Université de Strasbourg
Département de Mathématiques

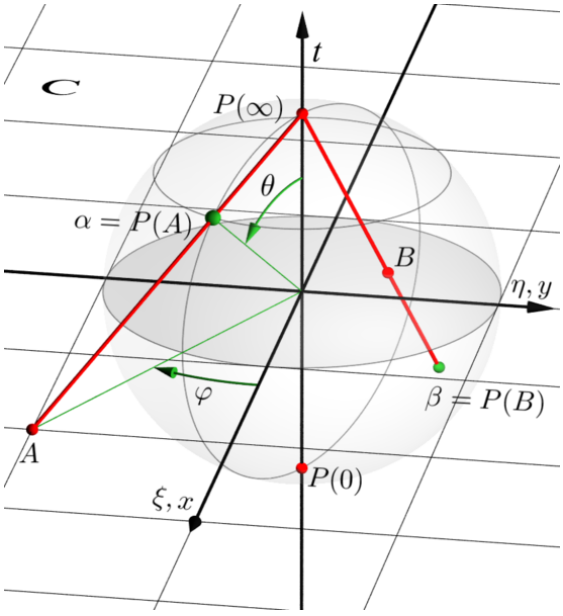
Avril 2017

Master Class Arithmétique et Géométrie Algébrique

Courbes elliptiques

1 $\mathbb{P}^1$ et la sphère de Riemann

La *projection stéréographique* définit un homéomorphisme entre $\mathbb{C}$ et $S^2 \setminus \{(0,0,1)\}$. Pour le voir, on considère la sphère unité dans $\mathbb{R}^3$ et on identifie $\mathbb{C}$ avec le plan $z = 0$ dans $\mathbb{R}^3$. La projection stéréographique est l'application qui envoie un point $P \neq (0,0,1)$ de S^2 sur le point d'intersection de la droite passant par $(0,0,1)$ et P avec le plan $\mathbb{C}$. Cela définit une carte sur $S^2 \setminus \{(0,0,1)\}$.



https://commons.wikimedia.org/wiki/File:RiemannSphere.png

Pour voir que cette application identifie S^2 avec $\mathbb{P}^1$, et tant que surface de Riemann, on note que la projection stéréographique par rapport à $(0,0,-1)$, composée avec la conjugaison complexe définit une carte sur $S^2 \setminus \{(0,0,-1)\}$. L'application de transition entre les deux cartes est l'application $\mathbb{C}^* \to \mathbb{C}^*$ donnée par $z \mapsto 1/z$.

On a donc défini sur S^2 la même structure de surface de Riemann que sur $\mathbb{P}^1$, le recollement de deux copies de $\mathbb{C}$ via l'isomorphisme $\mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto 1/z$.
Notons aussi que, en tant qu'espace topologique, S^2 (où encore $\mathbb{P}^1$) s'identifie ainsi à la compactification minimale de $\mathbb{C}$, c'est-à-dire l'espace topologique $\mathbb{C} \cup \{\infty\}$ dans lequel un sous-ensemble U est ouvert si et seulement si $U \subset \mathbb{C}$ est ouvert ou $\mathbb{C} \setminus U$ est compact.

2 La courbe nodale $Y^2Z = X^2(X + Z)$ est rationnelle

En étudiant les intersections de la courbe projective plane C donnée par l'équation

$$Y^2Z = X^2(X + Z)$$

avec les droites d'équation $aX + bY = 0$ on définit pour tout point $[a : b] \in \mathbb{P}^1$ un point $f([a : b]) \in C$. Cela définit une application polynomiale $f\colon \mathbb{P}^1 \to C$ qui induit une bijection $\mathbb{P}^1 \setminus \{[\pm 1 : 1]\} \to C \setminus \{[0 : 0 : 1]\}$. Pour les points $[\pm 1 : 1] \in \mathbb{P}^1$ on a $f([1 : 1]) = f([-1 : 1]) = [0 : 0 : 1]$ donc C s'identifie à la droite projective $\mathbb{P}^1$ où les 2 points $[1 : 1]$ et $[-1 : 1]$ ont été identifiés.
Notons que le point $[0 : 0 : 1]$ est l'unique point singulier de C.

3 Intersection d'une courbe projective avec une droite

Soit $C \subset \mathbb{P}^2$ une courbe algébrique de degré d, définie par le polynôme homogène $P \in \mathbb{C}[X, Y, Z]$. Si $A = [a_1 : a_2 : a_3]$ et $B = [b_1 : b_2 : b_3] \in \mathbb{P}^2$ sont distincts alors il existe une unique droite projective passant par A et B. Sous forme paramétrée on a

$$D = \{[\lambda a_1 + \mu b_1 : \lambda a_2 + \mu b_2 : \lambda a_3 + \mu b_3] \mid [\lambda, \mu] \in \mathbb{P}^1\}.$$

Cette représentation permet de calculer l'intersection $C \cap D$ comme l'ensemble des solutions $[\lambda_i : \mu_i] \in \mathbb{P}^1$ de l'équation

$$Q(\lambda, \mu) = P(\lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2, \lambda a_3 + \mu b_3) = 0.$$

En effet $Q(\lambda, \mu)$ est un polynôme homogène de degré d en λ, μ. En utilisant la factorisation de $Q(T, 1)$ dans $\mathbb{C}[T]$ on voit que

$$Q(\lambda, \mu) = \prod_i (\mu_i \lambda - \lambda_i \mu)^{m_i}$$

pour des points distincts $[\lambda_i : \mu_i] \in \mathbb{P}^1$ et des exposants $m_i \in \mathbb{N}^*$ avec $\sum_i m_i = d$. Les $[\lambda_i : \mu_i]$ sont exactement les points de $\mathbb{P}^1$ tels que $Q(\lambda_i, \mu_i) = 0$ et les $S_i = [\lambda_i a_1 + \mu_i b_1 : \lambda_i a_2 + \mu_i b_2 : \lambda_i a_3 + \mu_i b_3]$ sont exactement les points de $C \cap D$. On définit la *multiplicité d'intersection en* S_i comme étant l'exposant m_i.
Cette discussion montre que le nombre de points de $C \cap D$, comptés avec leurs multiplicités, est égal à d.

4 La tangente à C en $A \in C$

Si $P(X, Y, Z) = X^a Y^b Z^c$ est un monôme, on vérifie immédiatement que

$$X\partial_X P + Y\partial_Y P + Z\partial_Z P = (a + b + c)P.$$

Cela implique que si $P \in \mathbb{C}[X, Y, Z]$ est homogène de degrée d, alors

$$X\partial_X P + Y\partial_Y P + Z\partial_Z P = dP.$$

Soit $C \subset \mathbb{P}^2$ la courbe définie par un polynôme homogène P de degrée d alors il résulte que pour tout point $A = [a : b : c] \in C$ on a

$$a\partial_X P(A) + b\partial_Y P(A) + c\partial_Z P(A) = dP(A) = 0$$

donc si A est un point non singulier alors A appartient à la tangente à C en A.
Ceci démontre aussi que $A = [x : y : 1]$ est un point non singulier si et seulement si les dérivées partielles par rapport à x et y du polynôme $P(x, y, 1)$ sont non-nulles en (x, y).
On vérifie enfin que si D est la tangente à C en A alors la multiplicité d'intersection en A est toujours ≥ 2.

5 Une courbe elliptique n'est pas rationnelle

On indique ici une démonstration algébrique du fait que la courbe projective (plane) donnée par l'équation

$$Y^2 Z = X(X - Z)(X + Z)$$

n'est pas rationnelle. Il suffit de montrer que le corps des fonctions de la courbe affine $y^2 = x(x - 1)(x + 1)$ n'est pas isomorphe à un sous corps du corps des

fractions rationnelles $\mathbb{C}(T)$. Pour cela, il suffit de montrer qu'il n'existe pas de fractions rationnelles $f(T), g(T)$ telles que $g(T)^2 = f(T)(f(T)-1)(f(T)+1)$.
Supposons qu'on peut trouver de telles f, g. En chassant les dénominateurs, on trouve des polynômes P, Q et $R, S \in \mathbb{C}[T]$ avec P, Q resp. R, S premiers entre eux et

$$R(T)^2 Q(T)^3 = S(T)^2 P(T)(P(T) - Q(T))(P(T) + Q(T)).$$

Comme $\mathbb{C}[T]$ est factoriel, cela donne $Q(T)^3 = S(T)^2$ et ensuite le fait que $P, Q, P+Q, P-Q$ sont tous des carrés.
Il s'agit maintenant de prouver qu'il n'existe pas de polynômes non-constants avec cette propriété. En raisonnant par contraposé, soient P et Q de tels polynômes pour lesquels $\deg P + \deg Q$ est minimal. En écrivant $P = P_1^2$ et $Q = Q_1^2$ on déduit que $P_1 \pm Q_1$ et $P_1 \pm iQ_1$ sont des carrés aussi et on retrouve deux carrés $(1+i)(P_1 + Q_1)$ et $(1-i)(P_1 - Q_1)$ dans $\mathbb{C}[T]$ de degrés inférieurs dont somme et différence sont encore des carrés.
L'argument se généralise au cas général de la courbe d'équation

$$Y^2 Z = X(X - Z)(X - \lambda Z).$$

6 Fonctions holomorphes et méromorphes sur $\mathbb{P}^1$

En utilisant le théorème de Liouville on montre que toute fonction holomorphe sur $\mathbb{P}^1$ est constante.
Il est à peine plus difficile à prouver que le corps (!) des fonctions méromorphes sur $\mathbb{P}^1$ est isomorphe au corps des fractions rationnelles $\mathbb{C}(z)$.

7 Les 9 points d'inflexion d'une courbe elliptique

Soit $C \subset \mathbb{P}^2$ une courbe elliptique. L'ordre d'un point $A \in C$ divise 3 si et seulement si la multiplicité d'intersection de C avec sa tangente en A vaut 3. Les points d'ordre divisant 3 sont donc exactement les *points d'inflexion* de C. Comme le groupe des points d'ordre divisant 3 est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$ il y a exactement 9 points d'inflexion.
Par ailleurs, les points d'inflexion de la courbe (supposé non singulière) d'équation projective homogène $P(X, Y, Z) = 0$ sont les points de C où le *Hessien* H de P

s'annule. Ici H est le polynôme

$$H = \begin{vmatrix} \partial_{xx}P & \partial_{xy}P & \partial_{xz}P \\ \partial_{yx}P & \partial_{yy}P & \partial_{yz}P \\ \partial_{zx}P & \partial_{zy}P & \partial_{zz}P \end{vmatrix}.$$

Si P est homogène de degré 3, alors H aussi est homogène de degré 3 et on peut s'attendre à trouver 9 d'intersection (comptés avec multiplicités). Dans ce cas, on voit que tous ces points d'intersection ont multiplicité 1.
La somme de deux points distincts de C d'ordre divisant 3 est encore un point d'ordre divisant 3, différent des deux premiers. Cela implique que toute droite passant par deux points d'inflexion distincts de C coupe C en un troisième point d'inflexion.

8 Toute cubique projective plane non singulière admet une équation sous forme de Weierstraß

Soit $P \in \mathbb{C}[X, Y, Z]$ un polynôme homogène de degré 3. On suppose que la courbe définie par P est non singulière. On résume les différentes étapes de la procédure pour trouver un changement de coordonnées pour mettre P sous forme de Weierstraß

$$Y^2Z - X(X-1)(X-\lambda).$$

La première étape est de trouver un point d'inflexion : un point $A \in \mathbb{P}^2$ tel que $P(A) = H(A) = 0$, voir **7**. Notons d'abord que P et H sont non constants (en fait, tous deux homogènes de degré 3). S'il existe un point d'inflexion avec $Z = 0$ il n'a plus rien à montrer, sinon il faut prouver qu'il existe $(a, b) \in \mathbb{C}^2$ tel que $P(a, b, 1) = H(a, b, 1) = 0$. On cherche donc un $a \in \mathbb{C}$ tel que $P(a, Y, 1)$ et $H(a, Y, 1)$ ont une racine $Y = b$ commune. On prouve l'existence d'un tel a (et on peut le déterminer explicitement) en utilisant le résultant de $P(X, Y, 1)$ et $H(X, Y, 1)$, en tant que polynômes en Y.
Si A est un point d'inflexion, on effectue un changement de coordonnées pour que $A = [0 : 1 : 0]$ et que la tangente à C en A est la droite $Z = 0$. L'équation de C prend alors la forme

$$YZL(X, Y, Z) = Q(X, Z)$$

avec L homogène de degré 1 et Q homogène de degré 3. Comme C est non singulière, le coefficient de Y dans L est non nul et on se ramène (en replaçant Y par une combinaison linéaire de X, Y, Z) à une équation de la forme

$$Y^2Z = Q(X, Z)$$

avec Q homogène de degré 3.
Comme C est non singulière, les racines de $Q(X, 1)$ sont distinctes. Un dernier changement de coordonnées (en X, Z) assure que $Q(X, 1) = X(X - 1)(X - \lambda)$ avec $\lambda \in \mathbb{C}$ différent de $0, 1$.

9 Propriétés des fonctions elliptiques

On fixe un réseau $\Lambda \subset \mathbb{C}$ et une base (ω_1, ω_2) de Λ. On note $\mathcal{E}(\Lambda)$ le corps des fonctions elliptiques par rapport à Λ et $\wp(z) \in \mathcal{E}(\Lambda)$ la fonction de Weierstraß. Soit

$$\Pi = \{x\omega_1 + y\omega_2 \mid x, y \in [0, 1]\}$$

un *parallélogramme fondamental* de Λ. L'ensemble Π a la propriété que $\Pi \to \mathbb{C}/\Lambda$ est surjective et $\mathring{\Pi} \to \mathbb{C}/\Lambda$ est injective, c'est-à-dire que Π contient un représentant de toute classe de $\mathbb{C}/\Lambda$ et pour les classes des éléments de $\mathring{\Pi}$ ce représentant est unique.
Soit $f \in \mathcal{E}(\Lambda)$ non nulle. Comme les zéros et les pôles de f sont isolés et Π est compact, f n'admet qu'un nombre fini de zéros et de pôles sur Π. Avec la périodicite de f, il en résulte qu'il existe $\alpha \in \mathbb{C}$ tel que f n'a ni zéros ni pôles sur le bord du parallélogramme translaté $\alpha + \Pi$. Comme les intégrales de f sur les segments $t \mapsto \alpha + t\omega_i$ et $t \mapsto \alpha + \omega_j + t\omega_i$ (pour $t \in [0, 1]$) coïncident, l'intégrale de f sur le bord de $\alpha + \Pi$, parcouru dans le sens positif, est nulle.
Si $f \in \mathcal{E}(\Lambda)$ est non constante alors cela implique que l'intégrale de f'/f sur le bord de $\alpha + \Pi$ est nulle et que le nombre de pôles de f (comptés avec multiplicités) dans l'intérieur de $\alpha + \Pi$ est égal au nombre de zéros de f (comptés avec multiplicités) sur cet ensemble. La fonction sur $\mathbb{C}/\Lambda$ définie par f a donc également le même nombre de zéros et de pôles (comptés avec multiplicités).
Comme $\wp$ et $\wp'$ ont des pôles d'ordre 2 resp. 3 dans les points de Λ et pas d'autres pôles, on en déduit que ces fonctions on 2 resp. 3 zéros sur $\mathbb{C}/\Lambda$ (comptés avec multiplicités). Le fait que $\wp'$ est Λ-périodique et impaire implique par ailleurs que

$\wp'(\lambda/2) = 0$ pour tout $\lambda \in \Lambda$ et on en déduit que $\wp'$ a 3 zéros simples sur $\mathbb{C}/\Lambda$, en $\overline{\omega_1/2}$, en $\overline{\omega_2/2}$ et en $\overline{(\omega_1+\omega_2)/2}$.
On sait qu'il existe un polynôme $P \in \mathbb{C}[T]$ de degré 3 tel que $\wp'(z)^2 = P(\wp(z))$ pour tout $z \in \mathbb{C}$. Écrivons $P(T) = a(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ avec a et les α_i dans $\mathbb{C}$. Comme $\wp'(\omega_1/2) = 0$, il y a un α_i, disons α_1, tel que $\wp(\omega_1/2) - \alpha_1 = 0$. Comme $\wp'(z)$ a une zéro simple en $\omega_1/2$, la fonction $\wp(z) - \alpha_1$ a un zéro de multiplicité 2 en ce point et comme $\wp'(z)^2 = P(\wp(z))$ a également un zéro de multiplicité 2 en $\omega_1/2$, il résulte que $\alpha_2, \alpha_3 \neq \alpha_1$. On voit aussi que $\wp(z) - \alpha_1$ n'a pas d'autres zéros sur $\mathbb{C}/\Lambda$, en particulier $\wp(\omega_2/2) - \alpha_1 \neq 0$. En répétant l'argument précédent pour les valeurs en $\omega_2/2$ on en déduit que $\alpha_2 \neq \alpha_3$ et que, en échangeant α_2 et α_3 si nécessaire, $\wp(z) - \alpha_2$ a une zéro double en $\omega_2/2$ et $\wp(z) - \alpha_2$ a une zéro double en $(\omega_1+\omega_2)/2$. Les racines de P sont donc distinctes.

10 L'injectivité de $\mathbb{C}/\Lambda \to \mathbb{P}^2$ donnée par $[\wp : \wp' : 1]$

On conserve les notations de **9**. On a vu que l'image de l'application

$$\begin{aligned} \varphi \colon C = \mathbb{C}/\Lambda &\to \mathbb{P}^2 \\ z &\mapsto [\wp(z) : \wp'(z) : 1] \end{aligned}$$

est égale à la courbe C' d'équation

$$Y^2Z = a(X - \alpha_1 Z)(X - \alpha_2 Z)(X - \alpha_3 Z).$$

Les résultats de **9** permettent de voir que φ est injective.
D'abord on remarque que $\overline{0} \in C$ est l'unique point dont l'image est de la forme $[x : y : 0] \in \mathbb{P}^2$, en fait $\varphi(\overline{0}) = [0 : 1 : 0]$. La discussion en **9** a montré que C contient exactement 3 points dont l'image est de la forme $[x : 0 : 1] \in \mathbb{P}^2$, ce sont les points $\overline{\omega_1/2}$, $\overline{\omega_2/2}$ et $\overline{(\omega_1+\omega_2)/2}$ dont les images (distinctes) sont $[\alpha_1 : 0 : 1]$, $[\alpha_2 : 0 : 1]$ et $[\alpha_3 : 0 : 1]$ respectivement.
Soit finalement fixé $x \in \mathbb{C}$ avec $x \neq \alpha_i$ pour $i = 1, 2, 3$. Alors C' contient exactement deux points de la forme $[x : y : 1]$ (pour deux valeurs opposées de y). La surjectivité de φ implique alors qu'il existe deux points $z_1, z_2 \in C$ avec $\wp(z_1) = x$ et $\wp'(z_1) = -\wp'(z_2) \neq 0$. On a trouvé deux racines simples de $\wp(z) - x$ et comme il n'y a pas d'autres racines il n'existe pas d'autre point $z_3 \in C$ avec $\varphi(z_3)$ de la forme $[x : y : 1]$ pour notre valeur fixé de x. L'injectivité de φ s'en déduit.

11 Intégrales elliptiques

On fixe la courbe elliptique $C \subset \mathbb{P}^2$ avec équation

$$Y^2Z = X(X-Z)(X-\lambda Z)$$

avec $\lambda \neq 0, 1$ et on note également C la surface de Riemann associée. On note $x = X/Z$ et $y = Y/Z$, ce sont des fonctions méromorphes sur C. L'expression $\omega = \frac{\mathrm{d}x}{y}$ est une *forme différentielle méromorphe* sur C, ce qui est à dire que sur tout ouvert $U \subset C$ où on dispose d'une paramétrisation avec coordonnée z, les fonctions x, y s'expriment comme fonctions méromorphes de z donc

$$\frac{\mathrm{d}x}{y} = \frac{x'(z)}{y(z)}\mathrm{d}z = f_U(z)\mathrm{d}z,$$

où $f_U(z) = \frac{x'(z)}{y(z)}$ est encore une fonction méromorphe de z. On vérifie que, sur tout ouvert U et pour toute expression comme ci-dessus, la fonction f_U est en fait holomorphe et que ω est donc forme différentielle holomorphe sur C.
Pour tout chemin $\gamma\colon [0,1] \to C$ de classe $\mathcal{C}^1$ on définit l'intégrale de ω le long de γ comme étant

$$\int_\gamma \omega = \int_\gamma \frac{\mathrm{d}x}{y} = \int_0^1 \frac{x(\gamma(t))'}{y(\gamma(t))}\mathrm{d}t.$$

Ici $x(\gamma(t))$ et $y(\gamma(t))$ sont les composés des fonctions x et y avec γ et la dérivée $x(\gamma(t))'$ est la dérivée par rapport à t. Cette définition s'étend de manière évidente aux chemins qui sont seulement de classe $\mathcal{C}^1$ par morceaux.
Notons que si $V \subset \mathbb{C}$ est un ouvert où on peut choisir une détermination de la fonction $\sqrt{x(x-1)(x-\lambda)}$, alors V s'identifie avec un ouvert $U \subset C$. Tout chemin γ dans U s'identifie donc avec un chemin dans V et l'intégrale qu'on vient de définir coïncide avec l'intégrale

$$\int_\gamma \frac{x}{\sqrt{x(x-1)(x-\lambda)}}\mathrm{d}x$$

vue en analyse complexe.
Comme pour les intégrales curvilignes dans $\mathbb{C}$, on montre que $\int_\gamma \omega$ ne dépend que de la classe d'homotopie de γ. L'application qui envoie un *lacet* γ sur $\int_\gamma \omega \in \mathbb{C}$ définit donc une application du groupe fondamental $\pi_1(C)$ vers $\mathbb{C}$. Il n'est pas difficile à voir que c'est un morphisme de groupes (pour le groupe additif de $\mathbb{C}$).

Comme C est (topologiquement) un tore, donc homéomorphe à $S^1 \times S^1$, on a $\pi_1(C) \cong \mathbb{Z} \times \mathbb{Z}$ et on peut montrer que l'image de $\pi_1(C)$ dans $\mathbb{C}$ est un réseau Λ. Si on fixe un point de base $A_0 \in C$, alors pour tout $A \in C$ on peut choisir un chemin γ de A_0 vers A. L'intégrale $\int_\gamma \omega$ dépend du choix de γ, mais si γ_1 est un autre chemin de A_0 vers A alors γ et γ_1 diffèrent, à homotopie près, d'un élément de $\pi_1(C)$. Cela implique que *à un élément de* Λ *près* $\int_\gamma \omega$ est indépendante du choix de γ. On définit ainsi une application $\psi\colon C \to \mathbb{C}/\Lambda$ dont on peut montrer (mais ce n'est pas facile !) que c'est un isomorphisme de surfaces de Riemann.

Références

[Cle03] C. H. Clemens. *A scrapbook of complex curve theory*, Graduate Studies in Mathematics 55. American Mathematical Society, second edition, 2003.

[Kir92] F. Kirwan. *Complex algebraic curves*, London Mathematical Society Student Texts 23. Cambridge University Press, 1992.

[Kob93] N. Koblitz. *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics 97. Springer-Verlag, second edition, 1993.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106. Springer-Verlag, 1986.