Les courbes elliptiques pour les nuls

Guillaume Lafon

16 janvier 2003

Table des matières

Introduction

Ce texte est destiné à tous ceux qui ont fait une recherche Google sur les mots "courbe elliptique" et ont sélectionné ma page parmi les quelque 3000 réponses données, à ceux qui ont décidé de comprendre la démonstration du théorème de Fermat et ont constaté qu'il y avait un vague rapport avec les courbes elliptiques, à ceux qui ont envie de pouvoir répondre autre chose que "Ben euh..." la prochaine fois qu'ils compareront les douces formes de leur dulcinée à des courbes elliptiques (quelle drôle d'idée, aussi) et qu'elle répondra "Mais c'est quoi, une courbe elliptique ?"...

Enfin bref, je m'égare, a priori, je pense qu'il intéressera surtout les gens qui ont une certaine curiosité vis-à-vis de ce domaine des mathématiques mais n'ont pas l'envie/le temps/le courage de lire un bouquin de 500 pages compliqué et trouveront peut-être ici un aperçu plus accessible. En effet, ce texte étant à l'origine censé remplacer un (ou plutôt plusieurs) exposés sur le sujet destinés à un ami physicien (d'où le titre de la chose ;-)) et néanmoins désireux d'enrichir sa culture mathématique, il ne comporte pour ainsi dire pas de démonstrations (mais par contre des explications pour mieux cerner

les phénomènes observés) et le style en est un sûrement plus libre que celui de la littérature mathématique standard (et plus bavard, oui, je sais).

Si vous avez déjà ouvert un livre sur les courbes elliptiques, vous aurez sûrement eu droit à une remarque concernant la vaste domaine d'application des dites courbes. Je ne dérogerai pas à la règle : les courbes elliptiques, ça s'utilise aussi bien en analyse qu'en algèbre ou en arithmétique, et ça fait une partie de leur intérêt. Je traiterai les différents points de vue successivement, en commençant par les courbes elliptiques complexes parce que c'est plus facile (ce sera la partie la plus analytique), puis le cas général parce que c'est plus joli (là, il y aura plus d'algèbre). Pour ce qui est du contenu, je pense que la table des matières le résume très bien, rentrons donc tout de suite dans le vif du sujet.

1 Courbes elliptiques complexes

Une courbe elliptique est, en gros, une courbe (enfin, quelque chose de dimension 1, donc ca ressemble plutôt à une surface dans le cas complexe, en fait), munie d'une loi de groupe. Pas n'importe quelle loi de groupe, évidemment, sinon ce serait facile mais ça n'aurait aucun intérêt, mais une loi telle que les cooordonnées de la somme s'exprime "gentiment" en fonction de celles des points de départ, par exemple de façon polynômiale (poue employer des termes plus savants, l'idée est de munir la courbe d'une structure de *schéma en groupes*).

Par exemple, le cercle réel $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ est muni d'une loi de groupe naturelle (pour laquelle il est isomorphe à $\mathbb{R}/2\pi\mathbb{Z}$) via sa paramétrisation par l'angle : $(\cos\theta, \sin\theta) + (\cos\theta', \sin\theta') = (\cos(\theta + \theta'), \sin(\theta + \theta'))$ On peut d'ailleurs faire pareil avec le cercle complexe et via les relations trigonométriques, on a bien une loi polynômiale : $(x_1, y_1) + (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$.

Dans le cadre complexe, comme souvent, tout est simple. En fait, les courbes elliptiques y ont le bon goût d'être de simples tores (à isomorphisme près pour une bonne notion d'isomorphisme, bien entendu). C'est d'ailleurs la définition provisoire que j'en donnerai ; pour rompre avec la tradition consistant à en donner une équation tout de suite, nous allons étudier les tores et, en extrayant les propriétés intéressantes de cette étude, proposer une généralisation du concept.

1.1 Tores et fonctions elliptiques

Rappelons pour commencer les propriétés élémentaires des réseaux dans $\mathbb{R}^2$:

Proposition 1. *Un sous-groupe discret maximal (ou* réseau*) de* $\mathbb{C}$ *est de la forme* $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$*, où* $\frac{\omega_2}{\omega_1} \notin i\mathbb{R}$.

Definition 1. *Un* tore complexe *est un quotient* $\mathbb{C}/\Lambda$*, où* Λ *est un réseau.*

Definition 2. *Deux réseaux (ou les tores correspondants)* L *et* L' *sont dits* équivalents *s'il existe un nombre complexe* λ *tel que* $\lambda L = L'$*. On dit que* λ *réalise une* isogénie *entre les deux réseaux si* $\lambda L \subset L'$*, on appelle* degré de l'isogénie *l'indice de* λL *comme sous-groupe de* L'

Exemple La multiplication par n est une isogénie de L dans lui-même (quel que soit le réseau L) de degré n^2.

Remarques 1) $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ et $L' = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$ sont équivalents $\Leftrightarrow$ $\exists M \in SL_2(\mathbb{Z})$ telle que $M\omega_1 = omega_1'$ et $M\omega_2'$.

2) La "bonne" définition d'un tore fait en fait intervenir sa structure de variété analytique. Les isogénies s'interprètent alors comme des morphismes entre variétés analytiques.

Le but va maintenant être de trouver une courbe elliptique isomorphe à notre tore mais qui puisse être définie par une équation polynômiale, pour pouvoir ensuite généraliser à un corps quelconque. On va maintenant introduire l'élément essentiel de la théorie, à savoir les fonctions elliptiques, qui sont à l'origine de la théorie des courbe elliptique :

Definition 3. *Une* fonction elliptique *sur un réseau* L *est une fonction* f *méromorphe sur* $\mathbb{C}$ *et* L*-périodique (ie* $\forall \omega \in L, f(z+\omega) = f(z)$*).*

Remarque Une fonction elliptique holomorphe est constante, puisque bornée.

On va maintenant énoncer une propriété fondamentale des fonctions elliptiques. Commençons par introduire une nouvelle notion :

Definition 4. *Le* parallélogramme fondamental *du réseau* $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *est celui dont les sommets sont* $0, \omega_1, \omega_2, \omega_1 + \omega_2$.

On définit l'ordre d'une fonction elliptique f en un point a, comme d'habitude, comme étant l'entier n, noté $ord_a(f)$ tel que $f(z) = (z-a)g(z)$ au voisinage de a, avec g holomorphe non nulle en a.

Theoreme 1. *Soit f une fonction elliptique sans zéros ni pôles sur le bord du parallélogramme fondamental P alors*

$$\sum_{a\in P} ord_a(f) = 0, \quad \sum_{a\in P} a.ord_a(f) \in L.$$

Démonstration. C'est élémentaire, il s'agit d'appliquer le théorème des résidus à de bonnes fonctions. Le lecteur curieux mais flemmard (non, non, ce n'est pas du tout incompatible) pourra par exemple regarder [MKM] pour plus de détails, comme pour la plupart des énoncés de cette section. □

On verra un peu plus loin en quoi cette dernière propriété est intéressante. Pour l'instant, on va essayer d'en savoir plus sur ces fonctions elliptiques. En fait, et c'est bien leur intérêt, on peut en obtenir facilement la liste. Pour ce faire, on va introduire une fonction particulière, qui mérite bien un paragraphe à elle seule au vu de sa place centrale dans la théorie.

1.2 La fonction $\mathcal{P}$ de Weierstrass

Le but est donc d'avoir une fonction periodique suivant un réseau L. On sait déjà qu'on ne pourra pas trouver de fonction holomorphe, on va donc tenter le coup avec un fonction méromorphe qui ait un pôle en chaque point du réseau (mais aucun aillleurs, pas besoin de foutre le bordel sans raison). Le pôle devra être "le même", bien sûr, pour que la fonction soit périodique, donc on a envie de prendre une somme de choses du genre $\frac{1}{(z-\omega)^n}$ pour ω parcourant le réseau, n étant l'ordre du pôle en chaque point du réseau. Et là, miracle, ça marche très bien, on constate qu'il suffit d'avoir $n \geqslant 2$ pour que la série converge (exercice laissé au lecteur).

Definition 5. *La* fonction $\mathcal{P}$ *associée au réseau* L *est* $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$.

Remarque 1) La dérivée de $\mathcal{P}$ est aussi une fonction elliptique (les dérivées suivantes aussi, mais on s'en fout, vous allez comprendre pourquoi rapidement).

2) En posant $G_{2k}(L) = \sum_{\omega\in L\setminus\{0\}} \frac{1}{\omega^{2k}}$, on a des développements en séries $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$ et $\mathcal{P}'(z) = \frac{-2}{z^3} + \sum_{k=1}^{\infty}(2k+1)2kG_{2k+2}z^{2k}$.

On a maintenant les deux résultats fopndamentaux suivants, le premier nous dit qu'en fait,les fonctions $\mathcal{P}$ et $\mathcal{P}'$ sont plus ou moins les seules fonctions elliptiques, la seconde va faire apparaitre, comme par miracle, la belle équation qu'on veut pour notre courbe.

Theoreme 2. *Toute fonction elliptique sur un réseau L s'écrit comme fraction rationelle en $\mathcal{P}(L)$ et $\mathcal{P}(L)'$*

Démonstration. Déjà, en constatant que $\mathcal{P}$ est paire est $\mathcal{P}'$ impaire, on se ramène aucas d'une fonction paire. Elle ne peut dont avoir de pôles qu'en $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ (modulo L), mais alors quitte à la multiplier par des bonnes puissances de $\mathcal{P}$, $\mathcal{P} - \mathcal{P}(\omega_1)$, etc..., on va obtenir une fonction elliptique holomorphe donc constante, et on en déduit le résultat. □

Grâce au théorème précédent, on voit que $\mathcal{P}$ et $\mathcal{P}'$ sont reliés parune équation fonctionnelle (on peut exprimer $\mathcal{P}'$ rationellement en fonction de $\mathcal{P}$ et $\mathcal{P}'$). On a en fait beaucoup mieux :

Theoreme 3. *La fonction $\mathcal{P}'$ satisfait l'équation différentielle suivante : $(\mathcal{P}')^2 = 4\mathcal{P}^3 - g_2\mathcal{P} - g_3$, où $g_2 = 60G_4$ et $g_3 = 140G_6$.*

Démonstration. Le principe est tout simple : on part des développements de Laurent et on constate que la différence des deux membres de l'équation est holomorphe (on a pris juste les coefficients qu'il faut pour quele pôle en 0 disparaisse) donc constante car périodique, et il ne reste qu'à calculer sa valeur en 0 ... □

On a donc un morphisme naturel de notre tore vers la courbe $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$, où $e_1 = \mathcal{P}(\omega_1)$, $e_2 = \mathcal{P}(\omega_2$ et $e_3 = \mathcal{P}(\omega_1+\omega_2)$ (on obtient ces valeurs pour les racines du polynôme intervenant dans l'équation différentielle par un bête calcul) : $z \to (\mathcal{P}(z), \mathcal{P}'(z)$. Bon, il y a un petit problème en zéro, c'est pas grave, on considère que son image par cette fonction est unpoint "à l'infini". Et là se produit le miracle auquel on n'ose même pas croire, cette application est en fait bijective ! D'où la belle équation dont on rêvait depuis le début...

Theoreme 4. *L'application (dite* d'Abel-Jacobi*) de E dans $\mathbb{C}/L$ définie par $P \to \int_O^P \frac{dx}{2y}(modL)$ est bijective réciproque de celle qu'on vient d'introduire (O étant le point à l'infini).*

Démonstration. Ce point est certainement le plus délicat (normal, c'est le point essentiel) donc on ne va pas trop s'attarder dessus. En fait, les méthodes efficaces utilisent une peu de géométrie analytique, il faut constater que les deux applications sont des morphismes entre surfaces de Riemann, et en remarquant qu'elles sont de degré 1, on obtient le résultat. □

Si on reprend l'exemple du cercle, on obtient comme équivalent de l'application d'Abel-Jacobi $P \to \int_O^P \frac{dx}{\sqrt{1-x^2}}$ (ici, O est le point $(0,1)$) qui envoie

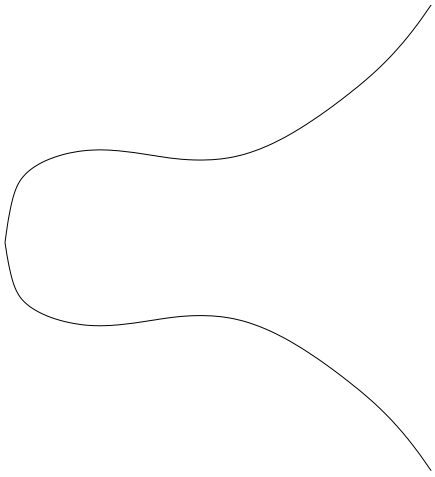
le cercle bijectement sur le cylindre $\frac{\mathbb{C}}{2\pi\mathbb{Z}}$ (qui n'est pas un tore, mais attention,on n'est pas dans le cadre des courbes elliptiques , le cercle est donné par une équation de degré 2 et non de degré 3).

On voit donc que le tore associé à une courbe n'est que l'ensemble des valeurs des intégrales d'une différentielle bien choisie sur cette courbe, et que le réseau définissant le tore est l'ensemble des valeurs des intégrales de cette même forme sur des chemins fermés (qui n'ont aucune raison d'être nuls, et qu'on appelle souvent les *périodes* de la courbe).

Remarque On peut obtenir une description explicite de la loi de groupe sur la courbe sans passer par le tore ; il suffit pour celà de trouver des formules d'addition pour $\mathcal{P}$, ie exprimer $\mathcal{P}(z+z')$ et $\mathcal{P}'(z+z')$ rationellement en fonction de $\mathcal{P}(z)$, $\mathcal{P}(z')$, $\mathcal{P}'(z)$ et $\mathcal{P}'(z')$, on obtient par exemple $\mathcal{P}(z+z') = \frac{1}{4}(\frac{\mathcal{P}'(z')-\mathcal{P}'(z)}{\mathcal{P}(z')-\mathcal{P}(z)})^2 - \mathcal{P}(z) - \mathcal{P}(z')$.

1.3 Mais, m'sieur, qu'est-ce qu'elles ont d'elliptique, ces courbes ?

Effectivement, les plus attentifs d'entre vous auront remarqué que les équations qu'on obtient sont de degré 3 et les courbes ne sont pas bornées (on a même un point à l'infini, c'est dire, mais bon, ceci dit, avec un petit changement de variable bien choisi, on peut le ramener à peu près où on veut), ça ne ressemble pas du tout à une ellipse, mais plutôt à ça (ce qui suit est un vague cousin du graphe de la courbe elliptique "standard" $y^2 = x^3 - x$)



Alors, pourquoi diable les avoir appelées comme ça, ces courbes ? Ben il y a une bonne raison, c'est qu'historiquement elles sont apparues pour la première fois lors de calculs de périmètres, et en particulier de celui d'ellipses.

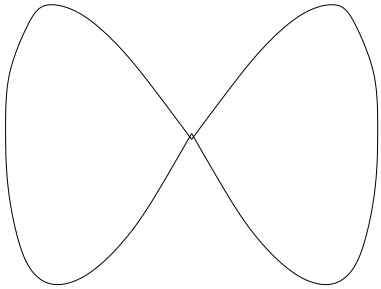
Prenons donc une bonne vieille ellipse, d'équation $x^2 + \frac{y^2}{b^2} = 1$ (oui, je sais, il y a un a^2 sous le x^2 pour l'équation générale, mais bon, là, on peut normaliser en x), on peut paramétrer par $x = \cos\theta$, $y = b\sin\theta$, la longueur d'arc s vérifie $(ds)^2 = (1-k^2\cos^2\theta)(d\theta)^2$ (où $k = 1-b^2$), d'où après un rapide calcul $s = \int \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}$. C'est ce qu'on appelle une intégrale elliptique du premier ordre (là, au moins, on voit d'où vient le nom). Plus généralement :

Definition 6. *On appelle* intégrale elliptique (resp. hyperelliptique) *une intégrale du type* $\int R(x, \sqrt{f(x)})$ *où* R *est une fonction rationelle et* f *un polynôme de degré* 3 *(resp.* 4*).*

Un tel machin n'est pas très loin de ressembler à une intégrale de différentielle donnant une bijection entre courbe elliptique et tore. En fait, il suffit de vérifier que les valeurs de l'intégrale forment un parallélogramme dans $\mathbb{C}$ et on aura de fait un isomorphisme avec une courbe elliptique via le tore défini par le réseau des périodes de l'intégrale ! C'est beau, non ? Comment ça, vous avez rien compris ? Bon, on va regarder ça sur un autre exemple, plus intéressant, celui de la lemniscate (en plus, historiquement, c'est Gauss qui l'a étudié, donc ça ne peut pas être mal).

Definition 7. *La* lemniscate *définie par les points* F_1 *et* F_2 *(dans* k^2*, où* k *est un corps gentil, ici ce sera* $\mathbb{C}$*) est l'ensemble des points* P *vérifiant* $\|F_1P\|.\|F_2P\| = \|F_1O\|.\|F_2O\|$*, où* O *est le milieu de* $[F_1f_2]$*.*

Ca ressemble à ça :



Pour un bon choix des points (que je vous laisse deviner, faut bien que vous bossiez un peu aussi), on obtient la belle équation suivante en polaires : $r^2 = \cos(2\theta)$. Un petit calcul (il ressemble à celui de l'ellipse) nous donne la longueur d'arc de la lemniscate : ça vaut $\int \frac{dr}{\sqrt{1-r^4}}$. Evidemment, ça ne se calcule pas bien, mais introduisons donc la fonction réciproque sl (pour sinus lemniscatique, parce que ça ressemble à du sinus, on a juste changé le carré qui est dans la racine du dénominateur dans l'intégrale par une puissance 4). On a donc $sl(s) = r$ si $s = \int_0^r \frac{dt}{\sqrt{1-t^4}}$. On sait que, pour un certain Ω (la

longueur de la demi-courbe), on a $sl(\Omega) = 0$. Au passage, on $sl\frac{Omega}{2} = 1$, mais ça ne nous intéresse pas tellement. Par contre, on voit facilement que sl est impaire et surtout doublement périodique de périodes 2Ω et $2i\Omega$. On peut donc la voir comme fonction elliptique sur le réseau $2\Omega\mathbb{Z} + 2i\Omega\mathbb{Z}$ et en déduire une structure de courbe elliptique sur la lemniscate... Maintenant, cette structure nous donne desinformations supplémentaires ; en particulier, grâce à la loi de groupe, on a une formule de doublement pour sl, due à l'origine à Fagnano (et montrée par des methodes élémentaires) : $sl(s_1+s_2) = \frac{sl(s_1)\sqrt{1-sl^4(s_2)}+sl(s_2)\sqrt{1-sl^4(s_1)}}{1+sl^2(s_1)sl^2(s_2)}$. Plusieurs formules similaires ont été montrées avant que l'on ne comprenne ce qui se cachait dessous, à savoir la merveilleuse théorie des courbes elliptiques . Citons par exemple la formule d'Euler, qui est une généralisation de la précédente, et qu'Euler a démontrée par un calcul astucieux :

Proposition 2. *Si* $f(t) = 1 + mt^2 + nt^4$, *on* $\int_0^w \frac{dt}{f(t)} = \int_0^u \frac{dt}{f(t)} + \int_0^v \frac{dt}{f(t)}$, *où* $w = \frac{u\sqrt{f(v)}+v\sqrt{f(u)}}{1-nu^2v^2}$.

Essayons d'exprimer tout ceci plus joliment et de façon plus générale. On va d'abord donner la définition d'un objet utile, le groupe de diviseurs d'une courbe :

Definition 8. *Un* diviseur *sur une courbe X est une somme finie formelle de points de la courbe $D = \sum_{i=1}^k n_i P_i$, $P_i \in X$ (attention, ça n'a rien à voir avec la loi de groupe sur une courbe elliptique , ces sommes formelles sont définies pour n'importe quelle courbe), les n_i sont des entiers. Le* degré *de D est juste la somme des entiers n_i. On munit l'ensemble des diviseurs de la loi de groupe naturelle et on note $Div(X)$ le groupe ainsi obtenu (qui est donc le groupe libre engendré par les points de la courbe). On appelle degré de*

Un diviseur en soi n'est pas quelque chose d'extraordinairement compliqué, leur intérêt réside surtout dans le fait qu'on peut associer à une fonction méromorphe sur un courbe un diviseur :

Definition 9. *Le* diviseur associé *à la fonction méromorphe f sur la courbe X est $D(f) = \sum_{P\in X} ord_P(f)P$. Un diviseur associé à une fonction méromorphe est dit* principal. *Le sous-groupe de $Div(X)$ formé des diviseurs principaux est noté $Pr(X)$.*

Proposition 3. *Tout diviseur principal est de degré* 0.

Dans le cas qui nous intéresse, ce n'est que la reformulation de la première partie du théorème 1. Là où ça devient beaucoup plus intéressant, c'est que la réciproque du théorème 1 est vraie :

Theoreme 5. *Soient $(n_i)_{1\leqslant i\leqslant k}$ des entiers, P_i des points d'un parallélogramme complexe tels que $\sum_{i=1}^{k} n_i = 0$ et $\sum_{i=1}^{k} n_i P_i = 0$ mod L (L un réseau dans $\mathbb{C}$) alors il existe une fonction elliptique sur le réseau L ayant des d'ordre n_i en P_i (et pas de pôles ailleurs).*

On a donc une interprétation intrinsèque de la loi de groupe sur notre courbe, elle est donnée par l'isomorphisme de groupe $E \to Div^0(X)/Pr(X)$, où $Div^0(X)$ est le groupe des diviseurs de degré 0, lequel isomorphisme est donné par $P \to (P - O)$ (à droite, on a la classe de $P - O$ dans le groupe $Div^0(X)/Pr(X)$, groupe qui est souvent noté $Cl(X)$ (groupe des classes de X)). Ces considérations vont nous guider vers la définition de courbes elliptiques sur des corps quelqconques, que nous allons maintenant aborder avec enthousiasme après cette première section apéritive.

2 Passons aux choses sérieuses

2.1 Quelques définitions

Definition 10. *Une courbe elliptique sur un corps K est l'ensemble des solutions dans K^2 d'une équation cubique $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, où les a_i sont des coefficients dans K (on appelle cette équation* forme normale de Weierstrass *de la courbe).*

Remarques 1) Pourquoi ces équations et pas d'autres ? Elles trouveront leur justification quand je donnerai la "vraie" définition d'une courbe elliptique un peu plus bas.

2) En fait, il faudrait plutôt voir une courbe elliptique comme une courbe projective, donc avec une équation homogénéisée dans $\mathbb{P}_2(K)$ de la forme $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X^2Z + a_6Z^3$ (celà revient à ajouter à la courbe ce fameux "point à l'infini" qu'on a déjà rencontré à la section précédente).

3) Sur un corps de caractéristique différente de 2, on peut compléter le carré dans le membre de gauche pour obtenir la forme plus sympathique $y^2 = f(x)$, où f est un polynôme de degré 3 en x. On peut de même compléter le cube dans le membre de droite en caractéristique différente de 3, et si $car(K) \notin \{2, 3\}$ (en particulier si $K = \mathbb{C}$), on a la forme réduite $y^2 = x^3 + Ax + B$.

On associe quelques invariants à une courbe elliptique, qui trouveront leur intérêt un peu plus tard, sauf en ce qui concerne l'invariant différentiel qui a déjà joué un rôle de premier plan dansla section précédente :

Definition 11. *Le* discrimant *de la courbe elliptique* $y^2 = x^3 + Ax + B$ *est* $\Delta = 4A^3+27B^2$. *Son* invariant absolu *est* $j = \frac{16(A^2+B)}{\Delta}$. *Enfin, la* différentielle invariante *associée à la courbe est* $\omega = \frac{dx}{2y+a_1+a_3}$.

Remarque Dans le cadre complexe, ou même simplement sur corps de caractéristique différente de 2 ou 3, toutes ces définitions se simplifient en utilisant l'équation réduite.

On voudrait maintenant munir notre courbe d'une loi de groupe. pour celà, on fixe un point O sur la courbe, qui sera l'élément neutre de la loi de groupe. Celle-ci est définie comme suit : à deux points P et Q de notre courbe, on associe d'abord le troisième point d'intersection de la droite (PQ) avec notre courbe (respectivement de latangente en P si $Q = P$; ici, il convient de vérifier d'une part que ce troisième point existe bien, et qu'il est bien dans notre corps de base K) qu'on note PQ, puis le troisième point d'intersection de $(O\ PQ)$ avec la courbe, noté $P \oplus Q$, qui sera donc la "somme" de P et Q. Plusieurs questions se posent : d'abord pourquoi avoir choisi cette loi bizarre (et pas prendre simplement PQ comme somme, par exemple) ? Ce sera expliqué dans la section suivante et c'est en fait une loi naturelle quand on comprend ce qu'il y a de caché derrière. On a d'ailleurs le résultat fondamental suivant :

Theoreme 6. *La bijection entre un tore complexe et une courbe elliptique vue au paragraphe précédent est un isomorphisme de groupes (la loi sur le tore étant celle induite par* $\mathbb{C}$ *et celle sur la courbe celle qu'on vient d'introduire.*

Une autre question est de prouver que la loi introduite fait bien de notre courbe un groupe (commutatif qui plus est, on aurait tort de se priver), ce qui n'a rien d'évident ! Le fait que O soit un élément neutre et que $-P$ soit la troisième intersection de (OP) avec la courbe sont à peu près clair (faites un petit dessin si vous n'êtes pas convaincu), la commutativité découle de la symétrie de la construction, mais l'associativité pose problème... En fait, la démonstration est assez technique et repose sur le fait que des systèmes de droites ou de coniques ne peuvent pas intersecter une courbe de degré 3 (comme notre courbe elliptique) en trop de points, l'ingrédient essentiel étant le classique :

Theoreme 7. *(théorème de Bézout) Deux courbes de degré respectif* n *et* m *dans* $\mathbb{P}_2(K)$ *n'ayant pas de composante commune s'intersectent en exactement* nm *points (comptés avec multiplicité)*

Je ne vais pas définir précisément ici ces histoires de multiplicité et de composantes communes, ça signifie en gros que les deux courbes ne contiennet pas de droite commune et que, si les courbes sont tangentes en un point, il

faut le compter plusieurs fois (regarder jusqu'à quel ordre les équations des courbes sont égales en ce point). Je renvoie à [Sil] pour plus de détails et la démonstration complète de l'associativité.

On choisit habituellement le point à l'infini comme neutre, ce qui simplifie les calculs : toute droite verticale coupe la courbe en exactement deux points (plus en fait le point à l'infini) qui sont opposés pour la loi de groupe.