# Fonctions elliptiques

**Exercice** [Bases et aires]
Montrer que deux éléments $\omega_1$, $\omega_2$, linéairement **R**-indépendants d'un réseau de **C** forment une base de ce réseau si et seulement si le parallélogramme de sommets 0, $\omega_1$, $\omega_1+\omega_2$, $\omega_2$ ne contient que ces 4 éléments de $\Omega$.

Supposons il n'y ait aucun point dans le parallélogramme. Pour $z \in \Omega$, nous pouvons écrire $z = \lambda_1\omega_1 + \lambda_2\omega_2$ avec $\lambda$'s réels. En enlevant à $z$ un élément de la forme $n\omega_1 + m\omega_2 \in \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ nous obtenons un point dans $\omega$ et dans le parallélogramme :

$$\nu_1\omega_1 + \nu_2\omega_2 \text{ avec } \nu_1, \nu_2 \in [0,1].$$

Ceci implique les $\nu$'s donc les $\lambda$'s sont entiers ainsi $z \in \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ *i.e.* $(\omega_1, \omega_2)$ est une base de $\Omega$.

Si $(\omega_1, \omega_2)$ est une base de $\Omega$ et $z$ est un point de $\Omega$ dans le parallélogramme. Les coordonnées réelles de $z$ étant (uniques et) entières, $z$ est l'un des 4 sommets du parallélogramme.

**Remarque 1.** *Si $(\eta_1, \eta_2)$ est une* **R***-base de* **C***, la valeur absolue du déterminant de $(\omega_1, \omega_2)$ dans cette base est l'aire du parallélogramme donné dans l'énoncé, normalisé de telle sorte que l'aire du parallélogramme construit sur $(\eta_1, \eta_2)$ soit 1. Soit $\Omega$ un réseau de* **C***. D'après un résultat du cours, tous les paralléllogrammes construits sur des bases de $\Omega$ ont même aire. Retrouvez ce résultat dans votre cours.*

On a par exemple le résultat suivant à l'origine de la célèbre **formule de Pick** : Soit $T$ un triangle de sommets de coordonnées entières ne contenant aucun point de coordonnées entières alors ce triangle est d'aire 1

**Remarque 2.** *Vous pouvez définir un réseau de $\mathbf{R}^n$ et montrer la version en dimension n du résultat de l'exercice. C'est très facile. Les interprétations en terme de volumes sont plus intéressantes : Que devient la formule de Pick ?*

**Exercice** [Endomorphismes de réseaux]
On appelle morphisme de réseaux de $\Omega_1$ dans $\Omega_2$, deux réseaux de **C**, une similitude $\ell(z) = \lambda z$ induisant un morphisme de groupe de $\Omega_1$ dans $\Omega_2$. Deux réseaux sont semblables s'ils sont isomorphe *via* une similitude

1. Montrer qu'à une similitude près, un réseau $\Omega$ est toujours de la forme $\mathbf{Z} + \tau\mathbf{Z}$ avec $\tau \in \mathbb{H}$.
   Soit $(\omega_1, \omega_2)$ une base de $\Omega$. Puisque les $\omega$'s sont non nuls, la similitude $z \mapsto \frac{1}{\omega_1}z$ (resp. $z \mapsto \frac{1}{\omega_2}z$) envoie $\Omega$ sur le réseau $\mathbf{Z} + \frac{\omega_2}{\omega_1}\mathbf{Z}$ (resp. $\frac{\omega_1}{\omega_2}\mathbf{Z} + \mathbf{Z}$).
   Puisque $\frac{\omega_1}{\omega_2}\frac{\omega_2}{\omega_1} = 1$ l'un de ces deux quotients à une partie imaginaire positive, et même strictement positive par indépendance sur **R**. On le note $\tau$.
2. Montrer que si $\tau$ et $\tilde{\tau}$ sont deux complexes de $\mathbb{H}$ tels que $\mathbf{Z} + \tau\mathbf{Z}$ soit semblable à $\mathbf{Z} + \tilde{\tau}\mathbf{Z}$ alors il existe $h \in \mathrm{PSL}_2(\mathbf{Z})$ tel que $\tau = h\tilde{\tau}$.
   Soit $\lambda$ le multiplicateur d'une telle similitude. D'après le cours $\lambda(1, \tau) = (1, \tilde{\tau})A$ avec $A \in \mathrm{SL}_2(\mathbf{Z})$, en exprimant les quotients des deux complexes de chaque coté de l'égalité, on obtient le résultat.
3. Soit $\Omega$ un réseau et $\ell$ un automorphisme de réseau de $\Omega$.
   (a) Montrez que $\lambda$ et $\overline{\lambda}$ sont les deux valeurs propres d'une matrice à coefficients entiers de déterminant 1.
   Il suffit de reprendre la question précédente. Pour $(\omega_1, \omega_2)$ une base de $\Omega$, $\lambda(\omega_1, \omega_2)$ est une autre base. Ainsi $\lambda(\omega_1, \omega_2) = (\omega_1, \omega_2)A$ avec $A \in \mathrm{SL}_2(\mathbf{Z})$. Ceci prove que $\lambda$ est du type annoncé dans l'énoncé. On sait que les valeurs propres complexes d'une matrice réelle arrivent par deux conjugués.

(b) En déduire que les valeurs possibles pour $\lambda$ sont

$$\pm 1, \pm i, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$$

Les valeurs propres de $A \in \mathrm{SL}_2(\mathbf{Z})$ sont des solutions de $\lambda^2 - \mathrm{tr}(A)z + 1$ avec $\mathrm{tr}(A) \in \mathbf{Z}$. (Ce sont en particulier des entiers quadratiques).

Si $\lambda$ est une racine, l'autre racine est $\frac{1}{\lambda}$ et $\lambda + \frac{1}{\lambda} \in \mathbf{Z}$.

— Si $\lambda$ est réel alors $\lambda\omega_1 \in \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Par unicité des coordonnées $\lambda \in \mathbf{Z}$. D'après la remarque ci-dessus on doit avoir $\frac{1}{\lambda} \in \mathbf{Z}$. Ceci implique $\lambda = \pm 1$.

— Si $\lambda$ n'est pas réel alors la seconde racine est $\bar{\lambda}$. Ainsi $\lambda\bar{\lambda} = 1$ et $\lambda + \bar{\lambda} \in \mathbf{Z}$. Si ce dernier est 0, $\lambda = \pm i$. Si ce dernier est 1, $\lambda = \frac{1}{2} \pm \frac{\sqrt{3}}{2} i$. Si c'est $-1$ ...Les autres valeurs entières ne peuvent pas apparaitre.

(c) Donner des exemples de réseaux et d'automorphismes réalisant ces 8 valeurs.

N'importe quel réseau admet $\pm 1$ comme automorphisme.

Vérifiez que :

$\mathbf{Z} + \mathbf{Z}i$ convient pour $\pm i$

$\mathbf{Z} + \mathbf{Z}j$ convient pour $\pm j$ et $\pm 1 - j$

**Remarque 3.** *On a toujours $\mathbf{Z} \subset \mathrm{End}(\Omega)$ les réseaux ayant un anneau d'endomorphismes strictement plus grand que $\mathbf{Z}$ sont dit* **à multiplication complexe***. L'ensemble des $\tau \in \mathbb{H}$ tels que $\mathbf{Z} + \tau\mathbf{Z}$ soit à multiplication complexe est un ensemble de points très spéciaux de $\mathbb{H}$. Nous avons montré qu'il est invariant sous l'action de $\mathrm{PSL}_2(\mathbf{Z})$. Trouvez où.*

**Exercice**[L'équation différentielle de la fonction $\wp$.]
Soient $\Omega$ un réseau, $\wp$ sa fonction de Weierstrass et $(f')^2 = 4f^3 - g_2 f - g_3$ son équation différentielle. Décrire toutes les solutions de cette équation différentielle.

La fonction de Weiestrass est solution de cette équation. Cette équation étant autonome, toutes les translatées de $\wp$ sont aussi solutions : pour $c \in \mathbf{C}$, $z \mapsto \wp(z+c)$ est solution.

Avons-nous toutes solutions ainsi ?

D'après le théorème de Cauchy une solution $f$ holomorphe en $z_0$ est uniquement déterminée par le choix de ses conditions initiales : $p_0 (= f(z_0))$ et le choix d'un $q_0 (= f'(z_0))$ verifiant $q_0^2 = 4p_0^3 - g_2 p_0 - g_3$. Fixons $p_0$ et construisons les deux solutions valant $p_0$ en $z_0$.

Puisque $\wp$ est elliptique de degré 2, il existe deux solutions (modulo $\Omega$) à l'équation $\wp(z) = p_0$. Notons l'une d'elle $c$, l'autre sera $-c$ par parité. Elles seront différentes si $2c \not\equiv 0 \mod \Omega$. Ainsi $\wp(z + (c - z_0))$ et $\wp(z + (-c - z_0))$ sont des solutions prenant la valeur $p_0$ en $z_0$. Reste à vérifier qu'elles sont différentes par exemple en calculant leurs dérivées en $z_0$ : $\wp'(c)$ et $\wp'(-c) = -\wp'(c)$ respectivement. Ces deux nombres sont différents si et seulement s'ils sont non nuls *i.e.* $2c \notin \Omega$ ($c$ n'est pas de 2-torsion).

Si $c$ est de 2-torsion, c'est-à-dire si $4p_0^3 - g_2 p_0 - g_3 = 0$ nous ne pouvons plus utiliser le théorème de Cauchy pour savoir combien de solutions vérifient $f(z_0) = p_0$.

Néanmoins les calculs ci-dessus donnent une solution valant $p_0$ en $z_0$. Le fait que $2c \in \Omega$ mais $c \notin \Omega$ implique que $p_0 = \wp(c)$ est un zéro de $4x^3 - g_2 x - g_3$, la fonction constante égale à $p_0$ est aussi une solution de l'équation différentielle.

Montrons qu'il n'y a pas d'autre solutions vérifiant $f(z_0) = p_0$ et $f'(z_0) = 0$. En dérivant l'équation nous obtenons $2f'f'' = 12f^2 f' - g_2 f'$. Si $f$ n'est pas constante alors $f'' = 6f^2 - g_2/2$. D'après le théorème de Cauchy il n'existe qu'une seule solution de cette dernière équation telle que $f(z_0) = p_0$ et $f'(z_0) = 0$ : c'est la fonction que nous avons construite ! Il n'y a donc pas d'autres solutons

Pour des valeurs réelles de $g_2$ et $g_3$ tracer le portait de phase réel de l'équation de Weierstrass.

**Exercice**[Les tangentes de la cubique]
Soient $\Omega$ un réseau de $\mathbf{C}$, et $(\wp, \wp')$ la paramétrisation "de Weierstrass" de la cubique $\mathscr{C} \subset \mathbf{C}^2$ d'équation $y^2 = 4x^3 - g_2 x - g_3$. Montrez que deux points $z_1$ et $z_2$ de $\mathbf{C} \backslash \Omega$ vérifient $2z_1 + z_2 \equiv 0 \mod \Omega$ si et seulement si leurs images respectives $A_1$ et $A_2$ portent la tangente à $\mathscr{C}$ en $A_1$.

Déterminer les paramètres des points d'inflexions de $\mathscr{C}$ (points où la courbe a un contact d'ordre au moins deux avec sa tangente).

Notons $\varepsilon$ un nombre complexe non nul suffisament petit. Puisque $(z_1+\varepsilon)+(z_1-\varepsilon)+z_2 \equiv 0$ leurs images par $(\wp,\wp')$ seront trois points alignés de la cubique : $A_1(\varepsilon)$, $A_1(-\varepsilon)$ et $A_2$. La restriction de l'équation cubique à cette droite est un polynome de degré 3 ayant ces racines en $A_1(\varepsilon)$, $A_1(-\varepsilon)$ et $A_2$. En laissant $\varepsilon$ tendre vers 0, nous obtenons une droite sur laquelle la restriction de l'équation cubique à un zéro double en $A_1$. Ce point est un zero de la dérivée, autrement dit; en ce point le vecteur directeur de la droite est dans le noyau de la différentielle de l'équation cubique : cette droite est une tangente.

Pourquoi les droites ci-dessus ne sont-elles pas verticales (d'équation $x=c$)?

En un point d'inflexion, la tangente a un contact anormale avec la courbe. La restriction de l'équation cubique à la tangente a un zéro triple au point de tangente : la tangent ne rencontre aucun autre point de la cubique.

Si $A$ est un tel point correspondant à $z \in \mathbf{C}\backslash\Omega$, montrons que $3z \equiv 0 \mod \Omega$. Nous avons $2z+(-2z)\equiv 0$ avec $z \notin \Omega$ et $-2z \notin \Omega$, ainsi la tangente en $A$ passe par l'image de $-2z$ ce qui implique que $-2z \equiv z \mod \Omega$.

Les points d'inflexions sont les points de 3-torsions.

Pourquoi a-t-on $2z \not\equiv 0$? Les points de 2-torsion annulent $\wp'$ et correspondent aux points de tangentes verticales qui ne sont pas des points d'inflexions.

**Exercice**[Formule d'addition et de duplication]

Soient trois points telles que $z_1+z_2+z_3 \equiv 0 \mod \Omega$ et $y=ax+b$ l'équation réduite de la droite passant par $(\wp(z_1),\wp'(z_1))$, $(\wp(z_2),\wp'(z_2))$ et $(\wp(z_3),\wp'(z_3))$.

Remarquons d'abord que pour avoir une équation réduite de la forme annoncée, la droite ne doit pas être verticale ainsi aucun des trois nombres ne doit appartenir à $\Omega$.

1. Montrer que $4x^3-a^2x^2-(2ab+g_2)x-(b^2+g_3)$ s'annule lorsque $x$ prend les valeurs $\wp(z_1)$, $\wp(z_2)$ et $\wp(z_3)$. Les points d'intersection de la cubique $y^2=4x^3-g_2x-g_3$ et de la droite $y=ax+b$ vérifient les deux équations. En éliminant les $y$, nous obtenons l'équation ci-dessus ne portant que sur l'abscisse du point. Ces dernièrss sont les valeurs prise par $\wp$.
2. En déduire que $4(\wp(z_1)+\wp(z_2)+\wp(z_3))=a^2$,
   ... la somme des racines d'un polynome ...
3. puis que
$$\wp(z_1+z_2)=\left(\frac{\wp'(z_1)-\wp'(z_2)}{2(\wp(z_1)-\wp(z_2))}\right)^2-\wp(z_1)-\wp(z_2)$$
   Par parité $\wp(z_3)=\wp(z_1+z_2)$ il nous suffit donc de montrer que $a=\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}$. Ce dernier est bien la pente de la droite passant par $(\wp(z_1),\wp'(z_1))$, $(\wp(z_2),\wp'(z_2))$.
4. Déterminer une fraction rationnelle $R$ telle que $\wp(2z)=R(\wp(z))$.
   Nous voulons faire tendre $z_2$ vers $z_1$, ce qui fait tendre la sécante en $(\wp(z_1),\wp'(z_1))$, $(\wp(z_2),\wp'(z_2))$ vers la tangente en $(\wp(z_1),\wp'(z_1))$.
   La pente de la tangente à la cubique en $(\wp(z_1),\wp'(z_1))$ est
$$-\frac{12\wp(z_1)^2-q_2}{2\wp'(z_1)}$$
   ce qui prouve que :
$$\wp(2z_1)=\frac{1}{4}\frac{\left(6\wp(z_1)^2-g_2/2\right)^2}{4\wp(z_1)^3-g_2\wp(z_1)-g_3}-2\wp(z_1)$$

# 1 Rappels ? ?

Il existe plusieurs définitions de courbes et elles ne sont pas toutes compatibles. Lorsqu'on nomme une courbe par son degré c'est que cette courbe est une courbe algébrique plane. Les courbes de degré deux sont les coniques, de degré trois les cubiques, puis viennent les quartiques, les quintiques, sextiques etc...

Une courbe algébrique plane $\mathscr{C}$ est le lieu des zéros une polynôme $P \in \mathbf{C}[X,Y]$. Ce polynome $P$ n'est pas unique. Si on note $I \subset \mathbf{C}[X,Y]$ l'ideal des polynomes s'annulant sur $\mathscr{C}$ (et peut être ailleurs aussi), on montre que $I$ est un idéal principal. N'importe quel générateur a le même degré. Nous noterons $P$ un de ces générateurs.

Une tangente à $\mathscr{C}$ en $p$ est une droite $d$ telle que $P|_d$ ait un zéro d'ordre au moins deux en $p$. Un point $\mathscr{C}$ est lisse en $p$ si la courbe n'a qu'une tangente en $p$. On dt aussi que $p$ est lisse.

On dispose du critère jacobien : $p$ est lisse si $\nabla P(p) \neq 0$ et dans ce cas la pente de la tangent est l'orthogonal du gradient.

**Exemples 1.** *La courbe d'équation $Y^2 - X^3$ n'est pas lisse en 0, toutes les droites passant par 0 sont des tangentes (il y en a quand même une de plus tangente que les autres, Laquelle ?). Ce type de singularité est un cusp, un point de rebroussement ...*
*La courbe d'équation $Y^2 - X^3 - X^2$ n'est pas lisse en 0, elle admet deux tangentes particulières en 0, lesquelles ? Ce type de singularité s'appelle un nœud, un point double, un node ... et nous trouverez encore d'autres noms. Les objets importants ont toujours plusieurs noms (et des définitions flottantes)*

Nous ne pouvons dessiner que la partie réelle des courbes algébriques planes (points à coordonnées entières vérifiant l'équation). Le **théorème d'universalilé de Kempe** permet au bricoleurs de les tracer exactement. `http://images.math.cnrs.fr/Les-systemes-articules-et-leurs-configurations.html?id`$_{f}orum = 11853$