valeur absolue d'un réel x est toujours positive ou nulle, et ce peu importe le signe de x.

Vue comme une fonction $|\cdot| : \mathbb{R} \to \mathbb{R}_+$, la valeur absolue possède le graphe suivant :



C'est une fonction *paire* : son graphe est symétrique par rapport à ________________.

Proposition 6.

1. Pour tout $x \in \mathbb{R}$, on a :
   - $|x| \geqslant 0$,
   - $|-x| = |x|$,
   - $|x| > 0 \iff x \neq 0$.
2. Pour tout $x \in \mathbb{R}$, on a $\sqrt{x^2} = \underline{\quad}$.
3. Pour tous $x, y \in \mathbb{R}$, on a $|xy| = \underline{\qquad}$.

Proposition 7. (Inégalités triangulaires) Pour tous $x, y \in \mathbb{R}$, on a les deux inégalités suivantes :

1. l'**inégalité triangulaire** :

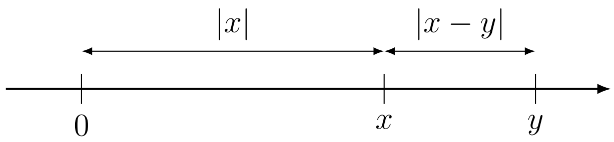
   $$\underline{\qquad\qquad\qquad\qquad}$$

   (parfois appelée *première inégalité triangulaire* pour la distinguer de la suivante),
2. la **seconde inégalité triangulaire** :

   $$\underline{\qquad\qquad\qquad\qquad}$$

Sur la droite réelle,

- $|x|$ représente la distance __________ ,
- $|x-y|$ représente la distance __________ .



Démonstration. (Inégalité triangulaire) Soient $x, y \in \mathbb{R}$. Par définition (démontrez-le), on a les deux encadrements :

$$-|x| \leqslant x \leqslant |x| \quad \text{et} \quad -|y| \leqslant y \leqslant |y|.$$

En sommant ces deux inégalités, on trouve :

$$-(|x|+|y|) \leqslant x+y \leqslant |x|+|y|.$$

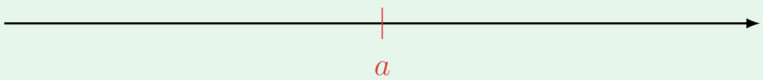
Ceci prouve (raisonnez par exemple par disjonction de cas sur le signe de $x+y$) que

$$|x+y| \leqslant |x|+|y|.$$

Remarque. Soient $x, a \in \mathbb{R}$ et $r \leqslant 0$. On utilise fréquemment la caractérisation suivante :

$$|x-a|<r \iff \underline{\hspace{4cm}} \iff \underline{\hspace{4cm}}.$$

On peut l'interpréter géométriquement sur la figure suivante :



IV.2. Intervalles et voisinages

IV.2.1. Intervalles, intervalles ouverts

Définition 2. Un **intervalle** de $\mathbb{R}$ est un sous-ensemble I de $\mathbb{R}$ tel que

____

Remarque. Un intervalle de $\mathbb{R}$ est donc à comprendre comme un ensemble « d'un seul bloc », sans « trou ».

Définition 3. Un **intervalle ouvert** est un sous-ensemble de $\mathbb{R}$ de la forme

où a et b sont des éléments de $\overline{\mathbb{R}}$.

$\overline{\mathbb{R}}$ désigne l'ensemble $\mathbb{R} \cup \{\pm\infty\}$. Concrètement cela veut simplement dire qu'on peut prendre comme valeurs de a et b n'importe quels nombres réels, mais aussi éventuellement $-\infty$ ou $+\infty$.

Remarque.

- $\varnothing$ est un intervalle ouvert (il suffit de prendre n'importe quels a et b tels que $a \geqslant b$),
- $\mathbb{R}$ est aussi un intervalle ouvert (il suffit de prendre $a = -\infty$ et $b = +\infty$),
- Un intervalle ouvert $]a, b[$ (au sens de la définition 3) est un cas particulier d'intervalle (au sens de la définition 2).
  En effet, soient $a', b' \in]a, b[$. Si $x \in \mathbb{R}$ vérifie $a' \leqslant x \leqslant b'$, alors on a $a < a' \leqslant x \leqslant b' < b$ donc $x \in]a, b[$.

IV.2.2. Voisinage d'un réel

Définition 4. Soit $a \in \mathbb{R}$ et V un sous-ensemble de $\mathbb{R}$. On dit que V est un **voisinage** de a s'il existe un intervalle ouvert I tel que $a \in I$ et $I \subset V$.

Remarque. Dit grossièrement, V est un voisinage de a si V contient (au moins) un peu d'espace « d'un seul bloc » autour de a (à gauche et à droite). L'ensemble V peut ensuite indifféremment contenir des « trous » ailleurs, et contenir des valeurs plus ou moins éloignées de a.

Exemple.

- L'ensemble $[-1, 4[\cup]5, 6[$ est un voisinage de $a = 2$.
- L'ensemble $[2, 3[$ n'est pas un voisinage de $a = 2$.
- L'ensemble $\left]2 - \frac{1}{1000}, 2 + \frac{3}{100}\right[$ est un voisinage de $a = 2$.
- L'ensemble $\mathbb{R}$ est un voisinage de $a = 2$.

IV.3. Bornes et extremums d'un sous-ensemble de $\mathbb{R}$

▷ *MAI2, module 2 — Borne supérieure*

IV.3.1. Maximum et minimum

Définition 5. Soit A une partie non-vide de $\mathbb{R}$.

- Le **plus grand élément** de A, aussi appelé **maximum** de A et noté $\max A$, est l'unique réel α tel que :

  et .

- Le **plus petit élément** de A, aussi appelé **minimum** de A et noté $\min A$, est l'unique réel α tel que :

$$\_\_\_\_\_\_ \quad \text{et} \quad \_\_\_\_\_\_\_\_\_\_ .$$

Remarque. La définition ci-dessus utilise le fait que si le maximum de A existe (attention, ce n'est pas toujours le cas !), alors il est unique.

Démonstration. *Supposons que α_1 et α_2 vérifient tous les deux la définition de maximum de A. Cela implique que :*

- *α_1 est supérieur ou égal à tous les éléments de A, donc en particulier il est supérieur ou égal à α_2,*
- *α_2 est supérieur ou égal à tous les éléments de A, donc en particulier il est supérieur ou égal à α_1.*

Ainsi les définitions impliquent à la fois $\alpha_2 \leqslant \alpha_1$ et $\alpha_1 \leqslant \alpha_2$, d'où nécessairement $\alpha_1 = \alpha_2$.

Il en va de même pour le minimum (et la démonstration est similaire).

Exemple. Soient $a, b \in \mathbb{R}$ avec $a < b$.

- $\max([a,b]) = b$ et $\min([a,b]) = a$.
- En revanche, $]a,b[$ ne possède ni minimum, ni maximum.
- $[0,1[$ a pour plus petit élément 0, mais n'a pas de plus grand élément.

Exemple. Étudions un sous ensemble plus complexe :

$$A = \left\{ 1 - \frac{1}{n} \mid n \in \mathbb{N}^* \right\}.$$

On peut voir A comme l'ensemble formé par tous les termes de la suite $(u_n)_{n \geqslant 1}$ de terme général $u_n = 1 - \frac{1}{n}$. Visuellement, on peut essayer de le représenter ainsi :

L'ensemble A est constitué d'une infinité de points distincts, mais ce n'est pas un intervalle !

- **Montrons que** $\min A = 0$**.**
  - On a $u_1 = 1 - \frac{1}{1} = 0$ d'où $0 \in A$.
  - Pour tout $n \geqslant 1$, on a $\frac{1}{n} \leqslant 1$ (par décroissance de la fonction inverse) d'où $1 - \frac{1}{n} \geqslant 1 - 1$ c'est-à-dire $u_n \geqslant 0$.

  Ainsi, 0 est bien le plus petit élément de A.
- **Montrons que** A **n'a pas de plus grand élément.**
  Supposons par l'absurde qu'il existe un plus grand élément $\alpha = \max A$. Cela signifie en particulier que
  $$\forall n \in \mathbb{N}, \quad u_n = 1 - \frac{1}{n} \leqslant \alpha.$$
  En faisant tendre n vers $+\infty$, on trouve alors $1 \leqslant \alpha$. Mais par définition, on devrait aussi avoir $\alpha \in A$, autrement dit
  $$\alpha = 1 - \frac{1}{n_0}$$

pour un certain $n_0 \in \mathbb{N}^*$. Or, on sait que $\frac{1}{n_0} > 0$, d'où

$$\alpha = 1 - \frac{1}{n_0} < 1$$

ce qui est contradictoire avec l'inégalité précédente.
C'est donc que l'hypothèse de départ était fausse, ce qui prouve que A ne possède pas de plus grand élément.

IV.3.2. Majorant et minorant

Définition 6. Soit A une partie non-vide de $\mathbb{R}$.

- Soit $M \in \mathbb{R}$. On dit que M est un **majorant** de A si

  $$\underline{\hspace{3cm}}.$$

  Si un tel majorant de A existe, on dit que la partie A est ________.
- Soit $m \in \mathbb{R}$. On dit que m est un **minorant** de A si

  $$\underline{\hspace{3cm}}.$$

  Si un tel minorant de A existe, on dit que la partie A est ________.

Remarque. Contrairement au maximum et au minimum, le minorant et le majorant n'appartiennent pas forcément à l'ensemble A.

Exemple.

- 3 est un majorant de l'ensemble $]0, 2[$.
- -7, $-\pi$ et 0 sont des minorants de $]0, +\infty[$. En revanche, $]0, +\infty[$ ne possède pas de majorant.
- Lorsqu'un ensemble admet un majorant (ou un minorant), il en admet nécessairement une infinité. Par exemple :
  - les majorants de $[0, 1[$ sont exactement les éléments de $[1, +\infty[$,
  - les minorants de $[0, 1[$ sont exactement les éléments de $]-\infty, 0]$.

IV.3.3. Borne supérieure et borne inférieure

Définition 7. Soit A une partie non-vide de $\mathbb{R}$, et soit $\alpha \in \mathbb{R}$.

- On dit que α est la **borne supérieure** de A si α est un majorant de A et si c'est le plus _____ des majorants de A. On le note _____.
- On dit que α est la **borne inférieure** de A si α est un minorant de A et si c'est le plus _____ des minorants de A. On le note _____.

Exemple.

1. Soient $a, b \in \mathbb{R}$ avec $a < b$.
   - $\sup([a, b]) = b$. Ici, la borne supérieure de $[a, b]$ coïncide avec le plus grand élément.
   - $\inf([a, b]) = a$. Ici, la borne inférieure de $[a, b]$ coïncide avec le plus petit élément.
   - $\sup(]a, b[) = b$ bien que $]a, b[$ n'admette pas de plus grand élément.
   - $\inf(]0, +\infty[) = 0$ bien que $]0, +\infty[$ n'admette pas de plus petit élément.

Ces exemples montrent notamment que la borne supérieure (ou inférieure) d'un ensemble A n'appartient pas nécessairement à cet ensemble.

2. Si une partie n'est pas majorée, alors il n'y a ni borne supérieure, ni plus grand élément. Par exemple, $]0, +\infty[$ n'admet pas de borne supérieure.

Théorème 1.

- Toute partie de $\mathbb{R}$ non-vide et majorée admet nécessairement ________________.
- Toute partie de $\mathbb{R}$ non-vide et minorée admet nécessairement ________________.

Exemple. Soit $A =]0, 1]$.

- Les majorants de A sont les éléments de $[1, +\infty[$. Le plus petit des majorants de A est donc 1, autrement dit $\sup A = 1$.
- Les majorants de A sont les éléments de $]-\infty, 0]$. Le plus grand des majorants de A est donc 0, autrement dit $\inf A = 0$.

Proposition 8. (Caractérisation de la borne supérieure) La borne supérieure de A est l'unique réel α tel que :

i. $\forall x \in A,\ x \leqslant \alpha$,

ii. $\forall y < \alpha,\ \exists x \in A,\ y < x$.

Remarque.

1. L'hypothèse i. indique que α est un majorant de A. L'hypothèse ii., plus subtile, indique qu'on peut trouver des éléments de A aussi proches que l'on veut de α.
2. Il existe de même une caractérisation de la borne inférieure d'un ensemble, que nous laissons au lecteur le soin de retrouver en ajustant convenablement les hypothèses i. et ii.

Exemple. Reprenons le cas de l'ensemble

$$A = \left\{1 - \frac{1}{n} \mid n \in \mathbb{N}^*\right\}.$$

- On avait vu que $\min A = 0$. Or, lorsqu'un ensemble admet un plus petit élément, alors c'est aussi la borne inférieure de cet ensemble. Ici, on a donc $\inf A = 0$.
- **Montrons que** $\sup A = 1$**. Première méthode possible : à l'aide de la définition.**
  On veut montrer que 1 est un majorant de A, et que c'est le plus petit.
  — On avait déjà montré que pour tout $n \in \mathbb{N}^*$, $1 - \frac{1}{n} \leqslant 1$ autrement dit 1 est un majorant de A.

— Soit M un majorant de A. Cela signifie que

$$\forall\, n \in \mathbb{N}^*, \quad M \geqslant 1 - \frac{1}{n}.$$

En faisant tendre n vers $+\infty$, on trouve $M \geqslant 1$. Autrement dit on vient de montrer que tous les majorants de A sont supérieur (ou égaux) à 1.

Ainsi, le plus petit des majorants de A est $\sup A = 1$.

- **Montrons que** $\sup A = 1$**. Seconde méthode possible : à l'aide de la caractérisation.**

  i. Soit $x \in A$. Alors x est de la forme
  $$x = 1 - \frac{1}{n}$$
  pour un certain $n \in \mathbb{N}^*$. Comme n est positif, alors $\frac{1}{n}$ aussi et donc $x \leqslant 1$.

  ii. Soit $y < 1$. Montrons qu'on peut trouver un élément $x \in A$ tel que $y < x$.
  Comme $y < 1$, on peut affirmer que $1 - y > 0$. Or, la suite $\left(\frac{1}{n}\right)_{n \geqslant 1}$ tend vers zéro, on peut donc trouver un entier $n_0 \in \mathbb{N}^*$ tel que

  $$0 < \frac{1}{n_0} < 1 - y.$$

  En posant $x = 1 - \frac{1}{n_0} \in A$, on a bien l'encadrement $y < 1 - \frac{1}{n_0} = x$.

Comme le nombre $\alpha = 1$ vérifie les deux propriété de la caractérisation ci-dessus, on peut affirmer que $\sup A = 1$.

Chapitre V.

Nombres complexes

V.1. Premières notions

▷ *MA11, module 7 — Nombres complexes*

V.1.1. Définition d'un nombre complexe et opérations usuelles

Définition 1. Un **nombre complexe** est un couple $(a, b) \in \mathbb{R}^2$, que l'on notera plutôt sous la forme

$$a + \mathrm{i}b.$$

Étant donnés deux nombres complexes $z = a + \mathrm{i}b$ et $z' = a' + \mathrm{i}b'$, on définit :

- leur somme $z + z'$ comme le nombre $(a + a') + \mathrm{i}(b + b')$,
- leur produit zz' comme le nombre $(aa' - bb') + \mathrm{i}(ab' + ba')$.

Remarque. Il n'y a pas besoin d'apprendre la formule du produit par cœur : il suffit de mener les calculs comme si i représentait un nombre tel que

$$\mathrm{i}^2 = -1$$

et respectant les relations de distributivité habituelles. En effet, en développant on trouve bien :

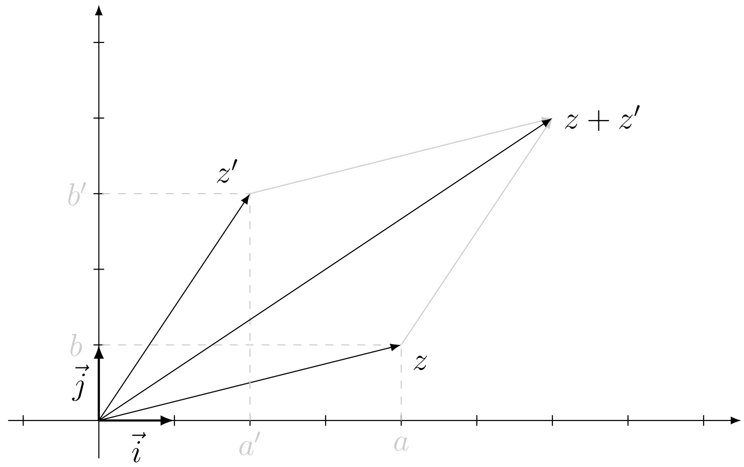
$$zz' = (a + \mathrm{i}b)(a' + \mathrm{i}b') = aa' + \mathrm{i}ab' + \mathrm{i}a'b + \mathrm{i}^2 bb' = aa' - bb' + \mathrm{i}(ab' + a'b).$$

On note $\mathbb{C}$ l'ensemble des nombres complexes.

Le couple $(a, b) \in \mathbb{R}^2$ peut donc maintenant être interprété de deux façons :

- comme un vecteur $\vec{u} = (a, b) = a\vec{i} + b\vec{j}$ dans le plan $\mathbb{R}^2$ muni d'un repère $(O, \vec{i}, \vec{j})$,
- comme un nombre complexe $z = a + \mathrm{i}b$.

En identifiant ces deux représentations, la somme de deux nombres complexes correspond exactement à la somme des vecteurs du plan qu'ils représentent.



Définition 2. Soit $z = a + ib$ un nombre complexe.

- Le nombre a s'appelle la **partie** ______ de z, notée ______.
- Le nombre b s'appelle la **partie** __________ de z, notée ______.

Remarque. Par définition, on a

$$z = z' \iff \begin{cases} \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\ \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \end{cases}$$

Remarque.

1. Un nombre réel $x \in \mathbb{R}$ peut être vu comme un nombre complexe de partie imaginaire nulle, c'est-à-dire :
$$x = x + \mathrm{i}0.$$
Ainsi on a $\mathbb{R} \subset \mathbb{C}$.
2. D'autre part, un nombre complexe de partie réelle nulle, c'est-à-dire de la forme
$$z = 0 + \mathrm{i}b$$
(avec $b \in \mathbb{R}$) est appelé un nombre **imaginaire pur**. On note parfois $\mathrm{i}\mathbb{R}$ l'ensemble des nombres imaginaires purs (et on a donc $\mathrm{i}\mathbb{R} \subset \mathbb{C}$).

Définition 3. Soit $z = a + ib$ un nombre complexe.

- L'**opposé** de z est le nombre complexe $(-a) + \mathrm{i}(-b)$, noté $-z$.
- Le produit de z par un *scalaire* $\lambda \in \mathbb{R}$ est le nombre complexe $(\lambda a) + \mathrm{i}(\lambda b)$, noté λz.

En identifiant encore le nombre complexe $z = a + ib$ et le vecteur $\vec{u} = a\vec{i} + b\vec{j}$, les nombres complexes $-z$ et λz correspondent aux vecteurs $-\vec{u}$ et $\lambda\vec{u}$ tels que vous les connaissez déjà.

V.1.2. Calcul avec les nombres complexes

Proposition 1. (Inverse d'un nombre complexe) Soit z un nombre complexe. Si $z \neq 0$, alors il existe un unique nombre complexe z' tel que

$$z \times z' = 1.$$

Dans ce cas, le nombre z' s'appelle l'**inverse** de z, on le note $\dfrac{1}{z}$ ou z^{-1}.

Si $z = a + ib$ avec $(a, b) \in \mathbb{R}^2$, alors on a la formule explicite :

$$\frac{1}{z} = \frac{a - ib}{a^2 + b^2}.$$

Démonstration. (Existence) Si $z \neq 0$, cela signifie que $a \neq 0$ ou $b \neq 0$, et donc $a^2 + b^2 > 0$. Ainsi le nombre complexe

$$z' = \frac{a - ib}{a^2 + b^2}$$

est bien défini (pas de division par zéro). Un calcul direct permet alors de vérifier que

$$zz' = (a + ib)\frac{(a - ib)}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1.$$

Définition 4. (Quotient de nombres complexes) Soit z, z' deux nombres complexes avec $z' \neq 0$.

Le **quotient** $\dfrac{z}{z'}$, est défini par :

$$\frac{z}{z'} = z \times \frac{1}{z'}.$$

Proposition 2. Soit z, z' deux nombres complexes. On a l'équivalence

$$zz' = 0 \iff (z = 0 \text{ ou } z' = 0).$$

*(On dit que l'ensemble $\mathbb{C}$ des nombres complexes est **intègre**.)*

Définition 5. (Puissance d'un nombre complexe)

Soit z' un nombre complexe.

- Pour tout $n \in \mathbb{N}^*$, on définit z^n comme le produit :

$$z^n = \underbrace{z \times z \times \cdots \times z}_{n \text{ fois}}.$$

- Par convention, on pose

$$z^0 = 1$$

- Si $z \neq 0$, alors pour tout $n \in \mathbb{N}^*$ on pose

$$z^{-n} = \frac{1}{z^n}.$$

Remarque. Notez que nous n'avons défini z^a que lorsque a est entier. Il ne faudra pas écrire z^a avec a une fraction ou un irrationnel !

Remarque. Il n'existe pas de relation d'ordre naturelle sur $\mathbb{C}$, autrement dit les symboles $\leqslant$, $\geqslant$, $<$ et $>$ ne doivent pas être utilisés avec des nombres complexes !

Proposition 3. Soit $z \in \mathbb{C}$ tel que $z \neq 1$. Pour tout $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} z^k = \underline{\qquad\qquad}.$$

Démonstration. En développant, on commence par vérifier que :

$$\left(\sum_{k=0}^{n} z^k\right)(1-z) = \left(\sum_{k=0}^{n} z^k\right) - \left(z \times \sum_{k=0}^{n} z^k\right) = \left(\sum_{k=0}^{n} z^k\right) - \left(\sum_{k=0}^{n} z^{k+1}\right)$$

Or, un changement d'indice donne l'égalité :

$$\sum_{k=0}^{n} z^{k+1} = \sum_{k=1}^{n+1} z^k.$$

On reconnaît un phénomène de télescopage qu'on fait apparaître explicitement en isolant les termes en trop :

$$\left(\sum_{k=0}^{n} z^k\right) - \left(\sum_{k=1}^{n+1} z^k\right) = \left(z^0 + \sum_{k=1}^{n} z^k\right) - \left(z^{n+1} + \sum_{k=1}^{n} z^k\right) = z^0 - z^{n+1}.$$

On vient donc de montrer que

$$\left(\sum_{k=0}^{n} z^k\right)(1-z) = z^0 - z^{n+1} = 1 - z^{n+1}$$

d'où finalement :

$$\sum_{k=0}^{n} z^k = \frac{1-z^{n+1}}{1-z}.$$

V.1.3. Conjugué et module

Définition 6. Soit $z = a + ib$ un nombre complexe. Le **conjugué** de z est le nombre complexe noté $\bar{z}$ et défini par

$$\bar{z} = \underline{\qquad\quad}.$$

Définition 7. Soit $z = a + ib$ un nombre complexe. Le **module** de z est le nombre réel positif noté $|z|$ et défini par

$$|z| = \underline{\qquad\qquad}.$$

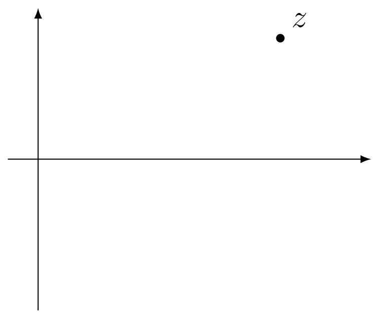
Remarque : on peut aussi écrire $|z| = \sqrt{z\bar{z}}$. *En effet, on a*

$$z\bar{z} = (a + ib)(a - ib) = \underline{\qquad}$$

(en particulier, $z\bar{z}$ *est toujours un nombre* ***réel positif****).*

En représentant les nombres complexes dans le plan :

- $\bar{z}$ est le symétrique de z par rapport à ____________________ ,
- $|z|$ est la distance entre _________________________ .



Proposition 4. Soient z, z' deux nombres complexes. Alors :

1. $\overline{z + z'} = \underline{\qquad}$
2. $\overline{zz'} = \underline{\quad}$
3. $\bar{\bar{z}} = \underline{\ }$
4. $|z + z'| \leqslant \underline{\qquad\quad}$
5. $|zz'| = \underline{\qquad}$
6. $|\bar{z}| = \underline{\quad}$
7. $z\bar{z} = \underline{\quad}$
8. $|z| = 0 \iff \underline{\qquad}$

Proposition 5. Soit z un nombre complexe. Alors :

$$z + \bar{z} = 2\,\mathrm{Re}(z) \qquad \text{et} \qquad z - \bar{z} = 2\,\mathrm{Im}(z).$$

On en déduit les caractérisations suivantes :

- $z \in \mathbb{R} \iff \mathrm{Im}(z) = 0 \iff \bar{z} = z$,
- $z \in \mathrm{i}\mathbb{R} \iff \mathrm{Re}(z) = 0 \iff \bar{z} = -z$.

Remarque. Des propositions précédentes découlent d'autres règles de calcul telles que

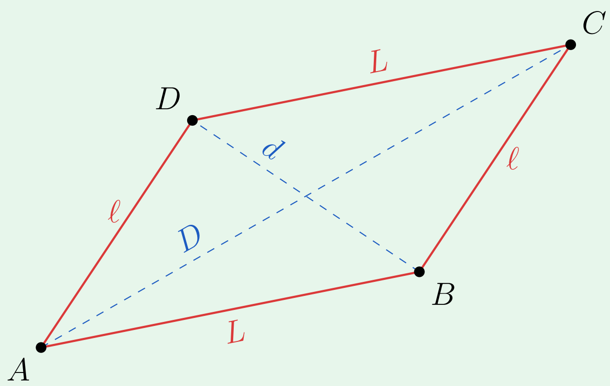
$$\overline{z - z'} = \bar{z} - \overline{z'}.$$

(En effet, $\overline{z - z'} = \overline{z + (-z')} = \overline{z + (-1) \times z'} = \bar{z} + \overline{(-1)} \times \overline{z'}$. Comme -1 est réel, on a $\overline{-1} = -1$ et donc finalement $\overline{z - z'} = \bar{z} + (-1) \times \overline{z'} = \bar{z} - \overline{z'}$.)

Mentionnons les autres propriétés de calcul remarquables suivantes :

$$\overline{\left(\frac{z}{z'}\right)} = \frac{\bar{z}}{\bar{z}'}, \qquad \overline{(z^n)} = (\bar{z})^n, \qquad \left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}, \qquad |z^n| = |z|^n.$$

Exemple. (Application des nombres complexes à la géométrie) Montrons que dans un parallélogramme, la somme des carrés des diagonales est égale à la somme des carrés des côtés.



$$D^2 + d^2 = 2\ell^2 + 2L^2$$

Sans perte de généralité, on peut supposer que le point A se trouve à l'origine du repère. On note z et z' les nombres complexes correspondant aux positions de B et D respectivement. Comme $ABCD$ est un parallélogramme, la position de C correspond au nombre complexe $z + z'$.

Ainsi, on a :

- $L = AB = CD = |z|$,
- $\ell = AD = BC = |z'|$,
- $D = AC = |z + z'|$.

De plus, on a $d = BD = |z - z'|$ (placer le point $z - z'$ sur la figure pour s'en convaincre).

Il n'y a plus qu'à utiliser les propriétés de calcul dans $\mathbb{C}$:

$$\begin{aligned}
D^2 + d^2 &= |z + z'|^2 + |z - z'|^2 \\
&= (z + z')\overline{(z + z')} + (z - z')\overline{(z - z')} \\
&= (z + z')(\bar{z} + \bar{z}') + (z - z')(\bar{z} - \bar{z}') \\
&= z\bar{z} + z\bar{z}' + z'\bar{z} + z'\bar{z}' + z\bar{z} - z\bar{z}' - z'\bar{z} + z'\bar{z}' \\
&= 2z\bar{z} + 2z'\bar{z}' \\
&= 2|z|^2 + 2|z'| \\
&= 2L^2 + 2\ell^2
\end{aligned}$$

V.2. Équations polynomiales dans $\mathbb{C}$

▷ *MA11, module 8 — Racines carrées, équations du second degré*

V.2.1. Racine carrée d'un nombre complexe

Définition 8. Soit z un nombre complexe. Une racine carrée de z est un nombre complexe $\omega \in \mathbb{C}$ tel que

$$\underline{\qquad\qquad}.$$

Exemple.

- Les racines carrées d'un réel positif x sont ___ et ___.
- Les racines carrées de ___ sont i et $-$i.
- Les racines carrées de i sont

$$\underline{\qquad\qquad} \quad \text{et} \quad \underline{\qquad\qquad}.$$

Remarque. On verra qu'un nombre complexe z admet toujours deux racines carrées opposées ω et $-\omega$ (éventuellement confondues dans le cas où $z = 0$).

En effet, si $\omega^2 = z$, *alors nécessairement* $(-\omega)^2 = (-1)^2 \times \omega^2 = 1 \times z = z$.

Remarque. Attention : on rappelle que lorsque x est un réel positif, $\sqrt{x}$ est seulement une *notation* pour désigner l'unique racine carrée **positive** de x, mais le réel x admet bien **deux** racines carrées. Par exemple, 9 possède deux racines carrées, 3 et -3. Lorsqu'on note $\sqrt{9}$, c'est pour désigner celle qui est positive, c'est-à-dire 3.

Pour un nombre complexe z quelconque, les notions de « positif » et « négatif » n'ont plus de sens. On évitera donc à tout prix la notation $\sqrt{z}$ (autant que $z^{\frac{1}{2}}$) car il est impossible de savoir à laquelle des deux racines carrées de z elle fait référence !

Méthode. (Calcul des racines carrées d'un nombre complexe)
Soit $z = a + ib$ un nombre complexe. Cherchons une racine carrée de z sous la forme d'un nombre complexe $\omega = x + \mathrm{i}y$. On veut donc résoudre l'équation

$$(E) : \quad \omega^2 = z.$$

0. **Point de départ.** On utilisera toujours l'astuce suivante :

$$(E) \iff \begin{cases} \omega^2 = z \\ |\omega|^2 = |z| \end{cases}$$

La seconde ligne du système ainsi formé n'est qu'une conséquence immédiate de la première, mais il est primordial de la faire apparaître explicitement car elle permet de simplifier énormément les calculs qui suivent.

1. **On développe sous forme algébrique.**

$$(E) \iff \begin{cases} (x + \mathrm{i}y)^2 = a + \mathrm{i}b \\ |x + \mathrm{i}y|^2 = |a + \mathrm{i}b| \end{cases} \iff \begin{cases} (x^2 - y^2) + 2\mathrm{i}xy = a + \mathrm{i}b \\ x^2 + y^2 = \sqrt{a^2 + b^2} \end{cases}$$

2. **On identifie les parties réelles et imaginaires.**

$$(E) \iff \begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases}$$

3. **On utilise des opérations de somme et différence.**
On remplace les lignes L_3 et L_1 par leur somme $L_3 + L_1$ et leur différence $L_3 - L_1$.

$$(E) \iff \begin{cases} 2x^2 = \sqrt{a^2+b^2} + a & {\scriptstyle (L_3+L_1)} \\ 2xy = b \\ 2y^2 = \sqrt{a^2+b^2} - a & {\scriptstyle (L_3-L_1)} \end{cases}$$

Cette opération a l'avantage d'isoler les inconnues x^2 et y^2.

4. **On isole les valeurs possibles de x et y** (sans oublier les solutions négatives !).
À partir de là les formules semblent se compliquer car on travaille ici avec des expressions littérales, mais en pratique vous aurez souvent des valeurs numériques donnant des systèmes plus simple que ci-dessous.

$$(E) \iff \begin{cases} x = \pm\sqrt{\frac{1}{2}(\sqrt{a^2+b^2} + a)} \\ 2xy = b \\ y = \pm\sqrt{\frac{1}{2}(\sqrt{a^2+b^2} - a)} \end{cases}$$

5. **On utilise le signe de b pour connaître les deux solutions à garder.**
Si on ne regarde que les lignes 1 et 3, on a *a priori* quatre solutions possibles :

$$\begin{aligned}
(x,y) &= \left(\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)},\ \sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)} \right), \\
(x,y) &= \left(\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)},\ -\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)} \right), \\
(x,y) &= \left(-\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)},\ \sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)} \right), \\
(x,y) &= \left(-\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)},\ -\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)} \right).
\end{aligned}$$

Toutefois la ligne 2 impose une condition supplémentaire permettant de ne retenir que deux de ces solutions. En effet :
   - si $b \geqslant 0$, alors x et y doivent être de même signe pour que le produit xy soit positif,
   - si $b < 0$, alors x et y doivent être de signes opposés pour que le produit xy soit négatif.

Attention : il ne faut surtout pas apprendre par cœur les expressions littérales faisant intervenir a et b, mais seulement savoir appliquer cette méthode dans des cas concrets (les expressions obtenues seront alors en général beaucoup plus simples, comme le montre l'exemple suivant).

Exemple. (Calcul des racines carrées de i) Soit $\omega = x + \mathrm{i}y$ avec $(x, y) \in \mathbb{R}^2$.

$$\omega^2 = \mathrm{i} \iff \begin{cases} (x+\mathrm{i}y)^2 = \mathrm{i} \\ |x+\mathrm{i}y|^2 = |\mathrm{i}|^2 \end{cases} \iff \begin{cases} (x^2-y^2) + 2\mathrm{i}xy = \mathrm{i} \\ x^2+y^2 = 1 \end{cases}$$

$$\iff \begin{cases} x^2 - y^2 = 0 \\ 2xy = 1 \\ x^2 + y^2 = 1 \end{cases} \iff \begin{cases} 2x^2 = 1 \\ 2xy = 1 \\ 2y^2 = 1 \end{cases}$$

$$\iff \begin{cases} x = \pm\frac{1}{\sqrt{2}} \\ 2xy = 1 \\ y = \pm\frac{1}{\sqrt{2}} \end{cases} \iff \begin{cases} x = \frac{1}{\sqrt{2}} \\ y = \frac{1}{\sqrt{2}} \end{cases} \text{ ou } \begin{cases} x = -\frac{1}{\sqrt{2}} \\ y = -\frac{1}{\sqrt{2}} \end{cases}$$

$$\iff \omega = \frac{1}{\sqrt{2}} + \mathrm{i}\frac{1}{\sqrt{2}} \quad \text{ou} \quad \omega = -\frac{1}{\sqrt{2}} - \mathrm{i}\frac{1}{\sqrt{2}}$$

Les racines carrées de i sont donc $\frac{1}{\sqrt{2}} + \mathrm{i}\frac{1}{\sqrt{2}}$ et $-\left(\frac{1}{\sqrt{2}} + \mathrm{i}\frac{1}{\sqrt{2}}\right)$.

V.2.2. Application aux équations du second degré

Proposition 6. Soit $(a, b, c) \in \mathbb{C}^3$ avec $a \neq 0$. L'équation

$$az^2 + bz + c = 0$$

admet pour solution les nombres

$$\frac{-b+\delta}{2a} \quad \text{et} \quad \frac{-b-\delta}{2a}$$

où δ une racine carrée du *discriminant* $b^2 - 4ac$.

Exemple. Considérons l'équation

$$z^2 + z + \frac{1-\mathrm{i}}{4} = 0.$$

Notons Δ son discriminant. Par définition :

$$\Delta = 1 - 4 \times \frac{1-\mathrm{i}}{4} = \mathrm{i}.$$

Or, les racines carrées de i sont (voir exemple précédent) :

$$\delta_1 = \frac{\sqrt{2}}{2}(1+\mathrm{i}) \qquad \text{et} \qquad \delta_2 = -\frac{\sqrt{2}}{2}(1+\mathrm{i}).$$

On prend n'importe laquelle des deux, par exemple δ_1, et on trouve pour solutions :

$$\frac{-1+\frac{\sqrt{2}}{2}(1+\mathrm{i})}{2} \qquad \text{et} \qquad \frac{-1-\frac{\sqrt{2}}{2}(1+\mathrm{i})}{2}.$$

Si on avait choisi δ_2, on aurait trouvé exactement les mêmes solutions (dans un ordre différent). **Le choix de la racine carrée de Δ n'a pas d'importance.**

Remarque. Dans le cas où le discriminant vaut 0, alors on ne peut prendre comme racine carrée que $\delta = 0$, et on trouve en fait une unique solution (dit *solution double*) égale à :

$$\frac{-b}{2a}.$$

Démonstration. Notons $P(z) = az^2 + bz + c$ le premier membre de l'équation. On a

$$P(z) = a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right).$$

Mettons ensuite sous forme canonique le second facteur :

$$z^2 + \frac{b}{a}z + \frac{c}{a} = \left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = \left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}.$$

En posant $\Delta = b^2 - 4ac$, puis en notant δ une racine carrée de Δ, on peut encore écrire :

$$z^2 + \frac{b}{a}z + \frac{c}{a} = \left(z + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2} = \left(z + \frac{b}{2a}\right)^2 - \frac{\delta^2}{4a^2}.$$

On reconnaît alors l'identité remarquable

$$\left(z + \frac{b}{2a}\right)^2 - \frac{\delta^2}{4a^2} = \left(z + \frac{b}{2a}\right)^2 - \left(\frac{\delta}{2a}\right)^2 = \left(z + \frac{b}{2a} - \frac{\delta}{2a}\right)\left(z + \frac{b}{2a} + \frac{\delta}{2a}\right).$$

En posant

$$z_1 = \frac{-b+\delta}{2a} \quad \text{et} \quad z_2 = \frac{-b-\delta}{2a},$$

on peut finalement écrire

$$P(z) = a(z - z_1)(z - z_2).$$

Or un produit de nombres complexes étant nul si et seulement si l'un de ses facteurs et nul, et comme $a \neq 0$, on a finalement :

$$P(z) = 0 \iff z - z_1 = 0 \text{ ou } z - z_2 = 0 \iff z = z_1 \text{ ou } z = z_2.$$

V.2.3. Équations de degré supérieur

Théorème 1. (Théorème de d'Alembert–Gauss) Soit

$$P(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_2 z^2 + a_1 z + a_0$$

un polynôme à coefficients complexes, de degré n (c'est-à-dire $a_n \neq 0$).

Alors l'équation $P(z) = 0$ admet n solutions $z_1, z_2, \ldots, z_n$ dans $\mathbb{C}$.

Remarque. Certaines solutions peuvent parfois coïncider, comme dans le cas où $\Delta = 0$ lorsque P est de degré 2. Le théorème de d'Alembert–Gauss sera un peu précisé de sorte à tenir compte de cette particularité lorsque nous aborderons le chapitre sur les polynômes.

V.3. Argument et trigonométrie

▷ *MA11, module 9 — Argument et trigonométrie*

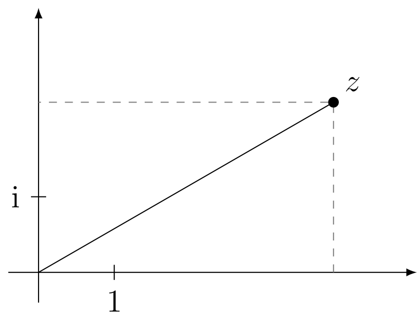
V.3.1. Argument d'un nombre complexe

Définition 9. Soit $z \in \mathbb{C}^*$. Un **argument** de z est un nombre réel θ tel que

$$\underline{\hspace{5cm}}\,.$$

On le note $\theta = \underline{\hspace{1.5cm}}$.

On peut se convaincre de l'existence de l'argument en analysant la figure suivante.



Remarque. Il n'y a pas unicité de l'argument d'un nombre complexe $z \in \mathbb{C}^*$. En effet, si θ est un argument de z, alors $\theta + 2\pi$, $\theta + 4\pi$ et, plus généralement, tous les nombres de la forme $\theta + 2k\pi$ avec $k \in \mathbb{Z}$ sont également des arguments de z.

Réciproquement, si θ et θ' sont deux arguments d'un même nombre complexe z, alors on peut affirmer qu'il existe un entier $k \in \mathbb{Z}$ tel que $\theta' = \theta + 2k\pi$. On dit que θ et θ' sont égaux modulo 2π, et on note $\theta' = \theta \pmod{2\pi}$.

On peut obtenir l'unicité en imposant éventuellement $\theta \in \,]-\pi; \pi]$.

Proposition 7. Soient z, z' deux complexes non-nuls, et $n \in \mathbb{N}$.

1. $\arg(z \times z') = \underline{\hspace{3.5cm}} \pmod{2\pi}$,
2. $\arg(z^n) = \underline{\hspace{2cm}} \pmod{2\pi}$,
3. $\arg(1/z) = \underline{\hspace{2cm}} \pmod{2\pi}$.
4. $\arg(\bar{z}) = \underline{\hspace{2cm}} \pmod{2\pi}$.

Démonstration.

1. Notons $\theta = \arg(z)$ et $\theta' = \arg(z')$. On a alors :

$$\begin{aligned} z \times z' &= |z|(\cos\theta + \mathrm{i}\sin\theta) \times |z'|(\cos\theta' + \mathrm{i}\sin\theta') \\ &= \underline{\hspace{12cm}} \\ &= \underline{\hspace{6cm}} \end{aligned}$$

(on utilise notamment les *formules d'addition* du cosinus et du sinus). Par définition, la dernière expression révèle que $\theta + \theta'$ est un argument de $z \times z'$.

2. La démonstration se ferait pas récurrence sur n, en utilisant la propriété précédente.
3. Si dans la première formule on pose $z' = 1/z$, alors on obtient $\arg(1) = \arg(z) + \arg(1/z) \pmod{2\pi}$. Or, $\arg(1) =$ __, donc $\arg(1/z) = -\arg(z) \pmod{2\pi}$.
4. On peut le montrer de deux manières :
   a) (Comme pour 1) Si $z = |z|(\cos\theta + \mathrm{i}\sin\theta)$, alors
   $$\bar{z} = \overline{|z|(\cos\theta + \mathrm{i}\sin\theta)} = |z|(\cos\theta - \mathrm{i}\sin\theta)$$
   car $|z|$, $\cos\theta$ et $\sin\theta$ sont des réels. En utilisant la parité de $\cos$ et l'imparité de $\sin$, on trouve bien
   $$\bar{z} = |z|(\cos(-\theta) + \mathrm{i}\sin(-\theta))$$
   ainsi $-\theta$ est un argument de $\bar{z}$.

   b) (Comme pour 3) En posant $z' = \bar{z}$, on obtient $\arg(z\bar{z}) = \arg(z) + \arg(\bar{z}) \pmod{2\pi}$. Or, $z\bar{z} = |z|^2$ est un nombre réel strictement positif, donc son argument vaut 0 modulo 2π. On retrouve donc $\arg(\bar{z}) = -\arg(z) \pmod{2\pi}$.

Proposition 8. (Formule de Moivre) Pour tout $(\theta, n) \in \mathbb{R} \times \mathbb{N}$,

$$\underline{\hspace{6cm}}\,.$$

Démonstration. On démontre la formule par récurrence sur n.

- **Initialisation.** Pour $n = 0$, on a, pour tout $\theta \in \mathbb{R}$, d'une part
  $$(\cos\theta + \mathrm{i}\sin\theta)^n = (\cos\theta + \mathrm{i}\sin\theta)^0 = 1$$
  et d'autre part
  $$\cos(n\theta) + \mathrm{i}\sin(n\theta) = \cos(0) + \mathrm{i}\sin(0) = 1.$$
  Donc la formule est vraie pour $n = 0$.
- **Hérédité.** Supposons la propriété vraie à un rang $n \in \mathbb{N}$ fixé. Pour tout $\theta \in \mathbb{R}$, on a alors
  $$\begin{aligned} (\cos\theta + \mathrm{i}\sin\theta)^{n+1} &= (\cos\theta + \mathrm{i}\sin\theta)^n \times (\cos\theta + \mathrm{i}\sin\theta) \\ &= (\cos(n\theta) + \mathrm{i}\sin(n\theta))(\cos\theta + \mathrm{i}\sin\theta) \\ &= (\cos(n\theta)\cos(\theta) - \sin(n\theta)\sin\theta) + \mathrm{i}(\cos(n\theta)\sin(\theta) + \sin(n\theta)\cos\theta) \\ &= \cos(n\theta + \theta) + \mathrm{i}\sin(n\theta + \theta) \\ &= \cos((n+1)\theta) + \mathrm{i}\sin((n+1)\sin\theta) \end{aligned}$$
  Ainsi, la formule est vraie au rang $n+1$.

V.3.2. Forme exponentielle

Définition 10. Pour tout $\theta \in \mathbb{R}$, on introduit la notation $e^{i\theta}$ en posant :

$$e^{i\theta} = \_\_\_\_\_\_\_\_\_\_ .$$

Ainsi, tout nombre complexe non-nul s'écrit sous **forme exponentielle**

$$z = \_\_\_$$

avec $\rho = |z|$ le ______ de z et $\theta = \arg(z)$ un _______ de z.

Remarque. On distinguera donc la *forme exponentielle* d'un nombre complexe z de sa *forme algébrique* (ou *cartésienne*) $z = a + ib$ avec $(a, b) \in \mathbb{R}^2$.

Proposition 9. Le choix de la notation exponentielle est justifié par les propositions suivantes.
Si $z = \rho e^{i\theta}$ et $z' = \rho' e^{i\theta'}$ sont deux nombres complexes, alors :

1. $zz' = \left(\rho e^{i\theta}\right)\left(\rho' e^{i\theta'}\right) = \_\_\_\_\_\_\_\_$,
2. $z^n = \left(\rho e^{i\theta}\right)^n = \_\_\_\_\_$,
3. $1/z = \left(\rho e^{i\theta}\right)^{-1} = \_\_\_\_$,
4. $\bar{z} = \overline{\left(\rho e^{i\theta}\right)} = \_\_\_\_$.

Démonstration. Ces propriétés découlent des propriétés de l'argument et de la formule de Moivre.

Proposition 10. («Unicité» de la forme exponentielle) Soient $(\rho, \rho', \theta, \theta') \in (\mathbb{R}_+^*)^2 \times \mathbb{R}^2$.

$$\rho e^{i\theta} = \rho' e^{i\theta'} \iff \begin{cases} \_\_\_\_\_ \\ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \end{cases}$$

V.3.3. Racines n-ièmes d'un nombre complexe

Définition 11. Soient $n \in \mathbb{N}$ et $z \in \mathbb{C}$. Une **racine n-ième** de z est un nombre $\omega \in \mathbb{C}$ tel que

$$\_\_\_\_\_\_ .$$

Remarque. Pour $n = 2$, on retrouve la notion de racine carrée étudiée dans la section V.2.1.

Proposition 11. Soit $z = \rho e^{i\theta}$ un nombre complexe non-nul (avec $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$). Les racines n-ièmes de z sont exactement les n nombres complexes $\omega_0, \omega_1, \ldots, \omega_{n-1}$ définis par :

$$\forall\, k \in \{0, 1, \ldots, n-1\}, \quad \omega_k = \_\_\_\_\_\_\_\_ .$$

Démonstration. Cherchons ω sous forme exponentielle $\omega = re^{\mathrm{i}t}$ (avec $r > 0$ et $t \in \mathbb{R}$).

$$\begin{aligned}
z = \omega^n \quad &\iff \quad \rho e^{\mathrm{i}\theta} = \left(re^{\mathrm{i}t}\right)^n \\
&\iff \quad \rho e^{\mathrm{i}\theta} = r^n e^{\mathrm{i}nt} \\
&\iff \quad \begin{cases} r^n = \rho \\ nt = \theta \pmod{2\pi} \end{cases} \\
&\iff \quad \begin{cases} r = \rho^{1/n} \\ nt = \theta + 2k\pi, \quad \text{avec } k \in \mathbb{Z}, \end{cases} \\
&\iff \quad \begin{cases} r = \rho^{1/n} \\ t = \frac{\theta+2k\pi}{n}, \quad \text{avec } k \in \mathbb{Z}, \end{cases}
\end{aligned}$$

On retrouve bien des solutions de la forme

$$\omega_k = \rho^{1/n} e^{\mathrm{i}\frac{\theta+2k\pi}{n}}, \qquad k \in \mathbb{Z}.$$

Or, pour tout $k \in \mathbb{R}$, on a

$$\omega_{k+n} = \rho^{1/n} e^{\mathrm{i}\frac{\theta+2(k+n)\pi}{n}} = \rho^{1/n} e^{\mathrm{i}\left(\frac{\theta+2k\pi}{n}+2\pi\right)} = \rho^{1/n} e^{\mathrm{i}\frac{\theta+2k\pi}{n}} = \omega_k$$

(c'est-à-dire $\omega_n = \omega_0, \omega_{n+1} = \omega_1, \ldots$). Il suffit donc de prendre n valeurs successives pour k pour obtenir toutes les solutions, par exemple $k \in \{0, 1, \ldots, n-1\}$ (mais on aurait pu prendre aussi $k \in \{1, 2, \ldots, n\}$).

Exemple. (Calcul des racines cubiques de 1 et -1)

- Déterminons les racines 3-ièmes (aussi appelées *racines cubiques*) de $z = 1$. Comme z a pour forme exponentielle $z = e^{\mathrm{i}0}$, ses racines cubiques sont

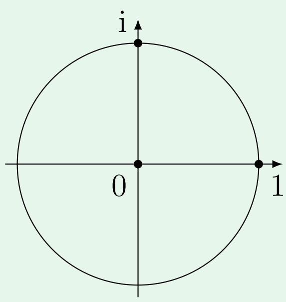
$$\omega_0 = 1^{1/n} e^{\mathrm{i}\frac{0+0\times 2\pi}{3}} = 1, \qquad \omega_1 = 1^{1/n} e^{\mathrm{i}\frac{0+1\times 2\pi}{3}} = \underline{\qquad}, \quad \text{et} \quad \omega_2 = 1^{1/n} e^{\mathrm{i}\frac{0+2\times 2\pi}{3}} = \underline{\qquad}.$$

  Dans le plan complexe, ces trois racines cubiques forment un triangle équilatéral.

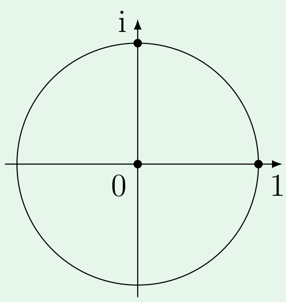
- Pour $z = -1 = e^{\mathrm{i}\pi}$, on trouve les racines cubiques

$$\omega_0 = 1^{1/n} e^{\mathrm{i}\frac{\pi+0\times 2\pi}{3}} = \underline{\qquad}, \qquad \omega_1 = 1^{1/n} e^{\mathrm{i}\frac{\pi+1\times 2\pi}{3}} = \underline{\quad}, \quad \text{et} \quad \omega_2 = 1^{1/n} e^{\mathrm{i}\frac{\pi+2\times 2\pi}{3}} = \underline{\qquad}.$$

  Encore une fois, ces trois racines cubiques forment un triangle équilatéral.

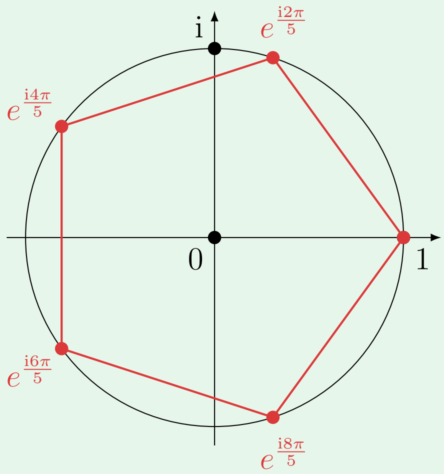


Racines cubiques de 1



Racines cubiques de -1

Exemple. (Racines cinquième de l'unité) Les racines 5-ième de $z = 1$ sont



Dans le plan complexe, ces 5 racines cinquièmes forment un ____________.

V.3.4. Application à la trigonométrie

Formules d'Euler

On a défini l'exponentielle complexe par la formule

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

qui, lorsqu'on l'applique à $-\theta$, donne

$$e^{-i\theta} = \_\_\_\_\_\_\_\_ .$$

En sommant ou soustrayant ces deux égalités, on obtient la proposition suivante.

Proposition 12. (Formules d'Euler) Pour tout $\theta \in \mathbb{R}$,

$$\cos\theta = \_\_\_\_\_\_ \quad \text{et} \quad \sin\theta = \_\_\_\_\_\_ .$$

Développement d'une expression trigonométrique

Le **développement** d'une expression de la forme $\cos(n\theta)$ ou $\sin(n\theta)$ consiste en la réécriture cette expression en fonction de puissances de $\cos(\theta)$ et $\sin(\theta)$. On peut procéder à l'aide de la formule de Moivre et la formule du binôme de Newton.

Exemple. (Développement de $\cos(3\theta)$ ou de $\sin(3\theta)$) En utilisant la formule de MOIVRE, puis en développant à l'aide du binôme de NEWTON :

$$\begin{aligned} \cos(3\theta) + \mathrm{i}\sin(3\theta) &= (\cos\theta + \mathrm{i}\sin\theta)^3 \\ &= \underline{\hspace{6cm}} \\ &= (\underline{\hspace{3cm}}) + \mathrm{i}(\underline{\hspace{3cm}}) \end{aligned}$$

Par identification des parties réelles et imaginaires, on trouve les *développements* suivants :

$$\cos(3\theta) = \underline{\hspace{3cm}} \qquad \text{et} \qquad \sin(3\theta) = \underline{\hspace{3cm}}.$$

Linéarisation d'une expression trigonométrique

À l'inverse, la **linéarisation** d'une expression trigonométrique de la forme $\cos^n(\theta)$ ou $\sin^n(\theta)$ (ou même, plus généralement, $\cos^n(\theta)\sin^m(\theta)$) consiste en la réécriture de cette expression comme combinaison linéaire de termes de la forme $\cos(k\theta)$ ou $\sin(k\theta)$ avec $k \in \{0, 1, \ldots, n\}$.

Exemple. (Linéarisation de $\sin^3\theta$)

1. On commence par exprimer $\sin\theta$ en fonction de $e^{\mathrm{i}\theta}$ et $e^{-\mathrm{i}\theta}$ à l'aide des formules d'EULER.

$$\sin^3\theta = \left(\frac{e^{\mathrm{i}\theta} - e^{-\mathrm{i}\theta}}{2\mathrm{i}}\right)^3.$$

2. On développe complètement l'expression obtenue à l'aide de la formule du binôme de NEWTON :

$$\begin{aligned} \sin^3\theta &= \frac{\left(e^{\mathrm{i}\theta}\right)^3 - 3\left(e^{\mathrm{i}\theta}\right)^2 e^{-\mathrm{i}\theta} + 3e^{\mathrm{i}\theta}\left(e^{-\mathrm{i}\theta}\right)^2 - \left(e^{-\mathrm{i}\theta}\right)^3}{(2\mathrm{i})^3} \\ &= -\frac{1}{8\mathrm{i}}\left(\underline{\hspace{5cm}}\right) \end{aligned}$$

3. On regroupe les termes conjugués deux à deux, de sorte à refaire apparaître des termes de la forme $\cos(k\theta)$ ou $\sin(k\theta)$ à l'aide des formules d'EULER :

$$\begin{aligned} \sin^3\theta &= -\frac{1}{8\mathrm{i}}\left((e^{3\mathrm{i}\theta} - e^{-3\mathrm{i}\theta}) - 3(e^{\mathrm{i}\theta} - e^{-\mathrm{i}\theta})\right) \\ &= -\frac{1}{4}\left(\frac{e^{3\mathrm{i}\theta} - e^{-3\mathrm{i}\theta}}{2\mathrm{i}} - 3\frac{e^{\mathrm{i}\theta} - e^{-\mathrm{i}\theta}}{2\mathrm{i}}\right) \\ &= -\frac{1}{4}\left(\sin(3\theta) - 3\sin(\theta)\right) \end{aligned}$$

On trouve donc comme forme linéarisée de $\sin(3\theta)$:

$$\sin(3\theta) = -\frac{1}{4}\sin(3\theta) + \frac{3}{4}\sin(\theta).$$

V.4. Nombres complexes et géométrie du plan

▷ *MA11, module 10 — Géométrie et nombres complexes*

V.4.1. Équations complexes

Définition 12. Soit M un point de coordonnées (x, y) dans le plan $\mathbb{R}^2$. On appelle **affixe** de M le nombre complexe

$$z = \underline{\qquad}.$$

Exemple.

- L'origine O du repère a pour affixe 0.
- Le point de coordonnées ____ a pour affixe 1.
- Le point de coordonnées $(0, 1)$ a pour affixe __
- Le point de coordonnées $(\rho\cos\theta, \rho\sin\theta)$ a pour affixe ____.

Proposition 13. Soit $\mathscr{D}$ la droite du plan d'équation cartésienne

$$ax + by = c$$

avec $(a, b, c) \in \mathbb{R}^3$. Alors $\mathcal{D}$ a pour équation complexe

$$\underline{\qquad\qquad\qquad}$$

avec $\omega = a + ib \in \mathbb{C}^*$ et $k = 2c \in \mathbb{R}$.

Démonstration. Posons $z = x + iy$ avec $(x, y) \in \mathbb{C}$. On a alors

$$x = \frac{z + \bar{z}}{2} \qquad \text{et} \qquad y = \frac{z - \bar{z}}{2\mathrm{i}}.$$

Ainsi,

$$\begin{aligned} ax + by = c \quad &\iff \quad a\frac{z + \bar{z}}{2} + b\frac{z - \bar{z}}{2\mathrm{i}} = c \\ &\iff \quad a(z + \bar{z}) - b\mathrm{i}(z - \bar{z}) = 2c \\ &\iff \quad az + a\bar{z} - b\mathrm{i}z + b\mathrm{i}\bar{z} = 2c \\ &\iff \quad (a - b\mathrm{i})z + (a + b\mathrm{i})\bar{z} = 2c. \end{aligned}$$

En posant $\omega = a + ib$ et $k = 2c$, la dernière équation s'écrit bien

$$\bar{\omega}z + \omega\bar{z} = k.$$

Proposition 14. Soit $\mathscr{C}$ le cercle de centre Ω et de rayon $r > 0$. Si on note ω l'affixe du point Ω, alors $\mathscr{C}$ a pour équation complexe :

$$\underline{\qquad\qquad\qquad\qquad}$$

Démonstration. Soit M un point du plan et z son affixe. Alors :

$$\begin{aligned} M \text{ appartient à } \mathscr{C} &\iff \operatorname{dist}(\Omega, M) = r \\ &\iff |z-\omega| = r \\ &\iff |z-\omega|^2 = r^2 \\ &\iff (z-\omega)\overline{(z-\omega)} = r^2 \\ &\iff (z-\omega)(\bar{z}-\bar{\omega}) = r^2 \\ &\iff z\bar{z} - \bar{\omega}z - \omega\bar{z} = r^2 - |\omega|^2 \end{aligned}$$

V.4.2. Recherche de lieux géométriques

Proposition 15. Soient A et B deux points distincts du plans, et $k \in \mathbb{R}_+$. L'ensemble des points M du plans tels que

$$\frac{MA}{MB} = k$$

est :

- la médiatrice de $[AB]$ si $k = 1$,
- un cercle si $k \neq 1$.

Démonstration. En notant a, b et z les affixes respectives de A, B et M, on a :

$$(E) : \quad \frac{MA}{MB} = k \iff \frac{|z-a|}{|z-b|} = k \iff |z-a| = k|z-b|.$$

Comme toutes les quantités en jeu sont positives, on peut élever au carrée dans chaque terme et on a

$$(E) \iff |z-a|^2 = k^2|z-b|^2 \iff (z-a)\overline{(z-a)} = k^2(z-b)\overline{(z-b)}.$$

En développant les calculs, on peut finalement montrer que l'équation (E) est équivalente à

$$(1-k^2)z\bar{z} - z(\bar{a} - k^2\bar{b}) - \bar{z}(a - k^2 b) + |a|^2 - k^2|b|^2 = 0.$$

On distingue alors deux cas :

1. Si $k = 1$, alors en posant $\omega = a - b$ on a $\bar{\omega} = \bar{a} - \bar{b}$ et donc
$$(E) \iff -z\bar{\omega} - \bar{z}\omega + |a|^2 - |b|^2 = 0 \iff z\bar{\omega} + \bar{z}\omega = |a|^2 - |b|^2.$$
On reconnaît une équation complexe de droite. De plus, cette droite n'est rien d'autre que la médiatrice de $[AB]$ puisque nous sommes alors en train d'étudier l'ensemble des points M tels que
$$\frac{MA}{MB} = 1,$$
autrement dit tels que $MA = MB$.
2. Si $k \neq 1$, alors en posant $\omega = \dfrac{a - k^2 b}{1-k^2}$ on a $\bar{\omega} = \dfrac{\bar{a} - k^2\bar{b}}{1-k^2}$ d'où :
$$(E) \iff z\bar{z} - z\bar{\omega} - \bar{z}\omega = \frac{k^2|b|^2 - |a|^2}{1-k^2}.$$
On reconnaît l'équation d'un cercle dont le centre a pour affixe ω, et dont le rayon est le réel $r > 0$ tel que
$$r^2 - |\omega|^2 = \frac{k^2|b|^2 - |a|^2}{1-k^2}$$
(on ne cherchera pas à donner son expression exacte ici).

Remarque. La démonstration ci-dessus n'est pas à connaître, mais il faut savoir mener les mêmes calculs dans le cas (beaucoup plus simple) ou a, b et c ont des valeurs explicites (voir exemple suivant).

Exemple. Prenons $A(1,0)$, $B(-1,0)$ et $k=3$. Dans ce cas, pour tout point M d'affixe z on a :

$$\frac{MA}{MB}=3 \iff |z-1|=3|z+1| \iff |z-1|^2=9|z+1|^2 \iff (z-1)\overline{(z-1)}=9(z+1)\overline{(z+1)}.$$

En développant les calculs, on trouve :

$$\frac{MA}{MB}=3 \iff z\bar{z}-\bar{z}-z+1=9(z\bar{z}+\bar{z}+z+1) \iff 4z\bar{z}+5z+5\bar{z}+4=0.$$

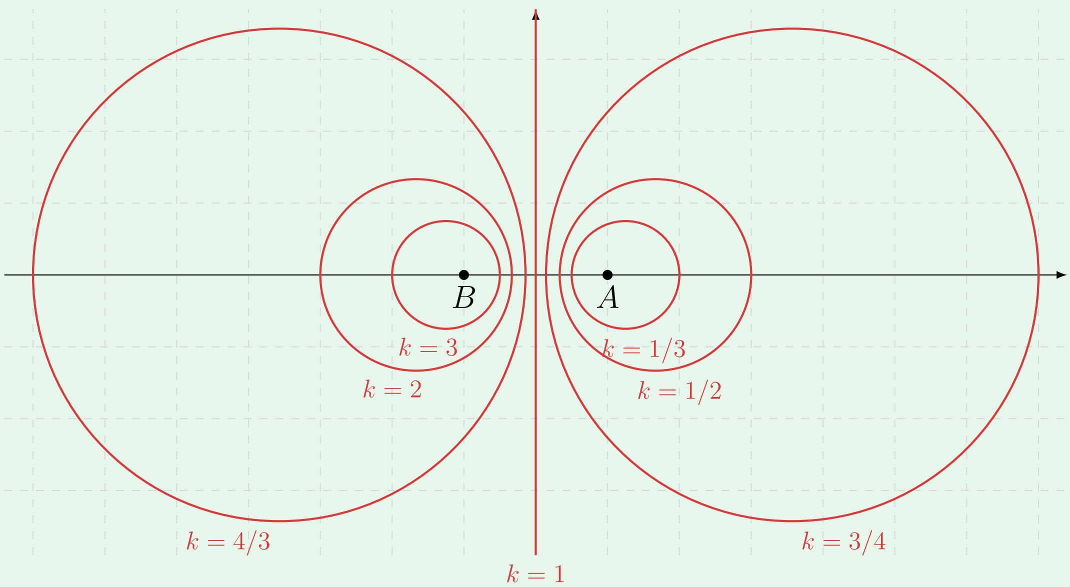
En introduisant le nombre $\omega=-\frac{5}{4}$, cela revient finalement à

$$\frac{MA}{MB}=3 \iff z\bar{z}-\bar{\omega}z-\omega\bar{z}=-1 \iff z\bar{z}-\bar{\omega}z-\omega\bar{z}=\frac{9}{16}-|\omega|^2$$

On reconnaît l'équation d'un cercle de centre $\Omega(-\frac{5}{4},0)$ et de rayon $r=\frac{3}{4}$.
Plus généralement, l'illustration ci-dessous représente l'ensemble des points M du plan tels que

$$\frac{MA}{MB}=k$$

pour diverses valeurs de k.



V.4.3. Transformations du plan

▷ *Pas de mimo associé sur IonisX.*

Transformations usuelles

Dans toute cette section, on note $\mathcal{P}$ le plan euclidien usuel.

Définition 13. On appelle **transformation du plan** une application $f : \mathcal{P} \to \mathcal{P}$ bijective.

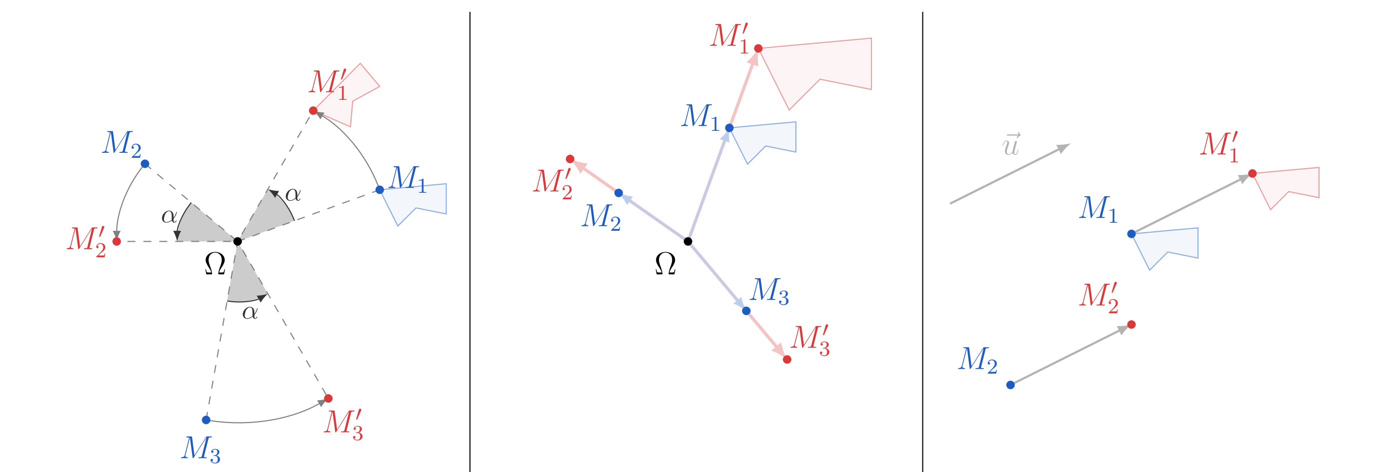
Exemple.

1. La rotation de centre O et d'angle $\frac{\pi}{3}$ est une transformation du plan. Sa bijection réciproque est la rotation de centre O et d'angle $-\frac{\pi}{3}$.
2. Une symétrie axiale est une transformation du plan. Sa bijection réciproque est elle-même.
3. Une projection orthogonale sur une droite n'est pas une transformation du plan (elle n'est ni injective, ni surjective).

Voici les transformations du plan les plus communes :

Définition 14.

1. Soient $\Omega \in \mathcal{P}$ et $\alpha \in \mathbb{R}$. La **rotation** de centre Ω et d'angle α est l'application qui à tout point $M \in \mathcal{P}$ associe l'unique point $M' \in \mathcal{P}$ tel que
$$\Omega M = \Omega M' \quad \text{et} \quad \widehat{(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'})} = \alpha.$$
2. Soient $\Omega \in \mathcal{P}$ et $k \in \mathbb{R}^*$. L'**homothétie** de centre Ω et de rapport k est l'application qui à tout point $M \in \mathcal{P}$ associe l'unique point $M' \in \mathcal{P}$ tel que
$$\overrightarrow{OM'} = k\,\overrightarrow{OM}.$$
3. Soit $\vec{u}$ un vecteur du plan. La **translation** de vecteur $\vec{u}$ est l'application qui à tout point $M \in \mathcal{P}$ associe l'unique point M' tel que
$$\overrightarrow{MM'} = \vec{u}.$$



Rotation de centre Ω et d'angle α — *Homothétie de centre Ω et de rapport k* — *Translation de vecteur u*

Remarque. Ce ne sont pas les seules transformations du plan : par exemple il existe encore les symétries axiales ou les similitudes.

Comme tout point (et tout vecteur) du plan peut être identifié à un nombre complexe via son affixe, une transformation du plan peut être représentée par une application de $\mathbb{C}$ dans $\mathbb{C}$ (souvent appelée **écriture complexe** de la transformation).

Proposition 16.

1. La rotation de centre $\Omega \in \mathcal{P}$ et d'angle $\alpha \in \mathbb{R}$ a pour écriture complexe
$$f : z \mapsto e^{i\alpha}(z-\omega)+\omega$$
avec ω l'affixe du point Ω.
2. L'homothétie de centre $\Omega \in \mathcal{P}$ et de rapport $k \in \mathbb{R}^*$ a pour écriture complexe
$$f : z \mapsto k(z-\omega)+\omega$$
avec ω l'affixe du point Ω.
3. La translation de vecteur $\vec{u}$ a pour écriture complexe
$$f : z \mapsto z+v$$
avec v l'affixe du vecteur $\vec{u}$.

Démonstration. Soient M, M' deux points du plan d'affixes respectives z et z'.

1. Notons que l'angle orienté $(\widehat{\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}})$ dans le repère orthonormé direct usuel $(O, \vec{e}_x, \vec{e}_y)$ peut être calculé de la façon suivante :
$$(\widehat{\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}}) = (\widehat{\vec{e}_x, \overrightarrow{\Omega M'}}) - (\widehat{\vec{e}_x, \overrightarrow{\Omega M}}) = \arg(z'-\omega) - \arg(z-\omega) = \arg\left(\frac{z'-\omega}{z-\omega}\right) \pmod{2\pi}.$$
Ainsi, si on note $r : \mathcal{P} \to \mathcal{P}$ la rotation de centre Ω et d'angle α, on a
$$M' = r(M) \iff \begin{cases} \Omega M' = \Omega M \\ (\widehat{\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}}) = \alpha \end{cases} \iff \begin{cases} |z'-\omega| = |z-\omega| \\ \arg\left(\frac{z'-\omega}{z-\omega}\right) = \alpha \pmod{2\pi} \end{cases} \iff \frac{z'-\omega}{z-\omega} = e^{i\alpha}.$$
En isolant ensuite z', on retrouve bien la relation $z' = e^{i\alpha}(z-\omega)+\omega$.
2. Notons h l'homothétie de centre Ω et de rapport k. Alors :
$$M' = h(M) \iff \overrightarrow{\Omega M'} = k\overrightarrow{\Omega M} \iff z'-\omega = k(z-\omega) \iff z' = k(z-\omega)+\omega.$$
3. Notons t la translation de vecteur $\vec{u}$. Alors :
$$M' = t(M) \iff \overrightarrow{MM'} = \vec{u} \iff z'-z = v \iff z' = z+v.$$

Classification des transformations complexes usuelles

Donnons maintenant une définition qui va s'avérer utile pour reconnaître les différentes transformations du plans données dans la définition V.4.3.

Définition 15. Soit $f : \mathbb{C} \to \mathbb{C}$ une application. Un **point fixe** de f est un nombre complexe $z \in \mathbb{C}$ tel que
$$f(z) = z.$$

Exemple.

- Une rotation non-triviale possède un seul point fixe (son centre).
- Une homothétie non-triviale possède un seul point fixe (son centre).
- Une translation non-triviale ne possède aucun point fixe.
- L'application $z \mapsto \bar{z}$ possède une infinité de points fixes (tous les nombres réels).

Par transformation « non-triviale », on entend une transformation différente de l'application identité $\mathrm{id}_{\mathcal{P}}$*, cette dernière pouvant être vue à la fois comme :*

- *une translation de vecteur* $\vec{0}$ *(le vecteur nul),*
- *une rotation d'angle* 0 *(modulo* 2π*),*
- *une homothétie de rapport* 1*.*

L'identité, elle, admet une infinité de points fixes puisque n'importe quel point du plan est un point fixe.

Ceci permet d'aboutir à la classification suivante.

Méthode. (Reconnaître l'écriture complexe d'une transformation)

Soit $f : \mathbb{C} \to \mathbb{C}$ une application. Pour déterminer si f est l'écriture complexe de l'une des transformations introduites dans cette section, on commence par chercher les points fixes de f en résolvant l'équation

$$f(z) = z.$$

- **Si f n'admet aucun point fixe.** Dans ce cas, on étudie l'expression $f(z) - z$.
  - **Si $f(z) - z$ est une constante complexe** v, alors pour tout $z \in \mathbb{C}$ on a

    $$f(z) = z + v$$

    et donc f est une translation de vecteur $\vec{u}$ d'affixe v.

    Remarque : en général dans ce cas on aura reconnu directement la forme $z \mapsto z + v$ *sans avoir eu besoin de passer par cette méthode.*
  - **Sinon**, f n'est pas l'une des transformations données dans la définition V.4.3.
- **Si f admet exactement un point fixe ω.** Dans ce cas, on étudie le rapport :

  $$\frac{f(z) - \omega}{z - \omega}.$$

  - **Si ce rapport est une constante réelle** $k \in \mathbb{R}^*$, alors pour tout $z \in \mathbb{C}$ on a

    $$f(z) = k(f(z) - \omega) + \omega$$

    et donc f est une homothétie de centre Ω d'affixe ω et de rapport k.
  - **Si ce rapport est une constante complexe $e^{i\alpha}$ de module** 1, alors pour tout $z \in \mathbb{C}$ on a

    $$f(z) = e^{i\alpha}(z - \omega) + \omega$$

    et donc f est une rotation de centre Ω d'affixe ω et d'angle α.
  - **Sinon**, f n'est pas l'une des transformations données dans la définition V.4.3.
- **Si f admet deux points fixes ou plus**, alors f n'est pas l'une des transformations données dans la définition V.4.3 (sauf si c'est la fonction identité).

Exemple. Déterminons la nature de la transformation $f : \mathbb{C} \to \mathbb{C}$ définie par

$$f(z) = -z + 2 - 4\mathrm{i}.$$

1. Commençons par déterminer les points fixes de f. Pour tout $z \in \mathbb{C}$ on a :

$$f(z) = z \iff -z + 2 - 4\mathrm{i} = z \iff 2z = 2 - 4\mathrm{i} \iff z = 1 - 2\mathrm{i}.$$

   Ainsi l'application f admet exactement un point fixe, à savoir le nombre $\omega = 1 - 2\mathrm{i}$ (donc, géométriquement, le point Ω de coordonnées $(1, -2)$).

2. On a alors :

$$\frac{f(z) - \omega}{z - \omega} = \frac{(-z + 2 - 4\mathrm{i}) - (1 - 2\mathrm{i})}{z - (1 - 2\mathrm{i})} = \frac{-z + 1 - 2\mathrm{i}}{z - 1 + 2\mathrm{i}} = -1.$$

   On trouve un rapport constant, qu'on peut interpréter de deux manières :
   - soit on remarque que -1 est un nombre réel non-nul, et donc on conclut que f correspond géométriquement à une homothétie de centre Ω et de rapport -1,
   - soit on remarque $-1 = e^{\mathrm{i}\pi}$ est un nombre complexe de module 1, et donc on conclut que f correspond géométriquement à une rotation de centre Ω et d'angle π.

Les deux conclusions sont justes : il faut se convaincre qu'une rotation d'angle π et une homothétie de rapport -1 correspondent à une seule même transformation du plan (qui est encore la même chose qu'une symétrie centrale). Nous sommes ici dans un cas exceptionnel : en général le rapport calculé sera soit réel, soit complexe de module 1 mais pas les deux à la fois, et il n'y aura donc qu'une seule bonne réponse possible (homothétie ou rotation).

Propriétés des transformations complexes usuelles

Terminons ce chapitre avec quelques résultats sur les transformations étudiées dans cette section.

Proposition 17. (Effet sur les longueurs)

- Les rotations et les translations conservent les longueurs (on dit que ce sont des **isométries**).
- Une homothétie de rapport $k \in \mathbb{R}^*$ multiplie les longueurs par $|k|$.

Démonstration. Soient A, B deux points du plan, et A', B' leurs images respectives par une transformation du plan f. On note z_A, z_B, z'_A, z'_B les affixes de ces points.

- Si f est une translation de vecteur $\vec{u}$ d'affixe ν, alors

$$A'B' = |z'_B - z'_A| = |(z_B + \nu) - (z_A + \nu)| = |z_B - z_A| = AB.$$

- Si f est une rotation de centre Ω d'affixe ω et d'angle $\alpha \in \mathbb{R}$, alors

$$A'B' = |z'_B - z'_A| = |(e^{\mathrm{i}\alpha}(z_B - \omega) + \omega) - (e^{\mathrm{i}\alpha}(z_A - \omega) + \omega)| = |e^{\mathrm{i}\alpha}(z_B - z_A)| = |e^{\mathrm{i}\alpha}||z_B - z_A| = AB.$$

- Si f est une homothétie de centre Ω d'affixe ω et de rapport $k \in \mathbb{R}$, alors

$$A'B' = |z'_B - z'_A| = |(k(z_B - \omega) + \omega) - (k(z_A - \omega) + \omega)| = |k(z_B - z_A)| = |k||z_B - z_A| = |k|AB.$$

Proposition 18. (Conservation des milieux) Soient A, B deux points du plan, I le milieu de $[AB]$, et soit f une translation, une homothétie ou une rotation.
Si on note A', B', I' les images respectives de A, B, I par f, alors I' est le milieu de $[A'B']$.

Démonstration. Notons $z_A, z_B, z_I, z'_A, z'_B, z'_C$ les affixes des points A, B, I, A', B', I'. Par hypothèse, on a

$$z_I = \frac{z_A + z_B}{2}, \qquad z'_A = f(z_A), \qquad z'_B = f(z_B), \qquad z'_I = f(z_I).$$

Montrons qu'alors I' est le milieu de $[A'B']$, c'est-à-dire que $z'_I = \dfrac{z'_A + z'_B}{2}$.
Pour éviter une disjonction de cas, remarquons que les translations, homothéties et rotations ont toutes une écriture de la forme

$$f : z \mapsto az + b$$

avec $(a, b) \in \mathbb{C}^2$. En travaillant directement avec cette forme générale, on trouve bien :

$$\frac{z'_A + z'_B}{2} = \frac{(az_A + b) + (az_B + b)}{2} = a\frac{z_A + z_B}{2} + \frac{2b}{2} = az_I + b = z'_I.$$

Proposition 19. (Conservation de certaines figures) Soit $f : \mathcal{P} \to \mathcal{P}$ une rotation, une homothétie ou une translation. Soient A, B deux points du plan, A', B' leurs images respectives par la transformation f, et $r > 0$ un réel. Alors :

1. l'image par f du segment $[AB]$ est le segment $[A'B']$,
2. l'image par f de la droite (AB) est la droite $(A'B')$,
3. l'image par f du cercle de centre A et de rayon r est le cercle de centre A' et de rayon

$$r' = \begin{cases} r & \text{si } f \text{ est une rotation ou une translation,} \\ |k| \times r & \text{si } f \text{ est une homothétie de rapport } k. \end{cases}$$

Chapitre VI.

Polynômes

VI.1. Introduction aux polynômes

▷ *MA11, module 11 — Introduction au polynômes*

VI.1.1. Définitions élémentaires

Dans ce chapitre, on utilisera la lettre $\mathbb{K}$ pour désigner au choix $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ à chaque fois qu'une définition ou un résultat est valide sur n'importe lequel de ces ensembles.

Définition 1. Un **polynôme** à coefficients dans $\mathbb{K}$ est une expression de la forme

$$P(X) = \underline{\hspace{6cm}}$$

avec $n \in \mathbb{N}$ et $a_0, a_1, \ldots, a_n \in \mathbb{K}$.

- $a_0, a_1, \ldots, a_n$ sont appelées les __________ du polynôme P,
- X est appelée l'**indéterminée** du polynôme.

On note ____ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Remarque. Attention, dans la définition ci-dessus, l'indéterminée X sert seulement de notation. Il ne faut pas la penser exactement comme une inconnue, mais plutôt comme une expression purement formelle que l'on pourra remplacer plus tard par un nombre (réel ou complexe), mais aussi par d'autres objets mathématiques (un autre polynôme, une fonction, une matrice, etc.). Quand on effectue cette substitution, on dit que l'on **évalue** le polynôme en une valeur donnée.

Définition 2. On appelle :

- **polynôme nul** de $\mathbb{K}[X]$ le polynôme dont tous les coefficients sont ____,
- **polynôme constant** un polynôme de la forme $P(X) =$ __ avec ______.

Le polynôme nul est donc un cas particulier de polynôme constant.

Définition 3. Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme non-nul. On appelle **degré** de P, noté $\deg P$, le plus grand entier i tel que

____

Par convention, on considère que le polynôme nul est de degré $-\infty$.

Exemple.
- $X^3 - 5X + \frac{3}{4}$ est un polnyôme de degré _ ,
- pour tout $n \in \mathbb{N}$, $X^n + 1$ est un polynôme de degré _ ,
- 2 est un polynôme constant, de degré _ .

Remarque. Attention, un polynôme constant a_0 est de degré 0 si et seulement si a_0 est non-nul ! Sinon, il s'agit du polynôme nul, et il est donc de degré ____ .

VI.1.2. Opérations élémentaires

Définition 4. Deux polynômes

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \qquad \text{et} \qquad Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$$

sont considérés égaux si et seulement si $\forall\, 0 \leqslant i \leqslant n,\ a_i = b_i$.

Définition 5. (Somme de polynômes) Soient

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \qquad \text{et} \qquad Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$$

deux polynômes. On définit leur somme $P + Q$ comme le polynôme

$$P + Q = (\_\_\_\_)X^n + (\_\_\_\_\_\_)X^{n-1} + \cdots + (\_\_\_\_)X + (\_\_\_\_).$$

Définition 6. (Produit de polynômes) Soient

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \qquad \text{et} \qquad Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$$

deux polynômes. On définit leur produit $P \times Q$ comme le polynôme

$$P \times Q = c_rX^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0$$

avec $r = n + m$ et pour tout $0 \leqslant k \leqslant r$,

$$c_k = \qquad \qquad .$$

Remarque. Évitez d'apprendre par cœur l'expression ci-dessus : il vaut mieux savoir la retrouver en se convaincant qu'il s'agit de la multiplication dont vous avez l'habitude. Par exemple,

$$\begin{aligned}(a_3X^3 + a_2X^2 + a_1X + a_0) \times (b_2X^2 + b_1X + b_0) = a_3b_2X^5 + (a_3b_1 + a_2b_2)X^4 + \\ (a_3b_0 + a_2b_1 + a_1b_2)X^3 + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + (a_1b_0 + a_0b_1)X + a_0b_0.\end{aligned}$$

Définition 7. (Multiplication par un scalaire) Soient

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

un polynôme et $\lambda \in \mathbb{K}$ un scalaire. On définit le produit $\lambda \cdot P$ comme le polynôme

$$\lambda P = (\quad)X^n + (\qquad)X^{n-1} + \cdots + (\quad)X + (\quad).$$

Proposition 1. Pour tout $(P, Q, R) \in (\mathbb{K}[X])^3$ et $\lambda \in \mathbb{K}$ on a :

1) $0 + P = P$ 2) $P + Q = Q + P$ 3) $(P + Q) + R = P + (Q + R)$
4) $1 \cdot P = P$ 5) $P \times Q = Q \times P$ 6) $(P \times Q) \times R = P \times (Q \times R)$
7) $P \times (Q + R) = P \times Q + P \times R$

Remarque. On dit que l'addition et la multiplication de polynômes sont *associatives* (propriétés 3 et 6) et *commutatives* (propriétés 2 et 5). De plus, la multiplication est *distributive* sur l'addition (propriété 7).

Proposition 2. Pour tout $(P, Q) \in \mathbb{K}[X]^2$,

- $\deg(P \times Q) =$ ____________,
- $\deg(P + Q) \leqslant$ ____________,
- $\deg(P(Q(X))) = \deg(P) \times \deg(Q)$.

Remarque. Attention à bien se souvenir qu'il n'y a pas égalité dans la deuxième propriété ci-dessus ! Par exemple, si

$$P = 2X^2 + 1 \qquad \text{et} \qquad Q = -2X^2 - X + 2,$$

alors $\deg P = \deg Q = 2$ et pourtant $\deg(P + Q) = \deg(-X + 3) = 1$.

VI.1.3. Compléments de vocabulaire

Définition 8. Pour tout $n \in \mathbb{N}$, on note $\mathbb{R}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n. Autrement dit,

$$\mathbb{R}_n[X] = \left\{ \qquad\qquad \right\}.$$

Définition 9.

- Un polynôme de la forme $a_k X^k$ est appelé un ______.
- Soit $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$ avec $a_n \neq 0$ (de sorte que P soit de degré n). Alors :
  - — $a_n X^n$ est appelé le ______ de P,
  - — a_n est appelé le ______ de P,
  - — si $a_n = 1$, on dit que le polynôme P est ______.

Exemple. Le polynôme $X^{n+1} - 1$ est un polynôme unitaire. Il est la somme de deux monômes : X^{n+1} (son terme dominant) et -1.

VI.2. Arithmétique des polynômes

▷ *MA11, module 12 — Division euclidienne*

VI.2.1. Divisibilité dans $\mathbb{K}[X]$

Définition 10. Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que B **divise** A, parfois noté $B \mid A$, s'il existe $Q \in \mathbb{K}[X]$ tel que ______.

On dit aussi que __ est **divisible** par __, ou que __ est un **multiple** de __.

Exemple. Le polynôme $X - 1$ divise le polynôme $X^2 - 3X + 2$, car $X^2 - 3X + 2 = (X - 1)(X - 2)$.

Proposition 3. Soit $(A, B, C) \in \mathbb{K}[X]^3$.

1. A divise A, 1 divise A et A divise 0.
2. Si A divise B et B divise A, alors ______.
3. Si C divise A et C divise B, alors pour tout $(U, V) \in \mathbb{K}[X]^2$, C divise ______.

VI.2.2. Division euclidienne

Théorème 1. (Division euclidienne) Soit $(A, B) \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

______ et ______.

On dit alors que Q est le ______ et R le ______ dans la division euclidienne de A par B.

Remarque.

- La condition $\deg R < \deg B$ revient à demander que soit $R = 0$, soit $0 \leqslant \deg R < \deg B$.
- La division euclidienne permet de caractériser la divisibilité : A est divisible par B si et seulement si le reste R est nul.

Exemple.

1. Effectuons la division euclidienne de $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ par $B = X^2 - X + 1$.

$$
\begin{array}{rrrrr|l}
2X^4 & -X^3 & -2X^2 & +3X & -1 & X^2 - X + 1 \\
\cline{6-6}
-2X^4 & +2X^3 & -2X^2 & & & 2X^2 + X - 3 \\
\cline{1-3}
 & X^3 & -4X^2 & +3X & & \\
 & -X^3 & +X^2 & -X & & \\
\cline{2-4}
 & & -3X^2 & +2X & -1 & \\
 & & 3X^2 & -3X & +3 & \\
\cline{3-5}
 & & & -X & +2 &
\end{array}
$$

On trouve un quotient égal à $Q(X) = 2X^2 + X - 3$ et un reste égal à $R(X) = -X + 2$.

2. Effectuons la division euclidienne de $A = X^4 - 3X^3 + X + 1$ par $B = X^2 + 2$.

$$
\begin{array}{rrrrr|l}
X^4 & -3X^3 & & +X & +1 & X^2 + 2 \\
\cline{6-6}
-X^4 & & -2X^2 & & & X^2 - 3X - 2 \\
\cline{1-3}
 & -3X^3 & -2X^2 & +X & & \\
 & 3X^3 & & +6X & & \\
\cline{2-4}
 & & -2X^2 & +7X & +1 & \\
 & & 2X^2 & & +4 & \\
\cline{3-5}
 & & & 7X & +5 &
\end{array}
$$

On trouve un quotient égal à $X^2 - 3X - 2$ et un reste égal à $7X + 5$.

VI.3. Racine d'un polynôme et factorisation

▷ *MA11, module 13 — Racine d'un polynôme et factorisation*

VI.3.1. Racine d'un polynôme

Définition 11. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une **racine** de P si $\underline{\hspace{3cm}}$.

Proposition 4. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

$$P(\alpha) = 0 \iff \underline{\hspace{4cm}}.$$

Démonstration. D'après le théorème de division euclidienne, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$P(X) = Q(X) \times (X - \alpha) + R(X) \qquad \text{et} \qquad \deg(R) < \deg(X - \alpha).$$

Comme $\deg(X - \alpha) = 1$, la condition sur le degré de R impose que R soit un polynôme constant, c'est-à-dire de la forme $R(X) = r_0$ avec $r_0 \in \mathbb{K}$. En évaluant l'égalité précédente en $X = \alpha$, on trouve alors

$$P(\alpha) = 0 + R(\alpha) = r_0.$$

Ceci donne bien la chaîne d'inégalités suivante :

$$(X - \alpha) \text{ divise } P \iff R \text{ est nul} \iff r_0 = 0 \iff P(\alpha) = 0.$$

Définition 12. Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$. On dit que α est une racine de P de **multiplicité** k (ou d'**ordre** k) si ________ divise P et ________ ne divise pas P.

En particulier :

- Si $k = 1$, on parle aussi de ________ (sinon, c'est une racine **multiple**),
- si $k = 2$, on parle aussi de ________,
- etc.

Proposition 5. (Caractérisations de la multiplicité) Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$. Les trois propositions suivantes sont équivalentes :

- α est racine de multiplicité k de P,
- il existe $Q \in \mathbb{K}[X]$ tel que $P =$ ________ et ________,
- ________ $= 0$ et ________.

VI.3.2. Existence des racines dans $\mathbb{C}$

Théorème 2. (Théorème de d'Alembert–Gauss)

- Tout polynôme à coefficients complexes de degré $n \geqslant 1$ admet au moins une racine dans $\mathbb{C}$.
- Plus précisément, tout polynôme à coefficients complexes de degré $n \geqslant 1$ admet exactement n racines dans $\mathbb{C}$ (comptées avec leurs multiplicités).

Compter le nombre de racines avec leurs multiplicités signifie qu'une racine de multiplicité k compte pour k fois.

Exemple. Considérons le polynôme

$$P(X) = 3X^3 - 2X^2 + 6X - 4.$$

- Si l'on travaille dans $\mathbb{Q}[X]$ ou dans $\mathbb{R}[X]$, alors P admet une seule racine (simple) : __. On a la factorisation :

$$P(X) = \qquad\qquad .$$

- Si l'on travaille dans $\mathbb{Q}[X]$ ou dans $\mathbb{R}[X]$, alors P admet ____ racines simples : $\frac{2}{3}$, $\mathrm{i}\sqrt{2}$ et $-\mathrm{i}\sqrt{2}$. On a la factorisation :

$$P(X) = \qquad\qquad .$$

Remarque. On voit dans l'exemple précédent que le théorème de d'Alembert–Gauss n'est valide que sur $\mathbb{C}$. Sur $\mathbb{Q}$ ou sur $\mathbb{R}$, on peut seulement affirmer qu'un polynôme de degré $n \geqslant 1$ admet *au plus* n racines.

Exemple. (Cas des polynômes de degré 2 dans $\mathbb{R}[X]$) Considérons le polynôme

$$P(X) = aX^2 + bX + c$$

avec $(a, b, c) \in \mathbb{R}^3$, $a \neq 0$.

- Si $\Delta = b^2 - 4ac > 0$, alors P admet deux racines réelles distinctes

$$\frac{-b + \sqrt{\Delta}}{2a} \quad \text{et} \quad \frac{-b - \sqrt{\Delta}}{2a}.$$

- Si $\Delta > 0$, alors P n'admet pas de racine réelle, mais il possède deux racines complexes conjuguées

$$\frac{-b + \mathrm{i}\sqrt{|\Delta|}}{2a} \quad \text{et} \quad \frac{-b - \mathrm{i}\sqrt{|\Delta|}}{2a}.$$

- Si $\Delta > 0$, alors P admet une racine réelle double

$$\frac{-b}{2a}.$$

On a bien toujours 2 racines, à condition de les compter avec leurs multiplicités et de s'autoriser à chercher des racines dans $\mathbb{C}$.

Exemple. (Raisonnement sur le nombre de racines) Soit $n \geqslant 2$ un entier. Montrons que le polynôme $P(X) = X^n - 1$ admet n racines distinctes sans les calculer.

- D'après le théorème de d'Alembert–Gauss, P admet n racines comptées avec leurs multiplicités.
- Supposons par l'absurde que P admette une racine $\alpha \in \mathbb{C}$ de multiplicité au moins 2. D'après la caractérisation de la multiplicité par les dérivées, cela signifie que $P(\alpha) = 0$ et $P'(\alpha) = 0$. Or,
  - $P(X) = X^n - 1$ donc $P(\alpha) = 0$ indique que $\alpha^n = 1$ et donc $\alpha \neq 0$,
  - $P'(X) = nX^{n-1}$ donc $P'(\alpha) = 0$ indique que $n\alpha^{n-1} = 0$, et donc $\alpha = 0$.

  On arrive à une contradiction. C'est donc que l'hypothèse de départ est fausse, c'est-à-dire que P ne contient que des racines simples.

Ainsi, on peut affirmer que P possède exactement n racines simples distinctes (on pouvait en réalité les calculer : ce sont les racines n-ièmes de l'unité).

VI.3.3. Liens avec la factorisation

Définition 13. Soit $P \in \mathbb{K}[X]$ tel que $\deg P \geqslant 1$. On dit que P est **irréductible** (dans $\mathbb{K}[X]$) si pour tout $Q \in \mathbb{K}[X]$,

$$Q \text{ divise } P \implies (Q \in \underline{\qquad} \quad \text{ou} \quad \exists \lambda \in \mathbb{K}^*,\ Q = \underline{\qquad}).$$

Dans le cas contraire, on dit que P est **réductible**.

Remarque. Il s'agit du concept équivalent à celui de *nombre premier* dans $\mathbb{Z}$: un nombre $p \in \mathbb{Z}$ est premier si ses seuls diviseurs dans $\mathbb{Z}$ sont ± 1 et $\pm p$.

Remarque. D'après la définition, un polynôme P est donc réductible dans $\mathbb{K}[X]$ s'il peut s'écrire sous la forme $P = A \times B$ avec $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ tous deux non-constants (c'est-à-dire $\deg(A)$ ___ et $\deg(B)$ ___).

Exemple.

- Le polynôme $X^2 - 1$ est réductible dans $\mathbb{R}[X]$ car il peut s'écrire $X^2 - 1 =$ ___.
- Le polynôme $X^2 + 1$ est réductible dans $\mathbb{C}[X]$ car il peut s'écrire $X^2 - 1 =$ ___), en revanche il est irréductible dans ___.
- Le polynôme $X^2 - 2$ est réductible dans $\mathbb{R}[X]$ car il peut s'écrire $X^2 - 2 =$ ___, en revanche il est irréductible dans ___.

Théorème 3. (Décomposition en facteurs irréductibles)

1. Tout polynôme non-constant $A \in \mathbb{K}[X]$ s'écrit sous la forme

$$A = \_\_\_\_$$

avec $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $(k_1, \ldots, k_r) \in (\mathbb{N}^*)^r$ et $P_1, \ldots, P_r$ des polynômes irréductibles et unitaires deux à deux distincts.

2. De plus, cette décomposition est unique à l'ordre des facteurs près.

Remarque. Ce résultat est l'analogue de la décomposition en facteurs premiers dans $\mathbb{Z}$.

Théorème 4. Les polynômes irréductibles de $\mathbb{C}[X]$ sont ___.

Remarque. Cela signifie que dans $\mathbb{C}[X]$, la décomposition donnée par le théorème VI.3.3 est de la forme

$$A = \_\_\_\_$$

où $\alpha_1, \alpha_2, \ldots, \alpha_r$ sont les racines de A dans $\mathbb{C}$ et $k_1, k_2, \ldots, k_r$ leurs multiplicités respectives.

Théorème 5. Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes ___, et
- les polynômes de degré 2 ayant un discriminant ___.

Exemple. Considérons le polynôme

$$P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1).$$

- P est déjà décomposé en produit de polynômes irréductibles dans $\mathbb{R}[X]$ car X^2+1 et X^2+X+1 ont des discriminants strictements négatifs.

- En revanche, la décomposition en facteurs irréductibles de P dans $\mathbb{C}[X]$ est

$$P(X) = 2X^4(X-1)^3(X-\mathrm{i})^2(X+\mathrm{i})^2(X-j)(X-\bar{j})$$

avec $j = e^{\frac{2\mathrm{i}\pi}{3}} = \dfrac{-1+\mathrm{i}\sqrt{3}}{2}$.

Exemple. Décomposons en facteurs irréductibles dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ le polynôme

$$P(X) = X^4 + 1.$$

- Commençons par décomposer en facteurs irréductibles sur $\mathbb{C}$. On reconnaît d'abord l'identité remarquable
$$P(X) = X^4 - \mathrm{i}^2 = (X^2+\mathrm{i})(X^2-\mathrm{i}).$$
En calculant ensuite les racines carrées de i et $-\mathrm{i}$, on arrive finalement à la décomposition
$$P(X) = \left(X - \frac{\sqrt{2}}{2}(1+\mathrm{i})\right)\left(X + \frac{\sqrt{2}}{2}(1+\mathrm{i})\right)\left(X - \frac{\sqrt{2}}{2}(1-\mathrm{i})\right)\left(X + \frac{\sqrt{2}}{2}(1-\mathrm{i})\right).$$
On aurait pu aussi directement calculer les racines quatrièmes de -1.
- Pour obtenir la décomposition en facteurs irréductibles sur $\mathbb{R}$, il suffit de regrouper les facteurs correspondant à des racines conjuguées. En effet, en réorganisant ainsi :
$$P(X) = \left(\left(X - \frac{\sqrt{2}}{2}(1+\mathrm{i})\right)\left(X - \frac{\sqrt{2}}{2}(1-\mathrm{i})\right)\right)\left(\left(X + \frac{\sqrt{2}}{2}(1+\mathrm{i})\right)\left(X + \frac{\sqrt{2}}{2}(1-\mathrm{i})\right)\right)$$
on trouve finalement $P(X) = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$.

Remarque. La méthode utilisée dans l'exemple précédent pour passer de la décomposition en irréductible dans $\mathbb{C}[X]$ à celle dans $\mathbb{R}[X]$ fonctionne pour n'importe quel polynôme $P \in \mathbb{R}[X]$. En effet, on a les deux résultats suivants.

1. Soit $\alpha \in \mathbb{C}$. Alors α est racine de P si et seulement si $\bar{\alpha}$ est racine de P.
   Preuve. *Notons $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Les propriétés de la conjugaison complexe donnent l'égalité*
   $$\overline{P(\alpha)} = \overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0} = \bar{a}_n\bar{\alpha}^n + \bar{a}_{n-1}\bar{\alpha}^{n-1} + \cdots + \bar{a}_1\bar{\alpha} + \bar{a}_0.$$
   Or le polynôme P est à coefficients réels, donc pour tout $0 \leqslant i \leqslant n$, $\bar{a}_i = a_i$, d'où finalement $\overline{P(\alpha)} = P(\bar{\alpha})$. Ceci permet alors d'établir l'équivalence :
   $$\alpha \text{ racine de } P \iff P(\alpha) = 0 \iff \overline{P(\alpha)} = 0 \iff P(\bar{\alpha}) = 0 \iff \bar{\alpha} \text{ racine de } P.$$
   Ce résultat garantit que dans la décomposition sur $\mathbb{C}$ d'un polynôme à coefficients réels, les racines complexes apparaissent toujours par paires de racines conjuguées.
2. Pour tout $\alpha \in \mathbb{C} \setminus \mathbb{R}$, $(X-\alpha)(X-\bar{\alpha})$ est un polynôme irréductible de $\mathbb{R}[X]$.
   Preuve. Pour tout $\alpha \in \mathbb{C}$,
   $$(X-\alpha)(X-\bar{\alpha}) = X^2 - (\alpha+\bar{\alpha})X + \alpha\bar{\alpha} = X^2 + 2\,\mathrm{Re}(\alpha)X + |\alpha|^2.$$

On trouve bien un polynôme à coefficients réels dans tous les cas, qui est irréductible lorsque $\alpha \in \mathbb{C} \setminus \mathbb{R}$ puisqu'il admet alors deux racines complexes conjuguées.

On peut donc toujours retrouver la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ d'un polynôme à coefficients réels en regroupant deux à deux les facteurs correspondant à des racines complexes conjuguées dans sa décomposition en irréductible dans $\mathbb{C}[X]$.