La quartique de Klein

et le groupe simple d'ordre 168

Voir, Penser, Dire, Agir,

Travailler, S'appliquer, Se concentrer, Méditer.

Le chemin des huit vertus vers le Nirvana.

> *Je remercie Pierre Michalak de m'avoir invité à cette journée d'hommage aux mathématiques allemandes. Je suis d'autant plus heureux de parler de Felix Klein qu'il s'agit de l'un des mathématiciens dont je me sens le plus proche, que ce soit par son fameux programme d'Erlangen, ou encore ses travaux sur les géométries non euclidiennes, ou enfin le souci qu'il avait de l'enseignement de sa discipline.*

Introduction

Cet exposé est inspiré[1] de l'article :

Über die Transformationen siebenter Ordnung der elliptischen Funktionen, Math. Ann. **14** *(1879), 428-471. Œuvres, Tome III, p. 90-136.*

Il est conçu comme une promenade dans l'un des plus beaux domaines des mathématiques, avec beaucoup de résultats et peu de démonstrations. Il nous mènera de la géométrie algébrique à la théorie des groupes en passant par la théorie des nombres, la topologie et la géométrie hyperbolique. On y verra, sous de multiples apparences, toutes plus belles les uns que les autres, la fameuse courbe (ou surface) de Klein. Cette courbe est si belle qu'on lui a même érigé une statue, appelée *The eightfold way*, au MSRI (Mathematical Sciences Research Institute) à Berkeley (le titre sera expliqué plus bas). On verra aussi plusieurs équations de cette courbe, très belles aussi, dont la fameuse $X^3Y + Y^3T + T^3X = 0$. On y rencontrera enfin un groupe simple remarquable d'ordre[2] $168 = 2^3 \times 3 \times 7$ (le plus petit groupe simple non trivial

[1] Je ne suivrai pas l'exposé de Klein, préférant une entrée plus élémentaire.

[2] Les nombres $2, 3, 7$ nous poursuivront tout au long de ce périple.

après le groupe alterné $\mathfrak{A}_5$, groupe de l'icosaèdre). Ce groupe a plusieurs habits : $PSL(2, \mathbf{F}_7)$, $PSL(3, \mathbf{F}_2)$, que l'on tentera de comprendre. On essaiera ici d'expliquer une toute petite partie de la théorie, renvoyant le lecteur curieux à la bibliographie, notamment à l'article initial de Klein, au très beau livre : *The eightfold way* édité par Silvio Levy (Cambridge University Press, 1999) à l'occasion de l'inauguration de la statue évoquée ci-dessus, à l'exposé de Christophe Bavard et au livre (épuisé) de Régine et Adrien Douady.

0.1 Rappels

Nous aurons besoin de quelques notions sur les groupes qu'on trouvera par exemple dans [Perrin1].

Soit G un groupe et X un ensemble. Dire que G opère (ou agit) sur X signifie qu'on a une application $(g, x) \mapsto g.x$ de $G \times X$ dans X avec les propriétés usuelles. On dit que le groupe opère transitivement si, pour tous x, y dans X, il existe $g \in G$ tel que $g.x = y$. Si ce n'est pas le cas, on considère les orbites de G dans X : l'orbite $\omega(x)$ est l'ensemble des transformés de x par les éléments de G. Le stabilisateur H_x de $x \in X$ est le sous-groupe formé des $g \in G$ qui fixent x : $g.x = x$. On a une relation entre orbite et stabilisateur : l'ensemble quotient (les classes à gauche) G/H_x est en bijection avec $\omega(x)$ par l'application qui à $\overline{g}$ associe $g.x$. En particulier, et c'est surtout ce point qui nous sera utile, on a $|G| = |H_x| \times |\omega(x)|$.

On rappelle aussi qu'un sous-groupe N d'un groupe G est dit **distingué** s'il est stable par conjugaison : pour tout n dans N et tout g dans G, gng^{-1} est dans N.

1 La quartique de Klein : variante affine réelle

Contrairement à Klein, je commence par l'étude de la variante affine réelle de la quartique de Klein. Ce n'est peut-être pas la plus intéressante, mais c'est sans doute la plus élémentaire.

1.1 La courbe et ses bitangentes

La quartique de Klein est une courbe algébrique K, dont une image réelle est la courbe K_0 de la figure 1. Cette courbe est tracée dans le plan affine réel et elle est inscrite dans un triangle équilatéral dont les sommets sont $1, j, j^2$ (si on identifie $\mathbf{R}^2$ et $\mathbf{C}$). Elle admet d'ailleurs manifestement comme groupe de symétries le groupe $\mathfrak{S}_3$ du triangle équilatéral (trois rotations d'angles $2k\pi/3$ et trois symétries axiales). À l'œil, cette courbe semble être une quartique i.e. une courbe de degré 4 (car une droite la coupe en au plus 4 points), lisse (sans points singuliers : ni points doubles, ni rebroussements). En revanche, certaines tangentes sont particulières. En effet, une tangente ordinaire recoupe la courbe en deux points distincts u, v et un cas particulier est celui des bitangentes (c'est-à-dire le cas $u = v$). Les côtés du triangle équilatéral sont des bitangentes à K. Leurs équations sont $2x+1 = 0$, $-x+\sqrt{3}y+1 = 0$ et $-x-\sqrt{3}y+1 = 0$. Les points de contact étant échangés par le groupe $\mathfrak{S}_3$, ils sont sur un cercle de centre O et de rayon R.

Une équation plausible pour cette courbe est donc :

$$(2x + 1)(-x + \sqrt{3}y + 1)(-x - \sqrt{3}y + 1) - k(x^2 + y^2 - R^2)^2 = 0.$$

En effet, une telle équation est invariante par $\mathfrak{S}_3$ (car $x^2 + y^2$ l'est) et les trois côtés du triangle équilatéral sont des bitangentes (quand on coupe par $2x + 1 = 0$ par exemple, les solutions sont doubles, à cause du carré de l'équation du cercle). En réalité, l'équation que nous choisirons pour K_0 est la suivante :

$$49(2x + 1)(-x + \sqrt{3}y + 1)(-x - \sqrt{3}y + 1) - 3(7(x^2 + y^2) - 4)^2 = 0$$

(on a donc $R = 2/\sqrt{7}$). Attention, ce choix numérique (on y notera la présence des trois nombres premiers $2, 3, 7$ que nous reverrons tout au long de l'exposé) n'est pas du tout innocent et c'est lui qui va faire que cette (belle) courbe réelle va s'avérer plus belle encore en complexes. En vérité, on peut s'en douter, ce n'est pas cette équation qui est apparue la première, mais une autre, plus naturelle, qui interviendra dans un cadre un peu plus général.

1.2 Les inflexions

Si l'on regarde bien le dessin de K_0 on y voit d'autres points remarquables : les points d'inflexion, points où la tangente traverse la courbe et la coupe avec multiplicité 3, puisque la dérivée seconde s'annule (penser à la formule de Taylor), de sorte que la tangente ne recoupe la courbe qu'un seul point. Il en apparaît 6, permutés par le groupe $\mathfrak{S}_3$, et formant deux triangles équilatéraux T_1, T_2. Sur la figure 1, on constate deux phénomènes :

1) Ces triangles ont une propriété géométrique remarquable[3] : la tangente en chaque point d'inflexion de T_1 recoupe K en un unique point qui est un autre point de T_1. Cette propriété mérite un nom :

1.1. Définition. *On appelle* **triangle d'inflexion** *d'une quartique K un triangle abc de points de K tel que :*
1) a, b, c sont des points d'inflexions de K,
2) les tangentes en a, b, c sont respectivement $(ca), (ab), (bc)$.

2) Les six points d'intersection sont sur un cercle qui a l'air d'être de rayon moitié du cercle des contacts des bitangentes : $1/\sqrt{7}$.

On peut calculer explicitement ces inflexions. Je propose pour cela deux voies, l'une plus théorique, l'autre plus adaptée à la situation.

D'une manière générale, on a une courbe plane définie par une équation implicite $f(x, y) = 0$. Comme elle est lisse, le théorème des fonctions implicites nous dit qu'on peut résoudre l'équation soit en y, soit en x, disons par exemple sous la forme $y = g(x)$. On sait calculer la dérivée $g'(x)$ en partant de l'identité $f(x, g(x)) = 0$ que l'on dérive :

$$\frac{\partial f}{\partial x}(x, g(x)) + \frac{\partial f}{\partial x}(x, g(x))g'(x) = 0$$

ce qui donne

$$g'(x) = -\frac{\frac{\partial f}{\partial x}(x, g(x))}{\frac{\partial f}{\partial x}(x, g(x))}.$$

Pour trouver les points d'inflexion il suffit d'écrire que la dérivée seconde $g''(x)$ est nulle, ce qui conduit à la relation (dite hessienne) :

$$\frac{\partial^2 f}{\partial x^2}\Big(\frac{\partial f}{\partial y}\Big)^2 - 2\frac{\partial^2 f}{\partial x \partial y}\frac{\partial f}{\partial x}\frac{\partial f}{\partial y} + \frac{\partial^2 f}{\partial y^2}\Big(\frac{\partial f}{\partial x}\Big)^2 = 0$$

ou encore, avec une notation plus économique :

$$f''_{x^2}\,(f'_y)^2 - 2f''_{xy}\,f'_x\,f'_y + f''_{y^2}\,(f'_x)^2 = 0.$$

Pour trouver les inflexions on peut alors éliminer x (ou y) entre ces deux équations, puis résoudre l'équation en y (ou x) obtenue. Il y a des techniques

[3]Même si on a une quartique avec un automorphisme d'ordre 3 et un triangle formé de trois inflexions qui s'échangent par cet automorphisme, les tangentes inflexionnelles ne sont pas nécessairement les côtés du triangle, cf. annexe 1.

pour cela (on peut par exemple écrire le résultant des polynômes) et les logiciels de calcul formel le font sans problème.

Dans notre cas, pour trouver les inflexions, comme on se doute qu'elles sont sur le cercle de rayon $1/\sqrt{7}$, le mieux est de couper K_0 par ce cercle, ce qui permet d'éliminer le dernier terme de f. Il reste une équation du troisième degré en x : $8 \times 49x^3 - 42x + 1 = 0$. Si l'on pose, pour éliminer le coefficient de x^3, $x' = 14x$, l'équation devient $x'^3 - 21x' + 7 = 0$.

Cela permet de calculer des valeurs approchées des inflexions (et de vérifier que ce sont bien des inflexions en utilisant la hessienne). On peut aussi les trouver sous une forme algébrique si la profusion de 7 et de $\sqrt{7}$ nous fait penser aux racines 7-èmes de l'unité. En effet, si on pose $\zeta = e^{2i\pi/7}$, on a la relation $1 + (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^3 + \zeta^{-3}) = 0$. Si on pose $u = \zeta + \zeta^{-1}$, on a $\zeta^2 + \zeta^{-2} = u^2 - 2$ et $\zeta^3 + \zeta^{-3} = u^3 - 3u$ et u est solution de l'équation $u^3 + u^2 - 2u - 1 = 0$.

Le changement de variable usuel $v = u + \frac{1}{3}$ élimine le terme de degré 2 et on obtient : $v^3 - \frac{7}{3}v - \frac{7}{27} = 0$. En posant $x' = 3v$ on retrouve l'équation ci-dessus. On peut donc calculer les inflexions en termes de racines septièmes de l'unité. Voilà les coordonnées des trois inflexions du premier triangle :

$$a = \Big(-\frac{1}{14}\big(1 + 3(\zeta + \zeta^{-1})\big)\ ,\ \frac{\sqrt{3}}{14}\big(\zeta^3 + \zeta^{-3} - \zeta^2 - \zeta^{-2}\big)\Big),$$

$$b = \Big(-\frac{1}{14}\big(1 + 3(\zeta^3 + \zeta^{-3})\big)\ ,\ \frac{\sqrt{3}}{14}\big(\zeta^2 + \zeta^{-2} - \zeta - \zeta^{-1}\big)\Big),$$

$$c = \Big(-\frac{1}{14}\big(1 + 3(\zeta^2 + \zeta^{-2})\big)\ ,\ \frac{\sqrt{3}}{14}\big(\zeta + \zeta^{-1} - \zeta^3 - \zeta^{-3}\big)\Big),$$

Les autres sont les symétriques de celles-là par rapport à Ox.

On peut encore écrire ces inflexions en termes de cosinus, par exemple :

$$a = \left(-\frac{1}{14}\left[1 + 6\cos\frac{2\pi}{7}\right], \frac{\sqrt{3}}{14}\left[2\cos\frac{6\pi}{7} - 2\cos\frac{4\pi}{7}\right]\right),$$

les autres s'obtenant par l'action du groupe $\mathfrak{S}_3$. Dans cette formule on notera encore la présence des entiers $2, 3, 7$.

1.2. *Remarque.* Nous verrons plus loin que la courbe K_0 a 24 inflexions si on la regarde comme une courbe projective complexe. En revanche, dans le plan affine réel elle n'a que les 6 considérées. En effet, le changement de repère qui transforme K_0 en K étant réel, il suffit de le voir pour K. Dans ce cas il y a les trois points a, b, c du repère, ainsi que leurs images a', b', c' par τ (qui est réelle en dépit des apparences, cf. plus loin). Les 18 autres inflexions sont les images de a', b', c' par le sous-groupe engendré à 21 éléments engendré par ρ et σ. Ce qu'il faut voir c'est que dans ce groupe les seuls éléments réels (y compris à un scalaire près) sont $\mathrm{Id}, \sigma, \sigma^2$. C'est évident car ces matrices sont les matrices de permutation affublées de ζ, ζ^2, ζ^4, à peu de choses près.

2 La quartique de Klein : variante projective complexe

2.1 Le plan projectif

Quand on fait de la géométrie algébrique (par exemple quand on étudie des courbes algébriques planes), on se rend vite compte que travailler dans le plan affine réel n'est pas satisfaisant. Ainsi, si l'on regarde l'intersection d'une conique et d'une droite on a envie de dire qu'il y a deux points d'intersection. Bien entendu cela peut être faux (penser à une droite extérieure à un cercle ou à une parallèle à l'asymptote d'une hyperbole). Dans le cas d'une droite et d'un cercle on trouve toujours deux points d'intersection, mais éventuellement imaginaires ou confondus. Dans le cas de l'hyperbole, le point manquant est “à l'infini”. Le même problème se rencontre avec l'intersection de deux coniques, ou le nombre de points d'intersection attendus est 4, mais où il n'est pas toujours atteint (penser à deux cercles), et de même pour deux courbes de degrés d et d'. La solution adoptée depuis Poncelet et d'autres, au début du XIX ème siècle, est de travailler dans le plan projectif complexe. Pour le mot complexe, cela veut dire simplement qu'on prend des points à coordonnées complexes. Ainsi, le cercle $x^2+y^2=1$ et la droite $x=2$ se coupent en deux points : $(2, \pm\frac{i\sqrt{3}}{2})$. Pour le mot projectif, cela signifie qu'on introduit des points à l'infini. Précisément, on considère, au lieu des points (x, y) du plan affine des points (x, y, t), mais avec des coordonnées **homogènes**, ce qui signifie que x, y, t ne sont pas tous nuls et que le point (x, y, t) est le même que $(\lambda x, \lambda y, \lambda t)$. L'ensemble de ces points est le plan projectif $\mathbf{P}^2(\mathbf{C})$. On y retrouve le plan affine en prenant les points $(x, y, 1)$, mais aussi une droite à l'infini formée des points $(x, y, 0)$, définis à un scalaire près.

Les courbes algébriques de $\mathbf{P}^2(\mathbf{C})$ sont définies encore comme zéros de polynômes, mais cette fois, de polynômes homogènes $F(X, Y, T)$ (en effet, si (x, y, t) est solution, il faut que $(\lambda x, \lambda y, \lambda t)$ le soit aussi). Par exemple,

$uX+vY+wT=0$ est une droite projective, dont la partie affine est l'ensemble des points $(x,y,1)$ qui vérifient $ux+vy+w=0$: c'est bien une droite affine, mais elle a, en plus, à l'infini l'unique point $(v,-u,0)$ (les coordonnées ne sont définies qu'à un scalaire près) qui correspond à la direction de D. Quand on a une courbe affine, on obtient sa complétion projective en homogénéisant son équation (usuellement avec la variable T). Par exemple, l'hyperbole $xy-1=0$ devient $XY-T^2$ et on voit, à l'infini, les deux points $(1,0,0)$ et $(0,1,0)$ qui correspondent aux points à l'infini de Ox et Oy.

Les bonnes applications du plan projectif sont les homographies : elles correspondent aux applications linéaires bijectives $u : \mathbf{C}^3 \to \mathbf{C}^3$, donc aux matrices 3×3 inversibles : le groupe $GL(3,\mathbf{C})$. En fait, comme les homothéties sont triviales en projectif (à cause de l'homogénéité des coordonnées), le groupe des homographies est le groupe $PGL(3,\mathbf{C})$, quotient du précédent par les homothéties. On verra plusieurs exemples d'homographies ci-dessous. Les applications affines bijectives (par exemple les isométries du groupe $\mathfrak{S}_3$ vu ci-dessus) se prolongent en des homographies par homogénéisation.

Dans le cas de la courbe de Klein K, on va voir que le passage en projectif complexe révèle des propriétés insoupçonnées, en particulier la présence de très nombreux automorphismes de K (i.e. des homographies qui conservent K).

2.2 La pseudo-quartique de Klein et ses automorphismes

2.2.1 Un triangle d'inflexion

Nous allons maintenant aller vers la forme définitive de la quartique de Klein. Pour cela, il faut repenser à un triangle d'inflexions. Lorsqu'on a un tel triangle, on peut toujours l'envoyer par une homographie sur n'importe quel autre triangle. On peut même envoyer quatre points (non trois à trois alignés) sur quatre autres.

Or, dans le plan projectif, avec les coordonnées (x,y,t) il y a un triangle particulièrement simple : $a=(1,0,0)$, $b=(0,1,0)$, $c=(0,0,1)$ (le point à l'infini de l'axe des x, celui de l'axe des y et l'origine du plan affine). On peut envoyer le triangle d'inflexions de K_0 (celui qui s'appelait déjà abc) sur abc. De plus, on peut aussi envoyer l'origine o du plan affine sur le point unité $d=(1,1,1)$ de $\mathbf{P}^2$. La rotation de centre o qui permute les inflexions de K_0 devient une homographie de $\mathbf{P}^2$ qui permute a,b,c et fixe d. À un scalaire près c'est l'homographie σ définie par $X \mapsto Y \mapsto T \mapsto X$.

Appelons $F(X,Y,T)$ la nouvelle équation de la quartique. Bien entendu, on peut déterminer F par le calcul à partir de l'équation de la quartique affine, mais on peut aussi (presque) le faire sans calculs en tenant compte du fait qu'elle admet le triangle abc comme triangle d'inflexion et qu'elle est stable par σ. C'est le lemme suivant :

2.1. Lemme. *Soit F une quartique de $\mathbf{P}^2(\mathbf{C})$. On suppose que les points a,b,c sont des inflexions de F et que les droites $(ca),(ab),(bc)$ sont les tangentes inflexionnelles en a,b,c. On suppose de plus que F est stable par σ. On peut écrire F sous la forme :*

$$F(X,Y,T) = X^3Y + Y^3T + T^3X + AXYT(X+Y+T).$$

Démonstration. Regardons le point c. Dire qu'il est sur K signifie que F n'a pas de terme en T^4. Pour trouver la tangente en c, on se place dans le plan affine $t=1$ en étudiant la courbe $f(x,y) = F(x,y,1)$. La tangente est alors donnée par les termes de degré 1 en x,y[4] (donc les termes en XT^3 et YT^3 de F) et dire que c'est la droite (bc) d'équation $X=0$ c'est dire que le terme en YT^3 est nul. Dire que c est un point d'inflexion signifie que, si on coupe par la tangente $x=0$, la multiplicité d'intersection est ≥ 3, c'est-à-dire qu'il n'y a pas de terme en y^2 (donc de terme en Y^2T^2). En appliquant le même raisonnement en a et b, et en tenant compte de la stabilité de F par σ, on obtient la forme annoncée (car F n'est définie qu'à un scalaire près).

2.2.2 Automorphismes et inflexions : premier épisode

Dans un premier temps nous supposerons que K est la courbe d'équation $F(X,Y,T) = X^3Y + Y^3T + T^3X + AXYT(X+Y+T) = 0$.

Les automorphismes d'une courbe algébrique C sont les homographies du plan qui conservent C. Ils forment un groupe qu'on notera G dans le cas de la courbe de Klein. Comme G est un sous-groupe de $PGL(3,\mathbf{C})$ et que ce groupe est isomorphe à $PSL(3,\mathbf{C})$ (le quotient est $\mathbf{C}^*/\mathbf{C}^{*3}$, cf. [Perrin1]), on peut supposer que l'image réciproque de G dans $GL(3,\mathbf{C})$ est formée de matrices de déterminant 1. Nous allons en exhiber trois et étudier le groupe G.

Le premier automorphisme de K a déjà été vu : c'est la permutation circulaire des coordonnées : $x \mapsto y \mapsto t \mapsto x$. Il s'agit d'un automorphisme

[4] Si $f(x,y) = ax + by + ...$, et si on coupe la courbe par $ax + by = 0$, comme il ne reste que des termes de degré ≥ 2 la multiplicité d'intersection est ≥ 2.

d'ordre 3, de matrice $\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Cet automorphisme permute les trois sommets a, b, c du triangle d'inflexions. Une bonne partie de notre travail va consister à regarder l'action de G sur l'ensemble I de ses inflexions. Il est clair que si m en est une et si g est dans G, $g(m)$ est aussi une inflexion (car la multiplicité d'intersection est conservée par les homographies). Autrement dit G permute l'ensemble I et il est intéressant de chercher le stabilisateur d'une inflexion, disons par exemple a. C'est le sous-groupe G_a des $g \in G$ tels que $g(a) = a$. On a la proposition suivante :

2.2. Proposition.
1) Si la constante A est non nulle, le stabilisateur G_a est réduit à l'élément neutre.
2) On suppose $A = 0$. Le stabilisateur G_a est un groupe d'ordre 7 engendré par l'homographie de matrice $\rho = \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix}$ où ζ est une racine primitive 7-ème de l'unité (disons $\zeta = e^{2i\pi/7}$).

Démonstration. 1) Soit $g \in G_a$. Notons que si on a $g(a) = a$ on a aussi $g(b) = b$ et $g(c) = c$. En effet, si g fixe a il transforme la tangente T_a en a en elle même. Comme T_a recoupe K en b, cela implique que b est fixe lui aussi, et de même pour c.

Attention, dire qu'on a $g(a) = a$ dans le projectif cela veut dire $g(a) = \lambda a$ en vectoriel : autrement dit a est un vecteur vecteur propre de g. Cela signifie que dans la base canonique g est diagonale : $g = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{pmatrix}$, avec λ, μ, ν non nuls et on peut supposer g de déterminant 1. Écrivons que cette matrice conserve K. Cela signifie que $F(\lambda X, \mu Y, \nu T)$ est proportionnel à $F(X, Y, T)$. Or, on a $F(\lambda X, \mu Y, \nu T) = \lambda^3 \mu X^3 Y + \mu^3 \nu Y^3 T + \nu^3 \lambda T^3 X + A\lambda\mu\nu XYT(\lambda X + \mu Y + \nu T)$. Si A est non nul, on doit donc avoir $\lambda^3\mu = \mu^3\nu = \nu^3\lambda = \lambda^2\mu\nu = \lambda\mu^2\nu = \lambda\mu\nu^2$. On voit aussitôt que cela impose $\lambda = \mu = \nu$, de sorte que g est une homothétie vectorielle, donc l'identité dans le projectif.

2) Supposons maintenant $A = 0$. Il reste seulement les relations $\lambda^3\mu = \mu^3\nu = \nu^3\lambda$. Intéressons-nous aux rapports $k = \lambda/\mu$ et $l = \mu/\nu$ en notant qu'on a alors $\lambda/\nu = kl$. On a $k^3 = \frac{1}{l}$ et $l^3 = kl$, d'où l'on déduit $l^2 = k$ et $l^6 = \frac{1}{l}$. On voit donc que l est une racine septième de l'unité, qui est

primitive si g n'est pas l'identité. Appelons ζ cette racine. On a donc $\mu = \zeta\nu$ et $\lambda = \zeta^3\nu$. Comme le déterminant de g vaut 1, on a $\zeta^4\nu^3 = 1$, ce qui donne $\nu^3 = \zeta^3$ donc $\nu = \zeta$, ou $\nu = j\zeta$ ou $\nu = j^2\zeta$. On en déduit que la matrice est égale à la matrice proposée ou à son produit par j ou j^2, ce qui, dans $PGL(3, \mathbf{C})$, est la même chose.

Réciproquement, on vérifie que $\lambda = \zeta^4$, $\mu = \zeta^2$ et $\nu = \zeta$ satisfait aux conditions requises.

2.2.3 Calcul des inflexions de K

Dans le cas d'une courbe projective, on a une méthode pour trouver toutes les inflexions de manière globale. Notons F'_X, F''_{XY}, etc. les dérivées partielles de $F(X, Y, T)$. On a le résultat suivant :

2.3. Proposition. *Soit $F(X, Y, T)$ une courbe projective lisse de $\mathbf{P}^2(\mathbf{C})$. Ses inflexions sont les intersections de F et de sa hessienne qui est la courbe définie par le polynôme suivant :*

$$H(X, Y, T) = \begin{vmatrix} F''_{X^2} & F''_{XY} & F''_{XT} \\ F''_{YX} & F''_{Y^2} & F''_{YT} \\ F''_{TX} & F''_{TY} & F''_{T^2} \end{vmatrix}.$$

Si F est homogène de degré d, H est homogène de degré $3(d-2)$, de sorte que le nombre d'inflexions, comptées convenablement, est $3d(d-2)$ (soit 24 lorsque d est égal à 4).

Démonstration. On calcule le déterminant en multipliant la première ligne par X, la seconde par Y et en les ajoutant à la troisième multipliée par T, puis on applique la formule d'Euler. Il apparaît un $d-1$ en facteur et la troisième ligne est remplacée par F'_X, F'_Y, F'_T. On refait la même chose avec les colonnes. La dernière colonne devient $F'X, F'_Y, F$ et en développant modulo F il reste le polynôme vu précédemment :

$$F''_{X^2}(F'_Y)^2 - 2F''_{XY}F'_XF'_Y + F''_{Y^2}(F'_X)^2.$$

2.4. Corollaire. *Le cardinal du groupe G est inférieur ou égal à 24 si A est non nul (resp. à 168 si A est nul).*

Démonstration. Cela résulte de la formule des classes : $|G| = |\omega(a)| \times |G_a|$ où $\omega(a)$ désigne l'orbite de a. Comme les éléments de G permutent les points d'inflexion, le cardinal de $\omega(a)$ est inférieur ou égal à 24 (et ce sera 24 si et seulement si l'opération est transitive). Par ailleurs, on a vu que le cardinal de G_a vaut 1 ou 7 selon les cas, d'où le résultat.

2.3 La courbe de Klein : la vraie

On va désormais travailler avec la courbe qui possède le groupe d'automorphismes le plus gros possible, donc celle qui correspond à $A = 0$:

2.5. Définition. *La quartique de Klein K est la courbe du plan projectif complexe définie par le polynôme $F(X,Y,T) = X^3Y + Y^3T + T^3X$.*

2.6. *Remarque.* Dans le cas de la quartique de Klein on a $H(X,Y,T) = 54(5X^2Y^2T^2 - YT^5 - TX^5 - XY^5)$. On retrouve bien les points a, b, c. Pour l'heure on sait qu'on a $3 \leq |I| \leq 24$. On pourrait d'ailleurs montrer directement à partir de ces équations qu'il y a exactement 24 points d'inflexion dans K.

2.7. *Remarque.* La droite $X + Y + T = 0$ est bitangente à K en les points $(1, j, j^2)$ et $(1, j^2, j)$.

2.8. *Remarque.* On peut montrer que les seuls points rationnels de K sont les trois points a, b, c du triangle d'inflexion initial. Cela implique d'ailleurs le théorème de Fermat pour l'exposant 7. En effet, si on a une solution entière de l'équation de Fermat $u^7 + v^7 + w^7 = 0$, avec u, v, w non nuls, on obtient un point rationnel de K en prenant $x = u^3w$, $y = v^3u$, $t = w^3v$, calcul très proche de celui effectué ci-dessus pour calculer G_a.

2.3.1 Une involution

On a vu que la variante réelle K_0 de la courbe de Klein admettait aussi des automorphismes d'ordre 2 (les symétries axiales du triangle équilatéral). On retrouve ces symétries pour K, mais elles sont un peu plus délicates à écrire. On peut les obtenir à partir des symétries de la courbe réelle par conjugaison, mais le calcul est un peu saumâtre. Il est plutôt plus simple de chercher τ comme une involution, qui conserve K et vérifie $\tau\sigma\tau^{-1} = \sigma^2$, voir Annexe 2.

On trouve l'involution suivante : $\tau = k \begin{pmatrix} \lambda & \mu & \nu \\ \mu & \nu & \lambda \\ \nu & \lambda & \mu \end{pmatrix}$, avec $k = \dfrac{i}{\sqrt{7}}$ et $\lambda = \zeta - \zeta^{-1}$, $\mu = \zeta^2 - \zeta^{-2}$, $\nu = \zeta^4 - \zeta^{-4}$.

On vérifie que τ conserve K (si on ne le sait pas déjà à partir de la courbe réelle)[5].

[5] On notera que τ est réelle, en dépit des apparences et (sans doute) conjuguée de la symétrie d'axe Ox de K_0. Les 6 inflexions réelles sont donc a, b, c et leurs images par τ.

2.3.2 Retour aux inflexions

L'étude de l'opération de G sur I va nous permettre de montrer le résultat principal :

2.9. Théorème. *Le groupe G a 168 éléments.*

Démonstration. En vertu de la formule des classes, il suffit de montrer que G opère transitivement sur I. On pose $I' = I - \{a, b, c\}$. Dans G il y a l'involution τ qui envoie a dans I' comme le montre sa matrice (car $\tau(a) \neq a, b, c$).

On regarde le sous-groupe H de G engendré par ρ et σ. Comme on a $\sigma^{-1}\rho\sigma = \rho^2$ (la conjugaison par σ permute les termes diagonaux et on conclut avec $\zeta^8 = \zeta$), on peut écrire tous les éléments de H sous la forme $\sigma^i\rho^j$ avec $0 \leq i \leq 2$ et $0 \leq j \leq 6$. Le groupe H est donc de cardinal 21. Il opère sur I' et son orbite Ω est de cardinal diviseur de 21. Dans cette opération, le sous-groupe $H_1 = <\rho>$ ne fixe personne (les seuls points fixes, i.e. vecteurs propres, des puissances de ρ sont a, b, c). Il a donc trois orbites de cardinal 7 dans I'. Par ailleurs, le sous-groupe $H_2 = <\sigma>$ laisse stable $\{a, b, c\}$ donc opère aussi sur I' et il n'a pas de point fixe (ses points fixes sont $(1, 1, 1)$ qui n'est pas sur K et $(1, j, j^2)$ et $(1, j^2, j)$ qui sont les contacts de la bitangente $X+Y+T$ donc ne sont pas des inflexions !). Il ne peut donc pas laisser stable une orbite de cardinal 7. Il en résulte que l'orbite Ω est égale à I', donc que G est transitif sur I.

2.10. *Remarque.* En fait il y a un groupe à 336 éléments qui conserve K. Il est formé d'homographies et d'anti-homographies, et s'obtient en rajoutant à G la conjugaison : $(x, y, t) \mapsto (\overline{x}, \overline{y}, \overline{t})$ et ses produits avec les éléments de G. On en aura une description plus géométrique dans la quatrième partie.

2.3.3 Les bitangentes

2.11. Corollaire. *La courbe K admet 28 bitangentes qui forment une orbite sous G. Le stabilisateur de la bitangente $X+Y+T$ est le sous-groupe $<\sigma, \tau>$, isomorphe à $\mathfrak{S}_3$.*

Démonstration. Le groupe opère sur les bitangentes et on voit aussitôt que le stabilisateur de la bitangente $X + Y + T$ contient le sous-groupe $<\sigma, \tau>$. On montre que le stabilisateur est égal à ce sous-groupe (cf. Annexe 3). L'orbite de cette bitangente est donc de cardinal 28. On conclut avec la proposition suivante :

2.12. Proposition. *Le nombre de bitangentes d'une courbe lisse de degré d est inférieur ou égal à* $\frac{d(d-2)(d-3)(d+3)}{2}\cdot$ *Il est égal à ce nombre si les bitangentes sont comptées avec leurs multiplicités. Une quartique lisse a au plus* 28 *bitangentes distinctes.*

Démonstration. Cela résulte des formules de Plücker, cf. [Fischer]. Une courbe lisse C de degré d est de classe $d^* = d(d-1)$ (cela signifie que l'on peut mener $d(d-1)$ tangentes à C d'un point extérieur). La courbe duale est donc de degré $d^* = d(d-1)$ et la formule de Plücker affirme qu'on a $d^*(d^*-1) = d+3i+2b$ où i est le nombre d'inflexions et b le nombre de bitangentes, comptées convenablement (les bitangentes et les inflexions sont respectivement les points doubles et les rebroussements de la courbe duale). Cette formule s'écrit encore $d^3(d-2) = 2b+3i$. Comme on a vu avec la hessienne qu'on a $i = 3d(d-2)$, on en déduit la formule annoncée.

2.13. *Remarque.* Dans le cas de la courbe de Klein on peut montrer à la main qu'il y a exactement 28 bitangentes, voir annexe 3.

2.3.4 Simplicité

2.14. Théorème. *Le groupe G est simple.*

Démonstration. La preuve consiste essentiellement à passer en revue les éléments de G et leurs conjugués.

Considérons les éléments d'ordre 7 du groupe G. On a vu qu'il y a déjà les éléments des stabilisateurs des 24 inflexions. Si un élément ρ' d'ordre 7 fixe une inflexion, il en fixe trois (comme dans le cas de a, b, c). Comme G est transitif sur I, ρ' est conjugué d'un ρ^i, donc il a trois droites propres seulement, donc il fixe seulement ces trois inflexions. Il y a donc 6 éléments d'ordre 7 par paquet de 3 inflexions (on exclut le neutre), et cela fait $6\times 8 = 48$ éléments d'ordre 7. De plus, un élément g d'ordre 7 est nécessairement dans le stabilisateur d'une inflexion. En effet, les orbites du sous-groupe $<g>$ sur I sont de cardinal 1 ou 7 et elles ne peuvent être toutes de cardinal 7 (car 7 ne divise pas 24). Il y a donc une orbite de cardinal 1, i.e. un point fixe.

En bref, on a 48 éléments d'ordre 7, qui sont exactement les éléments qui fixent les inflexions.

De la même façon, pour chaque bitangente T, il y a 2 éléments d'ordre 3 qui laissent stable T et un élément d'ordre 3 laisse nécessairement stable une bitangente (même argument que ci-dessus : 3 ne divise pas 28), et une seule (car un élément d'ordre 3 ne fixe pas plusieurs bitangentes, cf. annexe 3). Il y a donc 56 éléments d'ordre 3.

Passons aux involutions (éléments d'ordre 2). On peut montrer qu'il y en a 21, toutes conjuguées, cf. ci-dessous. On peut aussi raisonner directement :

1) Une involution et un élément ρ d'ordre 7 ne commutent pas. Sinon, l'involution permuterait les points fixes de ρ, i.e. un triangle d'inflexion. Or il y a 3 pointsdans un triangle, donc elle en fixerait nécessairement un et on a vu que le stabilisateur des inflexions est uniquement formé d'éléments d'ordre 7.

2) Une involution et un élément d'ordre 3 ne commutent pas. En effet, si σ' est un élément d'ordre 3, il stabilise une bitangente et une seule et, comme G est transitif sur les bitangentes, on peut supposer que c'est T et que σ' c'est σ. Si τ', d'ordre 2, commute avec σ, il stabilise aussi T. Or, on a calculé le stabilisateur d'une bitangente et on a vu que c'était le groupe $<\sigma, \tau>$, isomorphe à $\mathfrak{S}_3$, ce qui contredit le fait que σ et τ' commutent.

Regardons alors les conjugués d'une involution sous l'action du groupe à 21 éléments $<\rho, \sigma>$. Le centralisateur ne contenant aucun élément d'ordre 3 ou 7 est réduit à l'élément neutre, donc l'orbite est de cardinal 21, autrement dit, une involution admet (au moins) 21 conjugués.

On peut alors prouver le théorème. Supposons que G contienne un sous-groupe distingué N, non réduit à l'élément neutre. Nous allons montrer que N est égal à G. Comme le cardinal d'un sous-groupe divise le cardinal du groupe, il suffit de montrer qu'on a $|N| > 84$. Dès que N contient un élément n, il contient tous ses conjugués gng^{-1}.

Si N ne contient pas d'élément d'ordre 7 ni d'ordre 3, son cardinal n'est ni multiple de 7, ni multiple de 3. Comme il divise 168, c'est donc un diviseur de 8. Le sous-groupe contient alors une involution, donc aussi ses 21 conjuguées et c'est absurde pour un sous-groupe d'ordre ≤ 8.

Supposons maintenant que N contienne un élément d'ordre 7 (resp. 3). Alors, je dis qu'il les contient tous. En effet, si N contient, par exemple, l'élément ρ, qui fixe a, il contient tout le fixateur de a (car ce groupe est cyclique). Si m est une autre inflexion, il existe un $g \in G$ tel que $g(a) = m$, mais alors $g\rho g^{-1}$, qui est contenu dans N, fixe m. Le sous-groupe N contient tous les fixateurs des inflexions, donc tous les éléments d'ordre 7. Le raisonnement est identique pour les éléments d'ordre 3. Mais alors, le cardinal de N est au moins $48 + 1$ (resp. $56 + 1$), donc c'est $56, 84$ ou 168 (resp. 84 ou 168). Le cas 84 est écarté car N contiendrait à la fois un élément d'ordre

7 et un d'ordre 3 donc au moins 105 éléments.

Il reste le cas $|N| = 56$. Dans ce cas, outre les éléments d'ordre 7, N contiendrait un élément d'ordre 2, donc il en contiendrait 21 et c'est absurde car $48 + 1 > 56$.

2.15. *Remarque.* Montrons qu'il n'y a que 21 involutions, toutes conjuguées. D'abord il y a une involution dont la classe de conjugaison contient exactement 21 éléments. En effet, on prend un 2-Sylow, S, de cardinal 8. Il a un centre, qui contient un élément d'ordre 2. Le centralisateur de cet élément est donc d'ordre 8 (on a vu qu'il ne contenait pas d'éléments d'ordre 3 et 7). Donc son orbite a 21 éléments. Ensuite, s'il y avait des classes plus grandes, elles auraient 42 ou 84 éléments. Le cas 84 est exclu par comptage. Pour 42, avec l'orbite précédente, cela donnerait 63 éléments d'ordre 2, donc il n'y aurait rien d'autre ($48 + 56 + 63 + 1 = 168$). Les Sylow n'auraient alors que des éléments d'ordre 2, donc seraient abéliens. Par ailleurs, le centralisateur d'une involution aurait 4 éléments. C'est absurde.

On peut montrer aussi qu'il y a 21 Sylow d'ordre 8. En effet, il y en a $1, 3, 7$ ou 21. Comme G est simple, 1 et 3 sont exclus. S'il y en avait 7, il y aurait au plus 49 éléments d'ordre une puissance de 2. Comme les éléments de G sont d'ordre $3, 7$ ou une puissance de 2 (car il n'y a pas de commutation entre des éléments d'ordre $2, 3, 7$), on aurait seulement $48+56+49+1 = 154$ éléments.

2.4 Commentaires

2.4.1 Automorphismes

Dans ce paragraphe nous expliquons en quoi la présence de ces 168 automorphismes est exceptionnelle et donc en quoi la courbe de Klein est particulièrement belle.

En ce qui concerne les automorphismes d'une courbe algébrique plane C, les choses sont assez différentes selon le degré d de C (ou encore son genre g, voir plus bas, cela revient au même car degré et genre sont liés par la formule $g = \dfrac{(d-1)(d-2)}{2}$). Lorsque d vaut 1, la courbe est une droite D et le groupe des isométries qui conservent une droite est très gros. Par dualité c'est le même groupe que celui des homographies qui fixent un point qui est un groupe algébrique de dimension 6. Pour $d = 2$, la courbe C est une conique définie par une forme quadratique q et son groupe d'automorphismes est le groupe $O^+(q)$, c'est un groupe algébrique de dimension 3. Pour $d = 3$ on a affaire à une courbe elliptique et son groupe d'automorphismes lui est essentiellement isomorphe : de dimension 1. À partir du degré 4 (ou du genre 3) le groupe G est un groupe fini. Voici un argument, dans un cas particulier :

2.16. Lemme. *Soit C une courbe algébrique plane lisse de degré 4 admettant au moins 4 points d'inflexion distincts. Alors le groupe des automorphismes de C est fini.*

Démonstration. On a vu qu'une telle courbe a un ensemble fini de points d'inflexions I. Soit alors $u \in \mathrm{Aut}\,(C)$. Il est clair que u envoie I sur I, de sorte qu'on a un homomorphisme $\varphi : G \to \mathfrak{S}(I)$. Comme trois inflexions ne peuvent être alignées, on a un repère projectif dans I et φ est injectif.

En fait, on a le théorème général suivant :

2.17. Théorème. (Hurwitz) *Si C est une courbe algébrique lisse de genre $g \geq 2$ on a $|\mathrm{Aut}\,(C)| \leq 84(g-1)$.*

Dans le cas de la courbe de Klein, le genre est 3 et la borne est donc de 168 : elle est donc atteinte, ce qui est exceptionnel (les plus petits genres pour lesquels c'est vrai sont 3, 7, 14, 17, voir l'article de A. Murray Macbeath dans [Levy]).

2.4.2 Groupes simples

Rappelons qu'un groupe est dit simple s'il n'a pas de sous-groupe distingué non trivial. Les groupes simples jouent un rôle essentiel en théorie des groupes. Si un groupe G a un sous-groupe distingué N, il y a un groupe quotient G/N et on peut espérer "dévisser " le groupe G en ramenant son étude à celle de N et de G/N qui sont plus petits. Si G est simple, on ne peut faire cela : les groupes simples sont en quelques sorte les particules élémentaires de la théorie et on doit les connaître tous. On sait effectivement les classifier depuis une vingtaine d'années (mais cela représente 10000 pages de texte mathématique !). Les plus petits, en dehors des groupes triviaux $\mathbf{Z}/p\mathbf{Z}$ pour p premier, sont le groupe alterné $\mathfrak{A}_5$ (groupe de l'icosaèdre) qui a 60 éléments et le groupe G qui en a 168.

Il est bien connu qu'il n'y a qu'un seul groupe simple à 168 éléments et qu'il a deux habits différents, étant isomorphe à la fois à $PSL(2, \mathbf{F}_7)$ et $PSL(3, \mathbf{F}_2)$, cf. [Perrin1]. Dans le paragraphe suivant, nous identifions le groupe G à $GL(3, \mathbf{F}_2)$ (ou $PSL(3, \mathbf{F}_2)$, c'est pareil), groupe des matrices inversibles 3×3 sur le corps à 2 éléments. Pour comprendre l'aspect $PSL(2,\mathbf{F}_7)$, il faut passer par le demi-plan de Poincaré, cf. [Bavard].

2.5 L'isomorphisme entre G et $GL(3,\mathbf{F}_2)$

2.5.1 L'anneau A et son quotient $\mathbf{F}_8$

Le groupe G, contenu dans $PGL(3,\mathbf{C})$, se relève en un groupe noté encore G et contenu dans $SL(3,\mathbf{C})$, engendré par ρ,σ,τ. En fait, ces matrices sont à coefficients dans un sous-anneau A de $\mathbf{C}$, précisément le sous-anneau $A = \mathbf{Z}[\zeta]_{2\alpha+1}$ où l'on a posé $\alpha = \zeta+\zeta^2+\zeta^4 = \dfrac{-1+i\sqrt{7}}{2}$, donc $2\alpha+1 = i\sqrt{7}$. L'anneau A est le localisé de $\mathbf{Z}[\zeta]$ obtenu en inversant $2\alpha+1$. On a alors le lemme suivant :

2.18. Lemme. *Le quotient de A par l'idéal $(2,\zeta^3+\zeta+1)$ est le corps $\mathbf{F}_8$.*

Démonstration. Rappelons qu'on a $\mathbf{Z}[\zeta] \simeq \mathbf{Z}[X]/(X^6+X^5+\cdots+X+1)$. Le corps $\mathbf{F}_8$ est formé de 7 racines septièmes de 1 et de 0. Comme on a, sur $\mathbf{F}_2$, $X^6+X^5+\cdots+X+1 = (X^3+X+1)(X^3+X^2+1)$ et que ces polynômes sont irréductibles, $\mathbf{F}_8$ est le corps de rupture de chacun de ces polynômes. Appelons ζ une racine du premier. On a donc $\zeta^3+\zeta+1=0$ et donc aussi $\zeta+\zeta^2+\zeta^4=0$. On envoie $\mathbf{Z}[X]$ dans $\mathbf{F}_8$ en envoyant X sur ζ. Comme on a, dans $\mathbf{F}_8$, $2\alpha+1=1$, le morphisme se factorise par le localisé et son noyau est l'idéal annoncé, d'où le résultat.

2.5.2 Le sous-groupe de $GL(3,\mathbf{F}_8)$

On considère l'homomorphisme de réduction $\pi : GL(3,A) \to GL(3,\mathbf{F}_8)$. Comme G est simple il est isomorphe à son image, notée encore G. On appelle encore ρ et σ les images des éléments correspondants qui s'écrivent de la même manière dans $\mathbf{F}_8$. Pour τ on considère i $\tau' = -i\sqrt{7}\tau = -(2\alpha+1)\tau$ qui s'envoie sur le même élément de $\mathbf{F}_8$. On appelle encore τ l'image. Sur $\mathbf{F}_8$ on a la formule :

$$\tau = \begin{pmatrix} \zeta^{-2} & \zeta^3 & \zeta^{-1} \\ \zeta^3 & \zeta^{-1} & \zeta^{-2} \\ \zeta^{-1} & \zeta^{-2} & \zeta^3 \end{pmatrix}.$$

Cela résulte de la table d'addition de $\mathbf{F}_8$ (qui vient de $\zeta^3+\zeta+1=0$).

2.5.3 La conjugaison

On va montrer le théorème suivant :

2.19. Théorème. *Il existe $p \in GL(3, \mathbf{F}_8)$ telle que les trois matrices $\rho' = p\rho p^{-1}$, $\sigma' = p\sigma p^{-1}$ et $\tau' = p\tau p^{-1}$ soient dans $GL(3, \mathbf{F}_2)$. Le groupe G est isomorphe à $GL(3, \mathbf{F}_2)$.*

Démonstration. La dernière assertion est évidente puisque pGp^{-1} est inclus dans $GL(3, \mathbf{F}_2)$ et que tous deux sont de cardinal 168.

Pour la première, comme σ est déjà dans $GL(3, \mathbf{F}_2)$ on va chercher un p qui commute à σ. Un calcul immédiat montre que p est alors de la forme suivante : $\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$, matrice dont le déterminant est $a^3 + b^3 + c^3 + abc$ qui va valoir 1 si on prend $\{a, b, c\} = \{\zeta^{-1}, \zeta^{-2}, \zeta^3\}$ (il vaudrait 0 avec ζ, ζ^2, ζ^4). Pour trouver p, on peut (par exemple) écrire que pgp^{-1} est invariant par le Frobenius $F(t) = t^2$ dans le cas de $g = \rho$ et τ. Cela conduit aux conditions $p^{-1}F(p)F(g) = gp^{-1}F(p)$. La matrice $p^{-1}F(p)$ est de la même forme que p et le calcul montre qu'elle doit être égale à σ. Là encore un petit calcul montre qu'il faut prendre $a = \zeta^{-1}$, $b = \zeta^3$, $c = \zeta^{-1}$, c'est-à-dire :

$$p = \begin{pmatrix} \zeta^{-1} & \zeta^3 & \zeta^{-2} \\ \zeta^{-2} & \zeta^{-1} & \zeta^3 \\ \zeta^3 & \zeta^{-2} & \zeta^{-1} \end{pmatrix} \quad \text{et} \quad p^{-1} = \begin{pmatrix} \zeta^{-1} & \zeta^{-2} & \zeta^3 \\ \zeta^3 & \zeta^{-1} & \zeta^{-2} \\ \zeta^{-2} & \zeta^3 & \zeta^{-1} \end{pmatrix}.$$

On peut alors calculer les conjugués de ρ et τ :

$$\rho' = p\rho p^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \qquad \tau' = p\tau p^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

3 La courbe de Klein vue comme une surface

Dans les deux prochaines sections, on va faire le lien entre la courbe de Klein et la statue du MSRI. Dans cette section on explique uniquement le fait que cette surface possède trois trous.

3.1 Courbes et surfaces

Une courbe projective complexe K étant de dimension 1 sur $\mathbf{C}$ est donc de dimension 2 sur $\mathbf{R}$. Par exemple, une droite projective complexe, qui n'est autre qu'une droite affine complexe (donc un plan réel !) auqel on adjoint un point à l'infini, est topologiquement une sphère (la sphère de Riemann), comme on le voit par projection stéréographique. La courbe complexe K est ainsi une surface réelle, sans bord, compacte puisque le plan projectif l'est, lisse car la courbe l'est, et orientable (à cause de la multiplication par i dans les plans tangents). Il y a un théorème (non trivial !) de classification de ces objets (cf. [Gramain]) : une telle surface est soit une sphère, soit un tore à g trous (g étant ce qu'on appelle le genre de la surface, c'est 0 pour la sphère).

3.2 Genre et triangulations

Pour calculer le genre d'une surface on a un moyen topologique simple qui consiste à trianguler la surface. Intuitivement, cela signifie qu'on pave la surface par des triangles (des traingles curvilignes, images par des applications continues injectives de vrais triangles euclidiens), avec des sommets, des arêtes et des faces. Un exemple type de triangulation est obtenu en prenant un polyèdre convexe de $\mathbf{R}^3$ et en le projetant sur une sphère à partir d'un point intérieur. On compte le nombre f de faces de la triangulation, son nombre a d'arêtes et son nombre s de sommets. On a alors le théorème suivant :

3.1. Théorème. *Le nombre $\chi = s - a + f$ (appelé caractéristique d'Euler) est indépendant du choix de la triangulation. Si la surface S est de genre g, on a, pour toute triangulation de S, $\chi = s - a + f = 2 - 2g$.*

Démonstration. Pour la sphère c'est la fameuse formule d'Euler $s-a+f = 2$ que nous admettrons, cf. [Perrin2]. Si on admet que la caractéristique d'Euler est indépendante du choix de la triangulation (cf. [Douady], [Reyssat]), le second point est facile par récurrence sur g. Pour passer de g à $g+1$ on ajoute une anse. On peut le dessiner aisément pour le passage de la sphère au tore. On commence par étirer la sphère pour en faire une saucisse, dont on rapproche ensuite les extrémités que l'on va recoller pour obtenir le tore. On peut choisir la triangulation de la sphère de façon à recoller les deux morceaux le long de deux triangles. Dans cette opération, les deux faces triangulaires de recollement disparaissent de sorte qu'on a $f' = f - 2$, les six sommets de ces faces sont réduits à trois : $s' = s - 3$, enfin les six arêtes de ces faces sont elles aussi réduites à trois : $a' = a - 3$. En définitive, on a donc $\chi' = s' - a' + f' = s - a + f - 2 = \chi - 2$, cqfd. Le calcul est identique pour le passage de g à $g+1$.

3.3 Genre et revêtements

Soit $p : X \to B$ une application continue entre deux surfaces. On dit que p est un revêtement de degré d si pour chaque point $b \in B$ il y a un voisinage V tel que $p^{-1}(V)$ soit homéomorphe à la somme disjointe de d copies de V (on donne classiquement l'image d'une pile d'assiettes, ou de feuilles). On parle d'un revêtement ramifié si, en certains points b de B, la fibre $p^{-1}(b)$ est de cardinal plus petit que d (c'est le cas où plusieurs feuilles coïncident).

3.2. *Exemples.*
1) Soit X la courbe algébrique plane d'équation :

$$(*) \qquad f(x, y) = y^d + a_{d-1}(x)y^{d-1} + \cdots + a_0(x) = 0.$$

On projette X sur l'axe des x (la base B) en posant $p(x, y) = x$. Pour un x donné, il y a d nombres y qui vérifient $(*)$, de sorte que p est un revêtement de degré d, ramifié en les points (x, y) où la tangente est parallèle à la direction de projection. Le dessin en réels est sans doute plus parlant et plus facile qu'en complexes.
2) Un exemple simple est donné par l'application de "doublement de la longitude" de la sphère dans elle-même : on associe à un point de la sphère le point de même latitude, mais de longitude double (modulo 2π). C'est un revêtement de degré 2 car, par exemple, Hawaï est (à peu près) l'image de Louang Prabang (au Laos) et de Santiago de Cuba. Il est ramifié aux pôles nord et sud. On peut aussi le voir comme l'application $z \mapsto z^2$ de la sphère de Riemann $\mathbf{C} \cup \{\infty\}$ dans elle-même, ramifiée en 0 et ∞.

On a alors le théorème d'Hurwitz :

3.3. Théorème. *Soit $p : X \to B$ un revêtement de degré d, ramifié en n points de B. On suppose qu'au-dessus de ces points il y a deux feuilles seulement qui coïncident (donc $n - 1$ points dans la fibre). On note g le genre de B et g' celui de X. On a la formule :*

$$g' - 1 = d(g - 1) + \frac{n}{2}\cdot$$

Démonstration. On utilise une triangulation de B qui fait intervenir les points de ramification comme sommets. On montre (ce n'est pas évident) qu'on peut la relever en une triangulation de X et on compte. Au dessus de chaque face de B il y a d faces de X : $f' = df$. Au-dessus de chaque arête de B il y a aussi d arêtes de X : $a' = da$. Au-dessus de chaque sommet de B il y a encore d sommets de X, sauf en les n points de ramification où il n'y en a que $d-1$. On a donc $s' = ds - n$. Au total on a $2(1-g') = s' - a' + f' = d(s-a+f) - n = 2d(1-g) - n$, d'où le résultat.

3.4. *Exemple.* Dans le cas de 3.2.2, on a $g = g' = 0$, $n = d = 2$ et on vérifie que la formule est correcte.

3.4 Le genre d'une courbe algébrique plane

Soit X une courbe algébrique plane projective complexe lisse de degré d. C'est donc une surface compacte et on a la formule suivante :

3.5. Théorème. *Le genre de X est égal à* $g = \dfrac{(d-1)(d-2)}{2}\cdot$

Démonstration. Quitte à choisir convenablement le système d'axes on peut écrire l'équation de X sous la forme $(*)$ vue en 3.2.1 et on considère le revêtement ramifié de degré d défini par $p(x,y) = x$. La base B, qui est l'axe des x, est une droite projective, donc une sphère du point de vue topologique, donc de genre 0. Les points de ramification sont donnés par $\partial f/\partial y = 0$. (Si on a choisi convenablement les axes, il n'y a que deux des points qui coïncident au-dessus d'un tel point.) On compte ces points de X (ou de B) : ce sont les intersections de $f = 0$ et $\partial f/\partial y = 0$, par Bézout il y en a $d(d-1)$. On a donc, avec Hurwitz : $g' - 1 = -d + \dfrac{d(d-1)}{2}\cdot$ C'est le résultat attendu .

3.6. Corollaire. *La quartique de Klein est une surface de genre* 3 *donc un tore à 3 trous.*

C'est ce qu'on entrevoit sur la statue du MSRI.

4 La courbe de Klein vue comme polyèdre hyperbolique

4.1 Introduction

Voici la dernière apparition de la courbe (ou plutôt de la surface) de Klein, la plus belle peut-être, dans la mesure où l'on y voit explicitement les 168 symétries, les 24 points d'inflexion, les 56 contacts des bitangentes, etc. C'est celle qui permettra de comprendre, sur la statue du MSRI, non seulement les trous, mais aussi les lignes qui convergent trois à trois en certains points et le nom de Eightfold Way ! Le lecteur est averti que les preuves des assertions qui suivent vont être plus que sommaires. On le renvoie à la littérature et notamment au livre de R. et A. Douady, qui est très précis sur le sujet.

Jusqu'à présent nous avons construit des surfaces de deux manières : soit algébriquement, à partir de courbes algébriques complexes, soit topologiquement par des opérations de déformation et de recollement à partir de sphères. Dans ce qui suit nous utilisons une troisième méthode qui consiste à partir d'une surface connue (plan, disque, demi-plan, etc.) et à prendre le quotient de cette surface sous l'action d'un groupe. *Via* l'utilisation d'un domaine fondamental, cette opération va se ramener à identifier les bords d'un certain un polygone. C'est aussi la réalisation de ce qu'on appelle l'uniformisation de la surface : il s'agit de trouver une paramétrisation de K par une seule variable complexe.

4.2 Opération de groupe, domaine fondamental, quotient : le cas général

Considérons un groupe Γ opérant sur un ensemble X, non transitivement. On se reportera au paragraphe suivant pour l'étude de l'exemple d'un groupe discret d'isométries du plan euclidien. On s'intéresse aux orbites de Γ sur X. Le quotient X/Γ est l'ensemble[6] de ces orbites. Pour le décrire, on cherche ce qu'on appelle un domaine fondamental de X sous Γ, c'est-à-dire une partie D de X qui contienne un point et un seul de chaque orbite, donc qui soit en bijection avec X/Γ. Cela signifie encore qu'on a :

$$X = \bigcup_{g\in\Gamma} g(D) \quad \text{et} \quad g(D) \cap g'(D) = \emptyset \quad \text{pour } g \neq g'.$$

En fait, dans les cas topologiques usuels, on se contentera, à la place de la deuxième condition, de demander que $g(D)$ et $g'(D)$ n'aient pas de points communs intérieurs à D (on parlera de domaine fondamental au sens large).

Attention, si on a un domaine fondamental au sens large, il faut identifier les points du bord qui sont échangés par Γ.

[6]Attention, pour que le quotient d'une variété par un groupe en soit encore une, il est prudent de supposer que les éléments du groupe n'ont pas de points fixes ou alors seulement des points fixes isolés. Cela nous conduira à écarter les symétries axiales des groupes Γ.

Supposons en outre qu'on dispose d'un sous-groupe $\Lambda \subset \Gamma$. *A priori*, Λ opère moins transitivement que Γ, de sorte qu'un domaine fondamental D' de Λ va être plus grand qu'un domaine fondamental de Γ. Précisément, on a la formule $D' = \bigcup_{\overline{g} \in \Gamma/\Lambda} g(D)$ et si Λ est d'indice n dans Γ, D' est réunion de n transformés de D. De plus, si Λ est un sous-groupe distingué de Γ, le groupe quotient Γ/Λ opère sur X/Λ qui est donc naturellement muni d'un groupe d'automorphismes. C'est cette situation que nous allons tenter de réaliser ci-dessous.

4.3 Un exemple dans le plan euclidien

Considérons le pavage le plus simple du plan euclidien $P = \mathbf{R}^2$ par les carrés de côté 1, cf. figure 2. Ce pavage est évidemment invariant par les translations de vecteurs $m\vec{i} + n\vec{j}$ qui forment un groupe Λ, mais aussi par d'autres isométries directes[7] : les rotations de $k\pi/2$ autour des points du réseau et des centres des pavés. En tout, on a un groupe Γ dont Λ est un sous-groupe distingué. On remarque que le groupe total Γ est engendré par les rotations, associées au triangle $OA'B'$, d'angles doubles des angles du triangle : $\rho = \rho(O, \pi/2)$, $\sigma = \rho(A', \pi)$, $\tau = \rho(B', \pi/2)$ (d'ordres $4, 2, 4$). Le quotient Γ/Λ est le groupe cyclique d'ordre 4 formé des rotations (de centre O) d'angles $k\pi/2$.

On considère le quotient du plan par le sous-groupe Λ des translations. On a vu que cela revient à identifier deux points du plan s'ils sont échangés par un élément de Λ. Or, on a un domaine fondamental pour Λ : le carré $Q = OABC$ et le quotient s'obtient en identifiant les bords parallèles de Q. La réalisation pratique du quotient (qui passe par l'intermédiaire d'un cylindre) montre que ce quotient est un tore[8]. En fait, dans ce cas et dans de nombreux autres, on sait calculer le genre de la surface quotient :

4.1. Proposition. *Soit D un polygone plan convexe (euclidien, ou hyperbolique, ou ...) à $2n$ côtés. On suppose qu'on identifie les côtés de D deux à deux ainsi que certains sommets, de telle sorte qu'il ne reste que p sommets. Si le quotient obtenu est une surface compacte, sans bord et orientable, elle est de genre $g = \dfrac{n-p+1}{2}$.*

[7] Voir note ci-dessus pour comprendre l'élimination des réflexions.

[8] Si on quotiente en ajoutant une symétrie axiale, c'est-à-dire en recollant les bords en changeant de sens, on obtient la fameuse bouteille de Klein (non orientable).

Démonstration. On triangule le polygone D en prenant un point o intérieur à D et les $2n$ triangles de sommet o et de base les côtés. Il y a alors $f = 2n$ faces, $a = 4n$ arêtes et $s = 2n + 1$ sommets. On procède aux identifications. Il y a encore $f' = 2n$ faces, mais seulement $a' = 3n$ arêtes (les arêtes du bord sont identifiées deux à deux) et $s' = p + 1$ sommets (les p sommets qui subsistent sur le bord et le point o). On en déduit le genre annoncé.

4.2. *Exemple.* Dans le cas du carré ci-dessus, on a $n = 2$ et $p = 1$ d'où $g = 1$, comme attendu pour un tore.

Le fait que le pavage initial admette un groupe d'isométries Γ plus grand que Λ a deux conséquences :

• le domaine fondamental de Λ est réunion de 4 transformés du domaine fondamental $OA'B'C'$ de Γ, double du triangle $OA'B'$

• ce domaine fondamental (et donc aussi le quotient) admet pour groupe d'automorphismes $\Gamma/\Lambda = \mathbf{Z}/4\mathbf{Z}$.

On a construit ainsi une surface, P/Λ, homéomorphe à un tore et munie d'un groupe d'automorphismes à 4 éléments : le quotient $G = \Gamma/\Lambda$.

4.4 Position du problème dans le cas du groupe simple d'ordre 168

On veut maintenant obtenir la surface de Klein comme un quotient d'une surface X simple : plan, disque, demi-plan, etc. avec le groupe d'automorphismes G d'ordre 168 en évidence. L'idée est de procéder comme dans l'exemple précédent en exhibant un groupe Γ d'automorphismes de X, pas trop transitif (et pour cela on va le choisir discret) et un sous-groupe Λ de Γ avec un isomorphisme du quotient Γ/Λ sur G. Pour cela on se souvient des éléments ρ, σ, τ de G, d'ordre $7, 3, 2$. On va donc chercher un groupe Γ engendré par trois éléments d'ordre $7, 3, 2$ dont G sera quotient (cela signifie que certaines relations entre ρ, σ, τ présentes dans G ne seront pas dans Γ). Pour trouver des éléments de ces ordres, on pense aussitôt, comme pour le triangle $OA'B'$ ci-dessus, à des rotations d'angles $2\pi/7, 2\pi/3, \pi$.

Malheureusement on ne peut pas trouver un tel groupe Γ en géométrie euclidienne, au moins en dimension 2. En effet, les sous-groupes discrets du groupe des isométries du plan euclidien sont bien connus (ce sont les 17 groupes de pavages du plan) et on vérifie facilement que notre groupe G n'en est pas quotient (essentiellement parce qu'il n'y a pas d'éléments d'ordre 7).

En revanche on va trouver le groupe Γ comme sous-groupe du groupe des isométries du plan hyperbolique[9].

4.5 Le plan hyperbolique et ses isométries

On renvoie à [Perrin3] pour tout ce qui concerne ce sujet. On utilisera ici exclusivement comme modèle du plan hyperbolique le disque de Poincaré $\mathbf{D}$[10]. Il s'agit du disque unité ouvert du plan euclidien, qui joue le rôle de plan, le cercle, appelé horizon, servant d'infini, et les droites étant les arcs de cercles orthogonaux à l'horizon. On peut faire une bonne partie de la géométrie dans ce cadre. Les isométries de ce plan correspondent aux éléments de $O^+(q)$ où q est la forme de Lorentz $x^2+y^2-t^2$. On peut se laisser guider (dans certaines limites !) par l'intuition euclidienne : on a encore des symétries axiales, des symétries centrales, des rotations, des pseudo-translations, etc.

Quand on regarde les figures dans le plan hyperbolique (cf. figure 3), la première chose qui frappe c'est que les angles sont plus petits que dans le plan euclidien. Précisément, la somme des angles $\alpha+\beta+\gamma$ d'un triangle ne vaut pas π, mais est toujours plus petite que π et il existe des triangles d'angles α, β, γ dès qu'on a cette condition.

4.6 Le sous-groupe discret Γ de $O^+(q)$

On considère, dans $\mathbf{D}$, un triangle $T = aef$ tel que les trois angles de ce triangle[11] soient $\widehat{a} = \pi/7$, $\widehat{e} = \pi/3$ et $\widehat{f} = \pi/2$. Un tel triangle existe (cf. figure 4, on peut le prendre de la forme $a = (0,0,1)$, $e = (\alpha,0,1)$ et $f = (x,y,1)$) et il est unique à isométrie près (cf. [Perrin3]). On note alors ρ, σ' et τ' les rotations de centres respectifs[12] a, e, f et d'angles $2\pi/7$, $2\pi/3$

[9] Un grand théorème, dû à Köbe et Poincaré, montre que toute surface de Riemann, de genre ≥ 2, est un quotient du demi-plan de Poincaré et est donc, en particulier, munie d'une métrique hyperbolique.

[10] Je n'ai pas vérifié, mais il est bien possible que dans la première version de son article Klein ait travaillé dans ce qu'on appelle maintenant le disque de Klein $\mathbf{K}$, dans lequel les droites sont rectilignes, mais les angles non conformes, la figure à laquelle nous nous référerons est celle de ses œuvres complètes, cf. [Levy] ou [Bavard].

[11] Précisément, il existe des triangles rectangles d'angles $\pi/2$, π/d, π/n dès que $1/d+1/n$ est strictement plus petit que $1/2$ et un tel triangle donne naissance à un pavage par des polygones réguliers à n côtés, qui est tel que d polygones aboutissent en chaque sommet.

[12] Les éléments σ et τ vus dans les parties précédentes ne sont pas les images de τ' et σ', mais de rotations de mêmes angles et de centres différents.

et π (le double des angles du triangle). On a un lemme général dans cette situation :

4.3. Lemme. *On a* $\rho^7 = (\sigma')^3 = (\tau')^2 = \mathrm{Id}$. *Le produit* $\rho\sigma'\tau'$ *est l'identité.*

Démonstration. Les première relations sont évidentes. Pour montrer la formule $\rho\sigma'\tau' = \mathrm{Id}$, il suffit de décomposer chaque rotation en produit de deux symétries. Précisément, si on pose $A = (ef)$, $B = (fa)$ et $C = (ae)$, on a $\rho = \sigma_B\sigma_C$, $\sigma' = \sigma_C\sigma_A$, $\tau' = \sigma_A\sigma_B$ d'où le résultat.

4.4. Définition. *On appelle* $\Gamma = \Gamma_{2,3,7}$ *le sous-groupe de* $O^+(q)$ *engendré par les trois éléments* ρ, σ', τ' *(ou simplement par* ρ *et* τ'*).*

On considère les transformés des points a, e, f par les éléments de Γ. Sur la figure 6, les transformés de a sont en rouge, ceux de e en vert, ceux de f en noir. On considère aussi les transformés du triangle aef et du triangle double Q, réunion du triangle T et de son symétrique T' par rapport à (ae).

4.5. Proposition. *Le groupe* Γ *est un sous-groupe discret de* $O^+(q)$*. La réunion* Q *du triangle* T *et de son symétrique* T' *par rapport à* (ae) *est un domaine fondamental de* Γ *(au sens large), autrement dit, les transformés* $g(Q)$*, pour* $g \in \Gamma$*, pavent le plan hyperbolique* $\mathbf{D}$.

Démonstration. Une preuve rigoureuse n'est pas évidente, cf. [Douady] 6.10.2. Intuitivement, on vérifie ce résultat sur la figure 5. Une remarque essentielle : si on a une transformation de Γ (disons la rotation ρ de centre a et d'angle $2\pi/7$) et si l'élément g de Γ envoie a sur a', Γ contient $g\rho g^{-1}$ qui est la transformation de même nature autour de a' (ici la rotation d'angle $2\pi/7$). On obtient d'abord, en appliquant les rotations de centre a et d'angles $2k\pi/7$ un heptagone régulier (hyperbolique). Le point crucial est de noter que les angles de ces heptagones sont égaux à $2\pi/3$ (ou 120 degrés, au lieu de 128, 5 degrés pour l'heptagone euclidien) par construction. On obtient ensuite, par exemple, deux autres heptagones par rotation de $\pm 2\pi/3$ autour de $d = \tau'(e)$ et tous ces heptagones, réunis trois à trois en chaque sommet, pavent le plan hyperbolique.

4.6. *Remarque.* Une autre possibilité est sans doute de revenir au demi-plan de Poincaré $\mathbf{H}$, autre avatar du plan hyperbolique. Les rotations de $\mathbf{D}$ correspondent à des isométries de $\mathbf{H}$ qui sont des homographies de $PSL(2, \mathbf{R})$. Le groupe Γ est se voit alors comme un quotient du sous-groupe $PSL(2, \mathbf{Z})$ de $PSL(2, \mathbf{R})$. Le fait que le sous-groupe soit discret en résulte et le calcul du domaine fondamental aussi (cf. [Serre] ou [Bavard]).

4.7 Le sous-groupe Λ

Le groupe Γ, même s'il contient des éléments d'ordre $2, 3, 7$ n'est certainement pas notre groupe d'ordre 168 (c'est un groupe infini : il y a, par exemple, une infinité de rotations d'angles $2\pi/7$ dont les centres sont les centres des heptagones). Par ailleurs, G contient aussi des éléments d'ordre 4 (par exemple $\sigma\tau\rho$). En fait, on montre qu'il manque juste une relation de ce type dans Γ pour qu'il soit égal à G, précisément :

4.7. Proposition. *Soit $\gamma := \tau'\rho^3 \in \Gamma$. Le groupe simple d'ordre 168 est le quotient de Γ par le sous-groupe distingué Λ engendré par l'élément $\gamma^4 = (\tau'\rho^3)^4$ (autrement dit par γ^4 et ses conjugués).*

Démonstration. Cela résulte du fait qu'on a une présentation du groupe G comme groupe engendré par deux générateurs R et T vérifiant $R^7 = T^2 = (TR)^3 = (R^4T)^4 = \mathrm{Id}$ (cf. [Coxeter-Moser]).

Signalons au passage une écriture de γ^{-1} comme commutateur :

4.8. Proposition. *Si on pose $\tau'' = \rho^{-1}\tau'\rho$, on a $\gamma^{-1} = \rho^4\tau' = [\tau'', \sigma']$ où le crochet désigne le commutateur : $[\tau'', \sigma'] = \tau''\sigma'(\tau'')^{-1}(\sigma')^{-1}$.*

Démonstration. Comme on a $\sigma' = \rho^{-1}\tau'$ et $(\sigma')^{-1} = \tau'\rho$, on obtient :

$$[\tau'', \sigma'] = (\rho^{-1}\tau'\rho)(\rho^{-1}\tau')(\rho^{-1}\tau'\rho)(\tau'\rho) = \rho^{-2}\tau'\rho\tau'\rho = \rho^4\tau',$$

la dernière égalité venant de $\rho^7 = \mathrm{Id}$ et $(\tau'\rho)^3 = \mathrm{Id}$.

Pour décrire géométriquement $\gamma = \tau'\rho^3$, on décompose ρ^3 et τ' en produit de symétries. On a ainsi $\rho^3 = \sigma_{(af)}\sigma_{(aa')}$ et $\tau' = \sigma_{(ef)}\sigma_{(af)}$, d'où $\gamma = \sigma_{(ef)}\sigma_{(aa')}$. Comme ces droites hyperboliques (rouges) ne sont pas concourantes, γ est une "translation" hyperbolique Attention, ce mot doit être pris avec des précautions. En particulier une translation hyperbolique n'a qu'une droite stable qui est la perpendiculaire commune aux deux axes (la droite pointillée Δ de la figure 6). Elle stabilise aussi ce qu'on appelle les équidistantes à cette droite (les points situés à une distance donnée de la droite) qui sont des arcs de coniques. Sur la droite et les équidistantes, γ est effectivement une sorte de translation. Si on regarde l'effet de γ sur les points verts voisins de Δ, par exemple e, on peut encore décrire cette transformation comme la démarche de l'homme politique indécis : un coup à gauche, un coup à droite.

4.8 Le quotient de D par Λ

Comme dans l'exemple euclidien, il s'agit maintenant de décrire le quotient de **D** par le groupe[13] Λ, engendré par toutes les translations hyperboliques du type de γ^4. Cela signifie qu'on va identifier deux points s'ils sont transformés l'un en l'autre par γ^4 (l'homme politique qui change quatre fois d'opinion), comme les points verts e_0 et e_8 (les points verts sont les seuls bien visibles sur la statue du MSRI). Le chemin vert entre e_0 et e_8 est le fameux *eightfold way* le chemin à huit pas (une allusion au chemin des huit vertus vers le nirvana de la philosophie bouddhique[14]). On doit ensuite effectuer cette identification pour tous les conjugués de γ^4. Pour cela on construit (comme dans l'exemple euclidien) un domaine fondamental de Λ en réunissant les 168 transformés par (les représentants de) G du domaine fondamental de Γ. On obtient le polygone hyperbolique à 14 côtés de la figure de Klein, formé de $336 = 14 \times 24$ petits triangles transformés de T donc de 168 transformés de Q. Dans le quotient, en utilisant γ^4, on voit que les côtés de ce polygone sont identifiés deux à deux. Ainsi, le côté 1, qui contient e_0 est identifié au 6 qui contient e_8. Il y a aussi d'autres éléments d'ordre 4 : les $\gamma_i = \rho^i \gamma \rho^{-i}$. Comme les ρ^i envoient le côté 1 successivement sur les côtés d'indices impairs $3, 5, 7, 9, 11, 13$, γ_i envoie le côté $2i + 1$ sur le côté $2i + 6$ (modulo 14). On a donc ainsi la règle d'identification. On notera que deux sommets du polygone seulement survivent : l'un qui regroupe tous les ronds rouges et l'autre toutes les croix rouges.

4.9. *Remarque.* La statue du MSRI représente la surface de Klein et on y a dessiné, en creux, le pavage par les 24 heptagones réguliers obtenu ci-dessus. Sur le polygone fondamental les centres de ces polygones sont les 24 points correspondant aux inflexions, figurés en rouge et les sommets de ces heptagones sont les 56 points correspondant aux contacts des bitangentes, figurés en vert. Si l'on se promène de l'un à l'autre des points verts en suivant les arêtes (des heptagones) qui y passent, avec la règle suivante : à chaque carrefour (à trois branches) on tourne successivement à gauche, puis à droite, puis à gauche, puis à droite, etc., alors, partant de n'importe quel point, avec n'importe qu'elle arête initiale, quand on a parcouru 8 arêtes (en tenant compte des identifications des bords, évidemment), on revient à son point de départ : eightfold way est partout !

[13]On montre que ce groupe opère sans point fixe, cf. [Douady] 6.10.13

[14]Dans la philosophie bouddhique, le chemin des huit vertus, *aṣṭāṅgika-marga*, est la voie qui mène au nirvana, cf. [Kitagawa].

4.10. *Remarque.*
La contemplation de la figure 7 montre que les orbites des points de $\mathbf{D}/\Lambda$ sous l'action de G ont toutes 168 éléments, à l'exception de trois d'entre elles. Chacun des 336 triangles comporte un point rouge, un vert et un noir. Les points rouges, centres des rotations d'ordre 7, sont communs à 14 triangles et forment une orbite de cardinal 24, les points verts, d'ordre 3, communs à 6, une orbite de cardinal 56 et les points noirs, d'ordre 2, communs à 4, une orbite de cardinal 84.

4.11. Proposition. *La surface* $\mathbf{D}/\Lambda$ *est de genre* 3.

Démonstration. On regarde le polygone hyperbolique. Il a 14 côtés, identifiés deux à deux et il reste 2 sommets. En vertu de 4.1 on a donc $g = (7 - 2 + 1)/2 = 3$.

Une autre preuve consiste à utiliser le pavage par des heptagones (réunions de transformés de Q par les rotations ρ^i). C'est d'ailleurs ce pavage qui apparaît sur la statue. Ces heptagones ont des sommets verts, leurs centres sont rouges, les milieux de leurs arêtes sont noirs. On a donc un pavage avec $s = 56$, $a = 84$ et $f = 24$, donc $2 - 2g = 56 - 84 + 24 = -4$ et $g = 3$.

4.12. Théorème. *La surface* $\mathbf{D}/\Lambda$ *est la surface de Klein.*

Démonstration. C'est le point non évident de l'histoire. On montre d'abord que $X = \mathbf{D}/\Lambda$ est une surface de Riemann. Cela résulte du fait que c'est le quotient de la surface de Riemann $\mathbf{D}$ par le groupe Λ qui opére sans point fixe (ce n'est pas évident que Λ est sans point fixe, même si c'est clair pour son "générateur" γ^4 qui est une tranlation hyperbolique, cf. [Douady] 6.10.13). On prouve ensuite qu'elle est compacte (car elle admet un domaine fondamental au sens large qui l'est) et orientée (on a une structure complexe naturelle). Il en résulte que X est une courbe algébrique (c'est un théorème, pas du tout trivial, cf. [Reyssat ?] ! !). Elle est de genre 3 en vertu de 4.11. On sait alors (cf. [Hartshorne]) que X est soit hyperelliptique (i.e. qu'il existe un revêtement de degré 2 de la droite projective $p : X \to \mathbf{P}^1$), soit qu'elle est isomorphe à une courbe plane lisse de degré 4. Le premier cas est impossible car une courbe hyperelliptique admet un automorphisme d'ordre 2 qui est dans le centre du groupe des automorphismes, ce qui n'est pas le cas ici. La surface X admet donc un plongement dans $\mathbf{P}^2$ comme courbe de degré 4. On sait alors que X admet des points d'inflexions, en nombre ≤ 24. Comme l'image d'une inflexion par un automorphisme en est une autre, et que les orbites de G sur X sont de cardinal ≥ 24 (cf. 4.10), c'est qu'il y a exactement 24 inflexions qui forment une orbite et correspondent aux points d'ordre 7. Si l'on regarde le point central a, qui est une inflexion, son stabilisateur $< \rho >$ fixe aussi les inflexions b et c (les deux points subsistant sur le bord du polygone) et il ne fixe aucun autre point de X (vu les cardinaux des orbites il ne peut fixer que des inflexions et on voit qu'il n'y en a pas d'autre). Il en résulte que abc est un triangle d'inflexion (car l'autre point d'intersection de la tangente en a avec X est fixe par ρ lui aussi). Par ailleurs, il y a bien un élément d'ordre 3 qui permute abc. L'analyse conduite dans la partie 2 montre alors que la courbe admet l'équation attendue $X^3Y+Y^3T+T^3X=0$. On peut aussi (et Klein le fait dans son article) exhiber des fonctions x, y, t qui vérifient la bonne équation, à l'aide de la fonction modulaire η.

5 Références

[Bavard] Christophe Bavard, *La surface de Klein*, Journal de maths des élèves de l'ENS Lyon, Volume 1 (1993), numéro 1, www.umpa.ens-lyon.fr /JME/ Vol1Num1/artCBavard/artCBavard.pdf

[Coxeter-Moser] H.S.M. Coxeter and W.O.J. Moser *Generators and relations for discrete groups*, Springer, 1957.

[Douady] Régine et Adrien Douady, *Algèbre et théories galoisiennes, vol. II*, Cedic, 1979.

[Fischer] Gerd Fischer, *Plane algebraic curves*, AMS, 2001.

[Gramain] André Gramain, *Topologie des surfaces*, PUF, 1971.

[Hartshorne] Robin Hartshorne, *Algebraic Geometry*, Springer, 1977.

[Kitagawa] J.-M. Kitagawa *The eightfold path to Nirvana*, p. 88-101 of *Great religions in the world*, M. Severy ed., National Geographics Society, 1971.

[Klein] Felix Klein, *Über die Transformationen siebenter Ordnung der elliptischen Funktionen*, Math. Ann. **14** (1879), 428-471. Œuvres, Tome III, p. 90-136.

[Levy] Silvio Levy ed. *The eightfold way*, Cambridge University Press, 1999.

[Perrin1] Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996.

[Perrin2] Daniel Perrin, *Mathématiques d'École*, à paraître, Cassini.

[Perrin3] Daniel Perrin, *Géométrie projective, applications aux géométries euclidienne et non euclidiennes*, en préparation.

[Reyssat] Éric Reyssat, *Quelques aspects des surfaces de Riemann*, Birkhäuser, 1989.

[Serre] Jean-Pierre Serre, *Cours d'arithmétique*, PUF, 1970.

6 Annexes

6.1 Annexe 1 : un contre-exemple

Voici un exemple d'une quartique C, avec un automorphisme d'ordre 3, noté σ, et trois inflexions a, b, c échangées par σ, dans lequel les tangentes inflexionnelles ne sont pas les côtés du triangle abc.

On considère la courbe d'équation :

$$F(X,Y,T) = X^3Y - X^3T + Y^3T - Y^3X + T^3X - T^3Y$$
$$+B(X^2Y^2 + Y^2T^2 + T^2X^2 - 2X^2YT - 2Y^2TX - 2T^2XY).$$

Il est clair que C est invariante par la permutation des coordonnées $\sigma(x,y,t) = (y,t,x)$. Les points $a = (1,0,0)$, $b = (0,1,0)$ et $c = (0,0,1)$ sont permutés par σ. On considère le point $c = (0,0,1)$ et on l'étudie dans le plan affine $t = 1$. L'équation devient $f(x,y) = x - y + B(x-y)^2 + g(x,y)$ où g est formé de termes de degré ≥ 3. On a donc une inflexion, avec tangente $y = x$. Par permutation, les points a et b sont aussi des inflexions, mais les tangentes inflexionnelles ne sont sont pas les côtés du triangle $x = y = t = 0$ (ce sont les "bissectrices" $y = t$, $t = x$, $x = y$).

Pour $B = 3$ (et donc pour presque tout B) on vérifie que la courbe C est lisse (je l'ai fait à l'aide du logiciel Macaulay en calculant l'idéal engendré par les dérivées partielles de F).

(Peut-être une preuve utilisant l'action de σ : s'il y a un point singulier, il y en a trois, sauf si le point est fixe par σ. Mais $(1,1,1)$ n'est pas sur C et les autres $(1,j,j^2)$ et $(1,j^2,j)$ sont sur C mais n'annulent pas F'_X.)

6.2 Annexe 2 : le calcul de τ

6.2.1 Chercher τ

On se souvient que τ est l'avatar complexe de la symétrie d'axe Ox. Il normalise donc la rotation de $2\pi/3$, dans son nouvel habit, évidemment. Comme on a $\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ et $\tau\sigma\tau^{-1} = \sigma^2$, donc $\tau\sigma = \sigma^2\tau$ cela impose que τ est de la forme $\tau = \begin{pmatrix} \lambda & \mu & \nu \\ \mu & \nu & \lambda \\ \nu & \lambda & \mu \end{pmatrix}$. Si on écrit que τ est une involution, on obtient les deux relations $\lambda + \mu + \nu = \pm 1 := \epsilon$, $\mu\nu + \nu\lambda + \lambda\mu = 0$ et on a $\det \tau = 3\lambda\mu\nu - \lambda^3 - \mu^3 - \nu^3$. Si on écrit que τ conserve K, on obtient, en identifiant les termes en X^4 : $\lambda^3\mu + \mu^3\nu + \nu^3\lambda = 0$ et en identifiant ceux en X^3Y :

$$\lambda^3\nu + \mu^3\lambda + \nu^3\mu + 3(\mu^2\nu^2 + \nu^2\lambda^2 + \lambda^2\mu^2) = 1.$$

Or, en écrivant $(\lambda^2+\mu^2+\nu^2)(\mu\nu+\nu\lambda+\lambda\mu) = 0$ on trouve $\lambda^3\nu+\mu^3\lambda+\nu^3\mu = -\lambda\mu\nu$ et en calculant $(\mu\nu + \nu\lambda + \lambda\mu)^2 = 0$ on trouve $\mu^2\nu^2 + \nu^2\lambda^2 + \lambda^2\mu^2 + 2\lambda\mu\nu(\lambda + \mu + \nu) = 0$, d'où $\mu^2\nu^2 + \nu^2\lambda^2 + \lambda^2\mu^2 = -2\epsilon\lambda\mu\nu$. En définitive on a $-7\epsilon\lambda\mu\nu = 1$. On choisit $\epsilon = -1$ pour avoir $\det \tau = 1$. Il en résulte que λ, μ, ν sont les trois racines de l'équation $X^3 + X^2 - \frac{1}{7} = 0$.

6.1. *Remarque.* La relation $\lambda + \mu + \nu = -1$ montre que τ laisse stable la bitangente $X + Y + T = 0$.

6.2.2 Calculs dans $\mathbf{Q}(\zeta)$

Nous allons identifier l'équation précédente en termes de racines septièmes de l'unité.

Le groupe de Galois de l'extension $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ est le groupe $(\mathbf{Z}/7\mathbf{Z})^*$. Il contient deux sous-groupes, l'un d'ordre 3, qui correspond aux carrés de $\mathbf{Z}/7\mathbf{Z}$: $1, 2, 4$, l'autre d'ordre 2 : $\{1, -1\}$. Le corps fixe du premier est de degré 2 engendré par $\alpha = \zeta + \zeta^2 + \zeta^4$ (ou $\overline{\alpha} = \zeta^{-1} + \zeta^{-2} + \zeta^3$). On a $\alpha + \overline{\alpha} = -1$ et $\alpha\overline{\alpha} = 2$, de sorte que α et $\overline{\alpha}$ sont les racines de $x^2 + x + 2 = 0$. On a donc :

$$\alpha = \frac{-1 + i\sqrt{7}}{2} \quad \text{et} \quad \overline{\alpha} = \frac{-1 - i\sqrt{7}}{2}.$$

Le corps fixe du sous-groupe d'ordre 2 (engendré par la conjugaison complexe : $\zeta \mapsto \zeta^{-1} = \overline{\zeta}$) est de degré 3. Il contient les trois éléments :

$$\lambda' = \frac{i}{\sqrt{7}}(\zeta - \zeta^{-1}), \quad \mu' = \frac{i}{\sqrt{7}}(\zeta^2 - \zeta^{-2}), \quad \nu' = \frac{i}{\sqrt{7}}(\zeta^{-3} - \zeta^3),$$

permutés par le sous-groupe d'ordre 3. Ces nombres sont racines d'une équation de degré 3 à coefficients dans $\mathbf{Q}$ que l'on trouve en calculant : $\lambda'+\mu'+\nu' = -1$, $\mu'\nu' + \nu'\lambda' + \lambda'\mu' = 0$ et $\lambda'\mu'\nu' = \frac{1}{7}$. Ces nombres sont donc les racines de l'équation $X^3 + X^2 - \frac{1}{7} = 0$ et on a bien les valeurs de λ, μ, ν annoncées dans le texte.

6.3 Annexe 3 : les bitangentes

6.3.1 Quelques remarques

Le lemme suivant va permettre de tester si une droite est bitangente à une quartique :

6.2. Lemme. *Soit $P(X) = AX^4 + BX^3 + CX^2 + DX + E$ un polynôme à coefficients complexes. On suppose $A \neq 0$. Alors P est un carré dans $\mathbf{C}[X]$ si et seulement si on a les deux relations :*

$$4ABC = B^3 + 8A^2D \qquad \text{et} \qquad EB^2 = AD^2.$$

La condition est identique pour le polynôme homogénéisé $P^\sharp(X,T)$.

Démonstration. Si $P(X) = (uX^2+vX+w)^2 = Q(X)^2$ on vérifie les relations. Réciproquement, si on a les relations, on pose $u = \sqrt{A}$ et $w = \sqrt{E}$, le signe étant choisi pour avoir $\sqrt{A}\,D = \sqrt{E}\,B$. On prend alors $v = B/2\sqrt{A}$ et on vérifie qu'on a $P = Q^2$.

6.3. Corollaire. *Les droites $X + jY + j^2T$ et $X + j^2Y + jT$ ne sont pas bitangentes à K.*

Démonstration. On résout en X, par exemple $X = -jY - j^2T$ pour la première, et on reporte dans l'équation de K. On trouve :

$$Y^4 + (3j-1)Y^3T + 3j^2Y^2T^2 + (j+1)YT^3 + j^2T^4 = 0$$

et ce polynôme n'est pas un carré en vertu de ce qui précède.

6.3.2 Stabilisateur d'une bitangente

On considère la bitangente D d'équation $X + Y + T = 0$. On sait que son stabilisateur H contient le groupe à 6 éléments $<\sigma, \tau>$. Il est donc de cardinal multiple de 6. Par ailleurs, l'orbite de D contient les droites $\rho^i(D)$ pour $i = 0, \dots, 6$. Ces 7 droites sont distinctes. On peut le voir soit sur leurs équations (de la forme $\zeta^4 X + \zeta^2 Y + \zeta T = 0$), soit en notant que le stabilisateur de D sous $<\rho>$ est réduit à l'identité. Il en résulte que H peut être de cardinal $6, 12, 24$, l'orbite de D étant alors de cardinal $28, 14, 7$.

Si l'orbite n'avait que 7 éléments, elle contiendrait exactement les $\rho^i(D)$, pour $i = 0, 1, \dots, 6$. Or, elle contient aussi $\tau\rho(D)$ qui est la droite $uX + vY + wT$ avec $u = \lambda\zeta^4 + \mu\zeta^2 + \nu\zeta$, $v = \mu\zeta^4 + \nu\zeta^2 + \lambda\zeta$ et $w = \nu\zeta^4 + \lambda\zeta^2 + \mu\zeta$ (notations de 6.2.2). On vérifie que cette droite est différente des $\rho^i(D)$ (sinon le rapport u/v serait une racine septième de 1, or, à $\frac{i}{\sqrt{7}}$ près, on a $u = 2\zeta^{-2} - \zeta^3 - 1$ et $v = 2\zeta^{-1} - \zeta^{-2} - 1$ et on vérifie que le rapport n'est pas une racine septième de l'unité.

Le cas d'une orbite ω de 14 éléments est impossible. En effet, comme σ ne fixe que D, le groupe $<\sigma>$ découpe $\omega - \{D\}$ en orbites de 3 éléments, ce qui est absurde puisque 3 ne divise pas 13.

En conclusion, l'orbite de D est de cardinal 28, donc le stabilisateur est de cardinal 6. Il y a donc au moins 28 bitangentes à K.

6.3.3 Il y a au plus 28 bitangentes à K

Dans ce paragraphe on indique comment montrer ce résultat à la main, sans utiliser les formules de Plücker. On se place en un point $(a, b, 1)$ de la partie affine de K. On a donc $a^3 b + b^3 + a = 0$. On écrit la tangente D en ce point sous la forme $uX + vY + wT$ avec $u = 3a^2 b + 1$, $v = 3b^2 + a^3$ et $w = 2a - a^3 b = 3a + b^3$. On coupe K par D. L'équation aux x d'intersection est de la forme $(x - a)^2(Ax^2 + Bx + C) = 0$, avec $A = uv^2$, $B = wv^2 + u^3 + 2auv^2$ et $a^2 C = w^3$. Ces coefficients sont des polynômes en a, b de degrés respectifs 9, 10 et 10. Dire que D est une bitangente c'est dire que le discriminant $\Delta = B^2 - 4AC$ est nul. En homogénéisant, on trouve que les points de contacts des bitangentes sont donnés par deux équations homogènes en (a, b, c) : l'équation $F = 0$ de la quartique et le discriminant $\Delta = 0$. Comme Δ est de degré 20, il y a 80 points d'intersection. Mais, en regardant le point $(0, 0, 1)$, on s'aperçoit que les 24 inflexions sont aussi dans l'intersection de F et de Δ. Il reste donc 56 points d'intersections pour les vraies bitangentes : il y a donc (au plus)

28 bitangentes.

6.4 Annexe 4 : Un plongement dans $\mathfrak{S}_8$

Le groupe G opère sur les huit triangles d'inflexions de K. On peut préciser analytiquement ces triangles. Il y a d'abord le triangle de base $T_0 = abc = a_0b_0c_0$, puis son image par τ, avec les notations de la figure 6 il s'agit du triangle $T_5 = a_5b_5c_5$ formé du point $c_5 = \tau(a) = (\zeta-\zeta^{-1}, \zeta^2-\zeta^{-2}, \zeta^4-\zeta^3)$ et de ses permutés par σ : $a_5 = \tau(b)$ et $b_5 = \tau(c)$. On a ensuite les triangles images de T_5 par ρ^i avec $i = 1, \dots, 6$: T_6, T_7, T_1, T_2, T_3, T_4. Voici un point pour chaque cas : $c_6 = (\zeta^{-2}-\zeta^3, \zeta^4-1, \zeta^{-2}-\zeta^{-3})$, $c_7 = (\zeta^2-1, \zeta^{-1}-\zeta^2, \zeta^{-1}-\zeta^{-2})$, $c_1 = (\zeta^{-1}-\zeta^4, \zeta-\zeta^4, 1-\zeta^{-1})$, $c_2 = (\zeta^3-\zeta, \zeta^3-\zeta^{-1}, \zeta-1)$, $c_3 = (1-\zeta^{-2}, \zeta^{-2}-\zeta, \zeta^2-\zeta)$, $c_4 = (\zeta^4-\zeta^2, 1-\zeta^3, \zeta^3-\zeta^2)$.

On peut alors décrire les éléments de G en termes de permutations de ces huit triangles. On a ainsi :

$$\rho = (0)(1234567), \quad \tau = (05)(12)(36)(47), \quad \sigma = (0)(143)(267)(5)$$

et on en déduit que $\sigma\tau\rho = (0514)(2763)$ est d'ordre 4. (Car G s'injecte dans $\mathfrak{S}_8$ puisqu'il est simple.) On a encore :

$$\tau' = (01)(27)(34)(56), \quad \text{et} \quad \sigma' = (071)(264)(3)(5).$$

On en déduit notre fameux $\gamma = \tau'\rho = (0135)(2674)$.

6.4. *Remarque.* On peut aussi décrire les symétries axiales en termes de permutations : on a $\sigma_{(ae)} = (0)(4)(17)(26)(35)$, $\sigma_{(af)} = (0)(1)(27)(36)(45)$ et $\sigma_{(ef)} = (01)(2)(35)(46)(7)$. Cela permet de montrer que dans le groupe d'ordre 336 il y a d'autres éléments négatifs que les symétries axiales, par exemple $\sigma_{(ae)}\sigma_{(af)}\sigma_{(ef)} = (07634521)$ est un élément d'ordre 8.