

Autour du dernier Théorème de Fermat

Cours de Licence - Module OpA

Thomas Hausberger
mailto :hausberg@math.univ-montp2.fr

Table des matières

1	L'équation de Fermat	2
1.1	Un peu d'histoire : avant Fermat	2
1.2	Généralités	3
1.3	L'équation de Fermat de degré 1	3
1.4	L'équation de Fermat de degré 2 sur \mathbb{Z}	3
1.5	L'équation de Fermat de degré $n \geq 3$ sur $\mathbb{C}[t]$	5
1.6	L'équation de Fermat de degré 4 sur \mathbb{Z}	6
1.7	L'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés	6
1.8	L'anneau $\mathbb{Z}[j]$ et l'équation de Fermat de degré 3 sur \mathbb{Z}	9
2	Arithmétique des courbes elliptiques	12
2.1	Motivations	12
2.2	Courbes planes et singularité	13
2.3	Courbes elliptiques et loi de groupe	18
2.4	Points rationnels et théorème de Mordell	23
2.5	Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$	33
2.6	Courbes elliptiques et nombres congruents	35
2.7	Détermination de $E(\mathbb{Q})_{\text{tors}}$	39
A	Annexes au chapitre 1	43
A.1	Anneaux factoriels	43
A.2	Excursion au pays des corps de nombres	44
B	Annexes au chapitre deux	45
B.1	Le plan projectif	45
B.2	Les nombres p -adiques	47

1. L'équation de Fermat

1.1. Un peu d'histoire : avant Fermat

Fermat a écrit son «dernier théorème» dans une marge d'un exemplaire du traité «Arithmetica» de Diophante, un mathématicien de la Grèce antique, sur la page où était traitée l'équation $x^2 + y^2 = z^2$ dont on cherchait les solutions entières (de telles équations algébriques à coefficients entiers sont appelées de nos jours *équations diophantiennes*).

Une telle solution correspond aux longueurs des trois côtés d'un triangle rectangle (théorème de Pythagore, 572-492 avant J-C). Pythagore est parfois considéré comme le père de la «théorie des nombres» : il était fasciné par le mystère des nombres et a même proclamé que «tout est nombre». Il attachait beaucoup d'importance aux nombres rationnels (à cause de l'harmonie des sons obtenus à partir de cordes vibrantes dont le rapport des longueurs est rationnel), mais a également découvert l'existence des nombres irrationnels (ce fut un choc !)

Les «Elements» d'Euclide est un traité écrit au III^e siècle avant J-C qui résume les résultats des mathématiciens grecques. On y trouve par exemple une preuve de l'existence d'une infinité de nombres premiers ; y est également abordée la question de la «construction de \mathbb{R} à partir de \mathbb{Q} », problème que n'a pas su résoudre Pythagore. Mais il faut attendre le XIX^e siècle pour qu'une réponse complète soit donnée. Il y a environ 100 ans, utilisant la même construction que celle de \mathbb{R} naquirent également les nombres p -adiques (les éléments du corps \mathbb{Q}_p), ravivant la question «que sont les nombres?» Le monde p -adique, bien que très différent du monde des nombres réels, s'avère en fait aussi naturel et d'égale importance que ce dernier. On a :

$$\mathbb{Q}_p \supset \mathbb{Q} \subset \mathbb{R}.$$

Diophante était un mathématicien du III^e siècle après J-C (époque romaine, fin de la Grèce antique), disciple de l'école grecque. Après lui, le développement de la théorie des nombre s'essouffla, jusqu'à la renaissance où son traité fut republié et parvint dans les mains de Fermat.

Fermat était juriste à Toulouse ; il a travaillé sur les équations des figures géométriques telles que l'ellipse et développé des outils d'analyse de fonctions, mais a également établi des résultats importants en théorie des nombres. Il est considéré comme le plus grand mathématicien du XV^e siècle.

Fermat a laissé 48 commentaires dans les marges de son exemplaire d'Arithmetica. Ils furent publiés par son fils après sa mort. Bien que Fermat avait affirmé avoir démontré un certain nombre des propositions qu'il énonçait, il en écrivait rarement une preuve. Ses contemporains s'efforcèrent de combler cette lacune ; les problèmes de Fermat s'avèrent être le dessus de l'iceberg de mathématiques profondes.

En particulier, le «dernier théorème de Fermat» concerne l'équation $x^n + y^n = z^n$, dont Fermat mentionne le cas $n \geq 5$ uniquement dans Arithmetica. On pense que Fermat a affirmé à tort en avoir une preuve, vu l'ardeur qui fut nécessaire à la communauté mathématique toute entière pour en donner une démonstration et qui culmina avec les travaux de Wiles en 1993.

1.2. Généralités

Il s'agit donc de l'équation

$$x^n + y^n = z^n,$$

où $n \geq 1$ est entier et le problème qui se pose est de trouver, pour n donné, toutes les solutions entières de cette équation, c'est-à-dire tous les triplets $(a, b, c) \in \mathbb{Z}^3$ tels que $a^n + b^n = c^n$.

Remarquons que ce problème garde un sens si l'on remplace \mathbb{Z} par n'importe quel anneau (qui sera pour nous, sauf mention explicite du contraire, commutatif et unitaire) : en effet, les solutions dans A^3 sont les racines dans A^3 du polynôme $x^n + y^n - z^n$ (l'évaluation a un sens dans A^3 car ce polynôme est à coefficients entiers). Plus tard, nous considérerons l'anneau $\mathbb{C}[t]$. D'autre part, si $\phi : A \rightarrow B$ est un morphisme d'anneaux et (a, b, c) une solution dans A^3 , alors $(\phi(a), \phi(b), \phi(c))$ est une solution dans B^3 . Cette propriété est également vraie pour tout système d'équations polynômiales à coefficients dans \mathbb{Z} .

Une autre propriété importante est la suivante : l'équation de Fermat est *homogène*, c'est-à-dire tous les monômes intervenant sont de même degré. Cela se traduit par la caractérisation suivante : si A est un anneau, $(a, b, c) \in A^3$ et $\lambda \in A$ non diviseur de zéro, alors (a, b, c) est une solution si et seulement si $(\lambda a, \lambda b, \lambda c)$ l'est. Géométriquement, cela s'exprime en disant que l'ensemble des solutions est un cône ; la propriété pour (a, b, c) d'être solution (au moins pour A un anneau intègre) ne dépend que de la droite passant par l'origine et (a, b, c) , donc de l'image de (a, b, c) dans le plan projectif $\mathbb{P}(A^3)$. L'intérêt de considérer les solutions dans l'espace projectif est que la dimension du problème (c'est-à-dire le nombre de variables) se trouve abaissé d'une unité.

Pour en revenir aux solutions entières, un triplet (a, b, c) sera dit *primitif* s'il vérifie $\text{pgcd}(a, b, c) = 1$. L'équation de Fermat étant homogène, il suffit de déterminer les triplets primitifs : en effet, tout triplet (a, b, c) solution s'écrit $d(a', b', c')$, où d est un pgcd de a , b et c et (a', b', c') est un triplet primitif solution de l'équation.

1.3. L'équation de Fermat de degré 1

Pour A n'importe quel anneau, nous avons une bijection de A^2 vers l'ensemble des solutions de $x + y = z$, qui envoie (a, b) sur $(a, b, a + b)$.

1.4. L'équation de Fermat de degré 2 sur \mathbb{Z}

Il s'agit de $x^2 + y^2 = z^2$; nous suivons [Sa] §1.2.

Les solutions (a, b, c) avec a , b et c des entiers positifs et abc non nuls sont appelés des *triplets pythagoriciens*.

- Première réduction : comme $(a, b, c) \in \mathbb{Z}^3$ est solution si et seulement si tous les triplets $(\pm a, \pm b, \pm c)$ sont des solutions, il suffit de déterminer les solutions dans \mathbb{N}^3 .
- Seconde réduction : comme l'équation est homogène, toute solution (a, b, c) dans \mathbb{N}^3 avec $abc \neq 0$ est de la forme (da', db', dc') , avec d dans \mathbb{N} non nul et (a', b', c') un triplet pythagorien *primitif*.

Nous allons classifier les triplets pythagoriciens primitifs, à l'aide de la *factorialité de l'anneau* \mathbb{Z} (voir A.1). On procède par étape :

1. Soit (a, b, c) un triplet pythagoricien ; les conditions suivantes sont équivalentes :
 - (a) $\text{pgcd}(a, b, c) = 1$
 - (b) $\text{pgcd}(a, b) = 1$
 - (c) $\text{pgcd}(a, c) = 1$
 - (d) $\text{pgcd}(b, c) = 1$
2. Soit (a, b, c) un triplet pythagoricien primitif. Alors c est impair, et l'un d'entre a et b est pair (considérer les carrés dans $\mathbb{Z}/4\mathbb{Z}$, qui sont 0 et 1)
3. Soit (a, b, c) un triplet pythagoricien primitif avec b pair. En écrivant

$$(b/2)^2 = ((c - a)/2)((c + a)/2),$$

on montre qu'il existe u et v dans \mathbb{N} , premiers entre eux, tel que $0 < u < v$, $(c - a)/2 = u^2$ et $(c + a)/2 = v^2$ (en effet, $(c - a)/2$ et $(c + a)/2$ sont premiers entre eux car tout diviseur commun divise leur somme et leur différence, soit c et a , qui sont premiers entre eux)

4. On conclut que les triplets pythagoriciens primitifs avec b pair sont les triplets $(v^2 - u^2, 2uv, v^2 + u^2)$, avec $0 < u < v$ premiers entre eux et l'un des deux pairs (sinon c serait pair).

Une autre façon de déterminer les triplets pythagoriciens utilise la *paramétrisation rationnelle du cercle* : à un triplet pythagoricien (a, b, c) on fait correspondre le point $(a/c, b/c)$ du cercle unité C de \mathbb{R}^2 . Un point du cercle est dit rationnel si ses deux coordonnées sont rationnelles. En considérant les droites passant par $(-1, 0)$, on montre que tout autre point rationnel de C est de la forme

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right),$$

le paramètre rationnel t étant la pente de la droite considérée.

En effet, notons $D_t : y = t(x + 1)$ cette droite, pour $t \in \mathbb{R}$, et $M(t) = (x(t), y(t))$ le deuxième point d'intersection de D_t avec le cercle $C : x^2 + y^2 = 1$. Alors t est rationnel si et seulement si $M(t)$ l'est :

- Si $M(t)$ est rationnel, la droite D_t contient deux points rationnels, donc sa pente est rationnelle
- Réciproquement, si $t \in \mathbb{Q}$, alors $x(t)$ est solution d'une équation de degré 2 à coefficients dans \mathbb{Q} , dont l'une des solutions $(-1, 0)$ est à la fois sur la droite et le cercle) est rationnelle. En résolvant cette équation, on trouve les formules données.

Enfin, écrivant $t = u/v$, avec u et v premiers entre eux, on trouve $a/c = \frac{v^2 - u^2}{v^2 + u^2}$ et $b/c = \frac{2uv}{v^2 + u^2}$. Si $a > 0$, alors $v > u$ et si b est pair et le triplet primitif, on retrouve le fait que l'un parmi u et v est pair et $(a, b, c) = (v^2 - u^2, 2uv, v^2 + u^2)$.

1.5. L'équation de Fermat de degré $n \geq 3$ sur $\mathbb{C}[t]$

En 1993, Andrew Wiles a montré qu'il n'y a pas de solution non triviale dans \mathbb{Z}^3 ; la démonstration est très difficile, comparé au cas de $\mathbb{C}[t]$, qui est plus qu'abordable :

Théorème 1.5.1. *Soit $n \geq 3$ un entier. Si a, b et c dans $\mathbb{C}[t]$ satisfont à $a^n + b^n = c^n$ et sont premiers entre eux (i.e. $\text{pgcd}(a, b, c) \sim 1$, alors a, b et c sont de degré zéro, c'est-à-dire sont dans \mathbb{C} .*

La preuve utilise la *méthode de descente* (de Fermat) :

Supposons donc qu'il existe au moins une solution primitive non constante. Soit alors (a, b, c) une solution où le maximum des degrés de a, b et c est *minimal*. Tout d'abord, notons que a, b et c sont premiers entre eux deux par deux, tous non nuls, et qu'au plus l'un d'entre eux est constant. On a :

$$a^n = c^n - b^n = \prod_{\zeta^n=1} (c - \zeta b).$$

Les facteurs $c - \zeta b$ sont premiers deux à deux; en effet, si un premier $p \in \mathbb{C}[t]$ divise $x_i = c - \zeta_i b, i = 1, 2$, alors il divise $x_1 - x_2$ et $\zeta_2 x_1 - \zeta_1 x_2$, donc c et b , qui sont premiers entre eux. D'autre part, par la factorialité de $\mathbb{C}[t]$, nous obtenons que les $c - \zeta b$ sont des puissances n èmes, à des inversibles près. Mais les inversibles sont les constantes non nulles, qui sont elle-mêmes des puissances n èmes. Finalement, il existe des x_ζ dans $\mathbb{C}[t]$ tels que $c - \zeta b = x_\zeta^n$.

Comme les $c - \zeta b$ sont premiers entre eux deux à deux, les x_ζ le sont également; de plus, au plus l'un des x_ζ est constant (considérer les coefficients dominants de c et b). Comme $n \geq 3$, il est possible de choisir un triplet (x, y, z) d'éléments x_ζ . Comme x^n, y^n et z^n appartiennent au sous- \mathbb{C} -espace vectoriel de $\mathbb{C}[t]$ engendré par b et c (qui est de dimension 2, car b et c sont premiers entre eux, donc linéairement indépendants sur \mathbb{C}), il y a une relation linéaire non triviale que l'on peut écrire :

$$\alpha x^n + \beta y^n = \gamma z^n,$$

avec α, β et γ dans \mathbb{C} non tous nuls.

Finalement, on peut écrire

$$x_1^n + y_1^n = z_1^n,$$

avec x_1, y_1 et z_1 premiers entre eux deux à deux, non tous constants, et de même degrés respectifs que x, y et z . Mais cela contredit la minimalité en terme des degrés de la solution (a, b, c) de départ.

Remarque. On a utilisé le fait que l'anneau $\mathbb{C}[t]$ est factoriel et que tout inversible de $\mathbb{C}[t]$ est une puissance n ème. Ce sont exactement ces deux propriétés qui posent un problème pour les anneaux $\mathbb{Z}[e^{2i\pi/n}]$. Kummer a réussi à remédier au défaut de factorialité de ces anneaux, en découvrant qu'il existe une «factorisation en idéaux premiers» qui remplace la factorisation en nombres premiers. Sa découverte a ouvert la voie de la «théorie algébrique des nombres» (l'étude des anneaux tels que $\mathbb{Z}[e^{2i\pi/n}]$, des extensions finies de \mathbb{Q} ; voir [Sa]) et il a réussi ainsi à démontrer le théorème de Fermat pour un certain nombre d'entiers n . Signalons aussi que la méthode de Wiles ne repose pas sur l'étude des anneaux $\mathbb{Z}[e^{2i\pi/n}]$, mais plutôt des anneaux de la forme $\mathbb{Z}[x, y]/(y^2 = x^3 + ax + b)$, c'est-à-dire associés à des courbes elliptiques.

1.6. L'équation de Fermat de degré 4 sur \mathbb{Z}

Nous suivons [Sa] §1.2 et démontrons d'abord :

Proposition 1.6.1. *Soient x, y et z dans \mathbb{Z} tels que $x^4 + y^4 = z^2$. Alors $xyz = 0$.*

La clef est de nouveau un *argument de descente* :

Par l'absurde, supposons qu'il existe (x, y, z) dans \mathbb{N}^3 avec $x^4 + y^4 = z^2$, $xyz \neq 0$ et z minimal. Alors x, y et z sont premiers entre eux (sinon on pourrait écrire $(\frac{x}{d})^4 + (\frac{y}{d})^4 = (\frac{z}{d^2})^2$). Pour obtenir une contradiction, on procède comme suit, en appliquant ce que nous savons déjà des triplets pythagoriciens :

- après permutation, si nécessaire, de x et y , on a x et z impairs, y pair. Il existe u et v dans \mathbb{N} , premiers entre deux, avec $u > v$, tels que :

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad z = u^2 + v^2.$$

- la première équation dit que $x^2 + v^2 = u^2$; comme x est impair, $v = 2v_1$ est pair ; la seconde équation dit que $(y/2)^2 = uv_1$, donc il existe a et b dans \mathbb{N} tels que $u = a^2$ et $v_1 = b^2$.
- de la première équation, on déduit qu'il existe c et d dans \mathbb{N} , premiers entre eux, tels que :

$$x = c^2 - d^2, \quad v = 2cd, \quad u = c^2 + d^2.$$

- la deuxième de ces nouvelles équations dit que $b^2 = cd$, donc que c et d sont des carrés, disons $c = e^2$ et $d = f^2$ avec e et f dans \mathbb{N} . Comme $u = a^2$, on a :

$$e^4 + f^4 = a^2,$$

et comme $a^2 = u$ et $z > u^2$, on a $z > u^2 \geq a^4 \geq a$, ce qui contredit la minimalité de z .

Corollaire. *L'équation $x^4 + y^4 = z^4$ n'a pas de solution en entiers $x, y, z \geq 1$.*

1.7. L'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés

La proposition suivante figure parmi les commentaires laissés par Fermat dans les marges de son exemplaire d'«Arithmetica» :

Proposition 1.7.1. *Soit p un nombre premier vérifiant $p \equiv 1 \pmod{4}$. Alors il existe un triangle rectangle dont l'hypothénuse est de longueur p . Inversement, il n'existe pas de tel triangle rectangle si $p \equiv 3 \pmod{4}$.*

Fermat a été le premier à découvrir de telles relations entre nombre premiers et triangles rectangles, dont le résultat :

Proposition 1.7.2. *Si p est un nombre premier vérifiant $p \equiv 1 \pmod{4}$, alors il existe des entiers naturels x et y tels que $p = x^2 + y^2$. Réciproquement, cette équation n'admet pas de solution en entiers si $p \equiv 3 \pmod{4}$.*

On peut voir en ces deux résultats les préludes de la «théorie du corps de classes» qui est une des plus belles théories mathématiques du XX^e siècle. Disons de manière vague que cette théorie établie une correspondance entre les corps de nombres (voir l'annexe A.2) et la factorisation des nombres premiers. La manière dont on démontre ces deux propositions de nos jours passe par l'anneau $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$; la clef est alors la décomposition de p en irréductibles dans $\mathbb{Z}[i]$, cette factorisation étant déterminée par la congruence modulo 4.

$$\begin{aligned} 5 &= 2^2 + 1^2 = (2 + i)(2 - i) ; & 13 &= 3^2 + 2^2 = (3 + 2i)(3 - 2i) \\ 5^2 &= (2 + i)^2(2 - i)^2 = (3 + 4i)(3 - 4i) = 3^2 + 4^2 \\ 13^2 &= (3 + 2i)^2(3 - 2i)^2 = (5 + 12i)(5 - 12i) = 5^2 + 12^2 \end{aligned}$$

Rappelons que :

Proposition 1.7.3. *La conjugaison complexe $z \mapsto \bar{z}$ induit sur $\mathbb{Z}[i]$ un automorphisme d'anneau. L'application $N : \mathbb{Z}[i] \rightarrow \mathbb{N}$, $a \mapsto a\bar{a} = |a|^2$ est multiplicative et s'appelle la norme de la \mathbb{Z} -algèbre $\mathbb{Z}[i]$. L'anneau $\mathbb{Z}[i]$ est Euclidien pour le stathme N (donc factoriel). Le groupe $\mathbb{Z}[i]^\times$ de ses éléments inversibles est $\{\pm 1, \pm i\}$ (éléments de norme 1).*

Un autre résultat déjà rencontré que nous utiliserons est le suivant :

Proposition 1.7.4. *Soit p un nombre premier impair ; alors (-1) est un carré modulo p si et seulement si $p \equiv 1 \pmod{4}$.*

Cela résulte de la proposition suivante, concernant les carrés modulo p :

Proposition 1.7.5. *Soit p un nombre premier impair. Les carrés $\mathbb{F}_p^{\times 2} \subset \mathbb{F}_p^\times$ constituent un sous-groupe d'indice 2. C'est aussi le noyau du morphisme $\Psi : x \mapsto x^{\frac{p-1}{2}}$, lequel a pour image $\{\pm 1\}$.*

En effet, $\mathbb{F}_p^{\times 2}$ est l'image du morphisme $\mathbb{F}_p^\times \ni x \mapsto x^2$, lequel a pour noyau $\{\pm 1\}$. Cela montre que $\text{Card } \mathbb{F}_p^{\times 2} = (p-1)/2$. Par conséquent, $\mathbb{F}_p^{\times 2} \subset \ker \Psi$. Comme $\ker \Psi$ est de cardinal au plus $(p-1)/2$ (car le polynôme $t^{\frac{p-1}{2}} - 1$ a au plus $(p-1)/2$ racines dans le corps \mathbb{F}_p), c'est une égalité. Enfin, $\text{Im } \Psi \subset \{\pm 1\}$ car $y = x^{\frac{p-1}{2}}$ vérifie $y^2 = 1$; c'est une égalité car $\text{Card Im } \Psi = \text{Card } \mathbb{F}_p^\times / \text{Card } \ker \Psi = 2$.

Remarque. Si $x \in \mathbb{F}_p^\times$, on définit

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{si } x \in \mathbb{F}_p^{\times 2}; \\ -1 & \text{sinon.} \end{cases}$$

Il s'agit du «symbole de Legendre». Comme $\left(\frac{x}{p}\right) = \Psi(x)$, c'est un morphisme $\left(\frac{\bullet}{p}\right) : \mathbb{F}_p^\times \rightarrow \{\pm 1\}$: en effet, l'application composée

$$\mathbb{F}_p^\times \xrightarrow{\left(\frac{\bullet}{p}\right)} \{\pm 1\} \xrightarrow{\sim} \{\pm i\}$$

est le morphisme Ψ . Si $x \in \mathbb{Z}$ est premier avec p , on note par définition $\left(\frac{x}{p}\right) = \left(\frac{\dot{x}}{p}\right)$ (et pose souvent $\left(\frac{x}{p}\right) = 0$ si $p \mid x$, par convention).

Avec ces notations, on a donc :

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{si } p \equiv 1 \pmod{4}; \\ -1 & \text{si } p \equiv -1 \pmod{4}. \end{cases}$$

En TD, vous allez voir que :

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod{8}; \\ -1 & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Le symbole de Legendre se calcule alors facilement pour tout entier x , à partir des formules précédentes et de la «loi de réciprocité quadratique» :

Théorème 1.7.1. Soient p et q deux nombres premiers impairs. On a

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

(exercice : calculer $\left(\frac{3871}{65537}\right)$)

Vous en verrez une preuve en TD (voir également [Sa], [Se]) ; cette loi de réciprocité se généralise dans le cadre de la théorie du corps de classe (DEA).

Prouvons maintenant la proposition 1.7.2 :

- Soit $p \equiv 1 \pmod{4}$ un nombre premier. Comme $\left(\frac{-1}{p}\right) = +1$, il existe un entier a tel que $a^2 \equiv -1 \pmod{p}$. Alors p n'est pas premier dans $\mathbb{Z}[i]$: en effet, p divise $a^2 + 1 = (a + i)(a - i)$, mais p ne divise ni $a + i$ ni $a - i$.
- p n'est donc pas irréductible ; il s'écrit donc $p = \alpha\beta$, avec α premier dans $\mathbb{Z}[i]$ et $\beta \notin \mathbb{Z}[i]^\times$. On obtient donc $N(p) = N(\alpha)N(\beta)$; comme $N(\alpha) \neq 1$ et $N(\beta) \neq 1$ (puisque ce ne sont pas des unités), nécessairement $N(\alpha) = p$, donc $p = \alpha\bar{\alpha}$. En écrivant $\alpha = c + id$, on voit que p est somme de deux carrés.
- Réciproquement, si $p = c^2 + d^2$, alors $-c^2 \equiv d^2 \pmod{p}$, donc -1 est un carré modulo p (d n'est pas divisible par p , donc est inversible modulo p). On en déduit que $p \equiv 1 \pmod{4}$.

Remarque. Pour 2, on a $2 = (1 + i)(1 - i) = i(1 - i)^2$. On a vu que si $p \equiv -1 \pmod{4}$, alors p reste irréductible dans $\mathbb{Z}[i]$, et si $p \equiv 1 \pmod{4}$, alors $p = \alpha\bar{\alpha}$ est produit de deux irréductibles conjugués de $\mathbb{Z}[i]$. Les irréductibles de $\mathbb{Z}[i]$ sont donc les nombres premiers p tels que $p \equiv -1 \pmod{4}$ et les $\alpha = a + ib$, où $p = a^2 + b^2$ est un nombre premier (nécessairement pair ou $\equiv 1 \pmod{4}$). En effet, si $\beta \in \mathbb{Z}[i]$ est irréductible, on décompose $\beta\bar{\beta} = N(\beta) \in \mathbb{N}$ en facteurs premiers dans \mathbb{Z} , puis applique ce que l'on sait de la décomposition des nombres premiers ; β sera un facteur irréductible du produit, donc de la forme précédente.

Remarque. Vous verrez en TD un algorithme relativement efficace pour trouver une factorisation dans $\mathbb{Z}[i]$ d'un nombre premier $p \equiv 1 \pmod{4}$. Cet algorithme assez simple utilise le fait que l'anneau $\mathbb{Z}[i]$ est Euclidien et qu'il est engendré par une racine de l'unité d'ordre 4.

Prouvons enfin la proposition 1.7.1 :

- Si $p \equiv 1 \pmod{4}$, on écrit $p = \alpha\bar{\alpha}$. Alors $p^2 = \beta\bar{\beta}$, où $\beta = \alpha^2 = c + id$, donc $p^2 = c^2 + d^2$ est somme de deux carrés. Il faut montrer que ces carrés sont non nuls, autrement dit que $\beta \notin \mathbb{Z} \cup i\mathbb{Z}$. Si tel était le cas, α aurait comme argument un multiple de $\pi/4$, donc s'écrirait $\alpha = r\gamma$, où $r \in \mathbb{Z}$ et $\gamma \in \{1, 1+i, i, -1+i\}$; on aurait $p = N(\alpha) = r^2 N(\gamma)$, d'où $r = \pm 1$ puis $p = 2$, ce qui est absurde.
- Si $p \equiv -1 \pmod{4}$ et $p^2 = c^2 + d^2 = (c+id)(c-id)$, l'unicité de la décomposition en irréductibles implique que $c+id = \pm p$ ou $\pm ip$, donc $c = 0$ ou $d = 0$.
- Par soucis d'exhaustivité, le cas $p = 2$: on voit facilement que $2^2 = c^2 + d^2$ n'admet pas de solution en entiers avec $c \neq 0$ et $d \neq 0$

Remarque. Dans la même veine :

Proposition 1.7.6. Si p est un nombre premier vérifiant $p \equiv \pm 1 \pmod{8}$, alors il existe des entiers naturels x et y tels que $p = x^2 - 2y^2$. Réciproquement, cette équation n'admet pas de solution en entiers si $p \equiv \pm 3 \pmod{8}$.

Ce résultat se démontre en travaillant dans $\mathbb{Z}[\sqrt{2}]$. Il est à mettre en relation avec le tableau suivant :

corps de nombres	premiers qui se décomposent
$\mathbb{Q}(\sqrt{-1})$	$p \equiv 1 \pmod{4}$
$\mathbb{Q}(\sqrt{-2})$	$p \equiv 1, 3 \pmod{8}$
$\mathbb{Q}(\sqrt{-3})$	$p \equiv 1 \pmod{3}$
$\mathbb{Q}(\sqrt{2})$	$p \equiv \pm 1 \pmod{8}$

Remarque. Concernant la décomposition d'un entier naturel en somme de carrés :

Corollaire. Soit $n \in \mathbb{N}$; alors n s'écrit comme somme de deux carrés si et seulement si $v_p(n)$ est pair pour tout nombre premier $p \equiv -1 \pmod{4}$.

En effet, si $n = a^2 + b^2$, alors $n = \alpha\bar{\alpha}$, avec $\alpha = a + ib$. Soit $p \equiv -1 \pmod{4}$ un nombre premier, donc irréductible dans $\mathbb{Z}[i]$; on écrit $\alpha = p^v \beta$, où $v = v_p(\alpha)$ et β est premier avec p dans $\mathbb{Z}[i]$. Alors $\bar{\alpha} = p^v \bar{\beta}$, puis $n = p^{2v} \beta\bar{\beta}$, où p ne divise pas $\beta\bar{\beta}$ dans $\mathbb{Z}[i]$ donc dans \mathbb{Z} . Réciproquement, si n vérifie la condition du corollaire, écrivant $p = (a_p + ib_p)(a_p - ib_p)$ pour un premier $p \equiv 1 \pmod{4}$, on a $n = \alpha\bar{\alpha}$, où

$$\alpha = (1+i)^{v_2(n)} \prod_{p \equiv 1 \pmod{4}} (a_p + ib_p)^{v_p(n)} \prod_{p \equiv -1 \pmod{4}} p^{\frac{v_p(n)}{2}}.$$

Enfin, citons le résultat suivant (preuve du même tonneau, mais on remplace $\mathbb{Z}[i]$ par l'anneau des quaternions d'Hurwitz; voir par exemple [Sa] §5.7) :

Théorème 1.7.2 (Lagrange). Tout n dans \mathbb{N} est somme de quatre carrés.

1.8. L'anneau $\mathbb{Z}[j]$ et l'équation de Fermat de degré 3 sur \mathbb{Z}

Nous allons travailler dans le sous-anneau $A = \mathbb{Z}[j]$, avec $1 + j + j^2 = 0$, de \mathbb{C} . La méthode est toujours la même : factorisation après adjonction des racines troisième de l'unité, et descente infinie. Pour l'argument de descente, il est nécessaire de démontrer un résultat légèrement plus fort :

Proposition 1.8.1. *Supposons que x, y et z sont dans A et u dans A^\times tels que $x^3 + y^3 = uz^3$. Alors $xyz = 0$.*

Corollaire. *L'équation $x^3 + y^3 = z^3$ ne possède pas de solution non triviale (i.e. telle que $xyz \neq 0$) en entiers x, y, z .*

Commençons par quelques préliminaires sur l'anneau A :

Proposition 1.8.2. *La conjugaison complexe $z \mapsto \bar{z}$ induit sur A un automorphisme d'anneau. L'application $N : A \ni a \mapsto a\bar{a} = |a|^2 \in \mathbb{N}$ est multiplicative et s'appelle la norme de la \mathbb{Z} -algèbre A . L'anneau A est Euclidien pour le stathme N . Le groupe A^\times des éléments inversibles est $\{\pm 1, \pm j, \pm j^2\}$. L'élément $\lambda = 1 - j$ de A est premier, et le quotient $A/\lambda A$ est un corps à trois éléments. Dans A , 3 se factorise en $3 = -j^2\lambda^2$.*

Remarque. $t^2 + t + 1$ est le polynôme minimal de j sur \mathbb{Q} ; $\mathbb{Q}(j) = \mathbb{Q}[j] \simeq \mathbb{Q}[t]/(t^2 + t + 1)$ est un corps quadratique (i.e. une extension de \mathbb{Q} de degré 2; voir A.2) dont $\mathbb{Z}[j] = \{x + jy | x, y \in \mathbb{Z}\}$ est l'anneau des entiers.

Pour calculer la norme, on utilise la formule :

$$N(x + yj) = (x + yj)(x + yj^2) = x^2 - xy + y^2.$$

Remarquer que les éléments de A forment un réseau de \mathbb{C} (A est un \mathbb{Z} -module libre de rang 2); géométriquement, ce réseau est l'ensemble des sommets d'un pavage de \mathbb{C} par des triangles équilatéraux de côté 1. Pour montrer que A est Euclidien, on se donne a et $b \neq 0$ dans A ; il s'agit de trouver q et r tel que $r = 0$ ou $N(r) < N(b)$. On prend pour q l'un des éléments de A le plus proche de a/b , de sorte que $|a/b - q| < 1/\sqrt{3} < 1$ (faire un dessin du réseau A); puis l'on pose $r = a - bq$. Alors

$$|r| = |b| \cdot |a/b - q| < |b|.$$

D'autre part, les éléments inversibles sont ceux de norme 1, c'est-à-dire les points du réseau qui sont sur le cercle unité.

Pour voir ce qu'est $A/\lambda A$, notons que $A \simeq \mathbb{Z}[t]/(t^2 + t + 1)$. En effet (attention : $\mathbb{Z}[t]$ n'est pas principal, donc on ne peut pas parler du polynôme minimal de j sur \mathbb{Z} et raisonner comme $\mathbb{Q}[j]$) le noyau de l'application $\Phi : \mathbb{Z}[t] \ni P \mapsto P(j) \in A$ est l'idéal $(t^2 + t + 1)$: considérant $P \in \ker \phi$, on peut soit effectuer la division euclidienne de P par $t^2 + t + 1$ dans $\mathbb{Z}[t]$ (car ce dernier polynôme est unitaire) et argumenter que le reste est nul car de degré inférieur ou égal à un, soit raisonner dans $\mathbb{Q}[t]$: $t^2 + t + 1$ divise P dans $\mathbb{Q}[t]$ et $t^2 + t + 1$ est de contenu 1, donc divisant le contenu de P , aussi $t^2 + t + 1$ divise-t-il P dans $\mathbb{Z}[t]$. Il en résulte :

$$\begin{aligned} A/\lambda A &\simeq \mathbb{Z}[t]/(1 + t + t^2, 1 - t) \simeq \mathbb{Z}[t]/(3, 1 - t) \simeq (\mathbb{Z}/3\mathbb{Z})[t]/(1 - t) \\ &\simeq \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3. \end{aligned}$$

Remarque. λ est donc premier dans $\mathbb{Z}[j]$ (ce que l'on savait déjà : $N(\lambda) = 3$ est premier, donc λ est irréductible).

Enfin, calculons :

$$\lambda^2 = (1 - j)^2 = 1 - 2j + j^2 = 1 + j + j^2 - 3j = -3j.$$

Nous aurons besoin du lemme suivant :

Lemme 1.8.1. *Les puissances troisièmes dans $A/9A = A/\lambda^4A$ sont $0, \pm 1, \pm \lambda^3$.*

Preuve : comme $A/\lambda A \simeq \mathbb{F}_3$, tout élément de A s'écrit $\pm 1 + \lambda a$ ou λa , avec $a \in A$. On calcule alors la puissance troisième de ces expressions : par exemple, $(1 + \lambda a)^3 = 1 + 3\lambda a + 3\lambda^2 a^2 + \lambda^3 a^3$. Mais on peut encore écrire $a = \varepsilon + \lambda a'$, où $\varepsilon \in \{0, \pm 1\}$ et $a' \in A$; on calcule les puissances de a dans $A/\lambda^4 A$ et obtient les égalités suivantes dans $A/\lambda^4 A$:

$$3\lambda a = 3\lambda \varepsilon, \quad 3\lambda^2 a^2 = 0, \quad \lambda^3 a^3 = \lambda^3 \varepsilon^3,$$

sachant que $\lambda^4 = 0$ et $3\lambda^2 = -9j = 0$ dans $A/\lambda^4 A$. Finalement :

$$(1 + \lambda a)^3 = 1 + 3\lambda \varepsilon + \lambda^3 \varepsilon^3 = 1 + \varepsilon \lambda (3 + \lambda^2) = 1 + 3\lambda^2 \varepsilon = 1.$$

On traite de même les autres cas.

Corollaire. *Les puissances troisièmes dans $A/\lambda^3 A$ sont $0, \pm 1$.*

Démontrons maintenant la proposition 1.8.1 : par l'absurde, on suppose qu'il existe x, y et z dans A et u dans A^\times tels que $x^3 + y^3 = uz^3$ et $xyz \neq 0$. Quitte à diviser par le pgcd, on se ramène au cas où x, y et z sont premiers entre eux deux à deux.

- Montrons que $\lambda \mid xyz$: dans le cas contraire, on aurait $\{x^3, y^3, z^3\} \subset \{\pm 1\}$ dans $A/\lambda^4 A$ (d'après ce que nous savons des cubes dans $A/\lambda^4 A$). Donc λ^4 diviserait $u \pm 2$. Or $0 \neq |u \pm 2| \leq 3$ tandis que $|\lambda^4| = 9$; c'est donc impossible.
- Montrons que si $\lambda \mid xy$ alors $u = \pm 1$: quitte à échanger x et y , on peut supposer que $\lambda \mid y$; alors $uz^3 = x^3$ dans $A/\lambda^3 A$. Comme λ ne divise pas z , on a donc $\pm u = \pm 1$ dans $A/\lambda^3 A$ (d'après ce que nous savons des cubes dans $A/\lambda^3 A$). Cela veut dire que λ^3 divise $u - 1$ ou $u + 1$. Or $|u \pm 1| \leq 2$ tandis que $|\lambda^3| = 3\sqrt{3} > 2$; cela n'est donc possible que si $u \pm 1 = 0$.
- Utilisant les deux points précédents, on se ramène au cas où $\lambda \mid z$: en effet, si ce n'est pas le cas alors $\lambda \mid xy$ (disons $\lambda \mid y$, la situation étant symétrique en x et y), donc $u = \pm 1$. Notre équation se réécrit alors $x^3 + (-uz)^3 = -y^3$: cela montre qu'il existe une équation $x^3 + y^3 = uz^3$, avec $\lambda \mid z$, possédant une solution (x, y, z) non triviale. On supposera alors que u et (x, y, z) sont tels que la λ -valuation $v_\lambda(z)$ de z est *minimale* (principe de descente) parmi toutes les solutions non triviales avec $\lambda \mid z$ de toutes les équations de la forme $x^3 + y^3 = uz^3$, avec u dans A^\times , que l'on peut écrire.
- Nous avons $x^3 + y^3 = 0$ dans $A/\lambda A$; d'autre part, comme λ ne divise ni x ni y , alors $x^3 + y^3 = 0$ ou ± 2 dans $A/\lambda^4 A$ (d'après ce que nous savons des cubes dans $A/\lambda^4 A$). Par conséquent, $x^3 + y^3 = 0$ dans $A/\lambda^4 A$, ou encore $\lambda^4 \mid uz^3$, donc $\lambda^2 \mid z$.
- Ecrivons maintenant :

$$(x + y)(x + jy)(x + j^2y) = x^3 + y^3 = uz^3.$$

Comme $\lambda^6 \mid uz^3$, au moins l'un des facteurs à gauche est divisible par λ^2 ; quitte à remplacer y par jy ou j^2y si nécessaire, on a $\lambda^2 \mid (x + y)$.

- Calculons la λ -valuation des trois facteurs : comme $x + jy = x + j^2y = x + y$ dans $A/\lambda A$ (car $j = 1$ dans $A/\lambda A$), alors λ divise $x + jy$ et $x + j^2y$. Par l'absurde, si λ^2 divisait $x + jy$, on aurait $x + jy = x + y$ dans $A/\lambda^2 A$, ou encore $0 = (1 - j)y = \lambda y$ dans $A/\lambda^2 A$. Donc λ diviserait y , ce qui est faux. De même pour $x + j^2y$; ainsi :

$$v_\lambda(x + jy) = 1, \quad v_\lambda(x + j^2y) = 1, \quad v_\lambda(x + y) = 3v_\lambda(z) - 2.$$

- De plus, ces éléments de A ont deux à deux λ pour pgcd : par exemple, $x + y = (x + jy) + \lambda y$, donc $\text{pgcd}(x + y, x + jy) = \text{pgcd}(x + y, \lambda y) = \lambda$ (car y est premier avec x donc avec $x + y$). La factorialité de A donne alors l'existence d'éléments α, β et γ de A qui sont premiers entre eux deux à deux et premiers à λ , et d'éléments u_1, u_2 et u_3 de A^\times tels que :

$$x + y = u_1 \lambda^{3v_\lambda(z) - 2} \alpha^3, \quad x + jy = u_2 \lambda \beta^3, \quad x + j^2y = u_3 \lambda \gamma^3.$$

- La combinaison linéaire avec coefficients $1, j$ et j^2 de ces trois équations, divisée par λ , donne :

$$0 = u_1 \lambda^{3v_\lambda(z) - 3} \alpha^3 + j u_2 \beta^3 + j^2 u_3 \gamma^3.$$

On pose alors $x_1 = \beta, y_1 = \gamma$ et $z_1 = \lambda^{v_\lambda(z) - 1} \alpha$, de sorte qu'avec ε_1 et ε_2 convenables dans A^\times on ait $x_1^3 + \varepsilon_1 y_1^3 = \varepsilon_2 z_1^3$. Comme $\lambda^3 \mid z_1^3$ (car $v_\lambda(z) \geq 2$), on a $\varepsilon_1 = \pm 1$ dans $A/\lambda^3 A$ donc dans A (raisonnement déjà vu). En remplaçant y_1 par $-y_1$ si nécessaire, on obtient donc $x_1^3 + y_1^3 = \varepsilon_2 z_1^3$, avec $v_\lambda(z_1) < v_\lambda(z)$, d'où la contradiction.

2. Arithmétique des courbes elliptiques

2.1. Motivations

Une définition moderne d'une *courbe elliptique* est la suivante :

Définition 2.1.1. *Une courbe elliptique E définie sur un corps k est une courbe projective plane non singulière de degré 3, munie d'un point $O \in E(k)$.*

Nous verrons plus loin le sens de ces mots. De manière vague, on s'intéresse à des équations du type

$$y^2 = x^3 + ax + b, \quad \text{où } 4a^3 + 27b^2 \neq 0.$$

(la condition signifie que le polynôme $x^3 + ax + b$ admet trois racines distinctes dans une clôture algébrique de k)

Comme nous allons le voir, l'arithmétique des courbes elliptiques est un sujet beau, riche et vaste. Mais encore, il s'est avéré que la théorie des courbes elliptiques permet de résoudre des problèmes qui, à priori, n'avait pas grand chose à voir avec les courbes elliptiques. Citons entre autres :

- *le dernier théorème de Fermat* : c'est notre 'prétexte' à l'étude des courbes elliptiques. Précisément, c'est la courbe de Frey $y^2 = x(x + a)(x - b)$ qui joue un rôle crucial, où $a = x^p$ et $b = y^p$, pour p un nombre premier impair et (x, y, z) une solution non triviale de l'équation de Fermat $x^p + y^p = z^p$. Alors les trois racines

$-a$, b et 0 du polynôme $x(x+a)(x-b)$ sont distinctes, de sorte qu'il s'agit bien d'une courbe elliptique. Or Wiles montre qu'une telle courbe elliptique ne peut pas exister.

- *les nombres congruents* : un entier naturel n est dit *congruent* s'il peut s'exprimer comme l'aire d'un triangle rectangle dont les longueurs des côtés sont des nombres rationnels. Ce problème a été soulevé par les mathématiciens de la Grèce Antique, puis a été discuté par les mathématiciens arabes du X^e siècle. Fibonacci a montré que 5 et 6 sont congruents, Fermat que 1, 2 et 3 ne le sont pas, enfin Euler que 7 est congruent. Cependant, le cas général est resté sans réponse ... jusqu'à 1983 (!) où Tunnell a relié le problème des nombres congruents à la théorie des courbes elliptiques.
- *la factorisation des entiers* : il existe un algorithme de factorisation des entiers due à Lenstra qui utilise les courbes elliptiques, meilleur sous plusieurs aspects que les précédents algorithmes (voir [Ko2] VI.4 ou [S-T] IV.4 ou [Ca] Chapter 26). De nos jours, cette question de la factorisation des entiers est devenue cruciale, en relation avec certains crypto-systèmes : étant donnés p et q deux nombres premiers très grands, toute personne connaissant $n = pq$ peut coder le message, mais le décodage requiert la connaissance de p et q . La sûreté du crypto-système est donc basée sur la difficulté à factoriser rapidement l'entier n . L'algorithme de Lenstra ne met pas en péril les crypto-systèmes en question, mais il montre qu'on est jamais à l'abri d'un rebondissement inattendu.

2.2. Courbes planes et singularité

2.2.1. Courbes affines planes

Soit k un corps et $\mathbb{A}^2(k) = k^2$ le *plan affine*. On note \bar{k} une clôture algébrique de k .

Définition 2.2.1. Une courbe affine plane $C = C_f$ définie sur k est la donnée (à multiplication près par un élément de K^\times) d'un polynôme $f \in k[X, Y]$ que l'on suppose sans facteur multiple dans sa décomposition en irréductibles dans $\bar{k}[X, Y]$. Les K -points de C_f ou points K -rationnels, pour $K \supset k$ un corps, sont les zéros de f dans K^2 :

$$C_f(K) = \{(x, y) \in K^2 \mid f(x, y) = 0\}.$$

On dit souvent que $f = 0$ est une équation de la courbe et écrit $C : f = 0$.

Soit $P \in C_f(K)$. Si au moins l'une des dérivées $\frac{\partial f}{\partial X}$ et $\frac{\partial f}{\partial Y}$ (dérivation «formelle» des polynômes) n'est pas nulle en P , on dit que P est un K -point *non-singulier* de C_f . La courbe C_f est dite *non-singulière* ou *lisse* si tout \bar{k} -point est non-singulier. Le contraire de non-singulier est *singulier*.

Si $P = (a, b) \in C_f(K)$ est non singulier, on peut définir la *droite tangente* D à C_f en P . C'est une *droite affine* définie sur K , c'est-à-dire une courbe affine donnée par un polynôme de $K[X, Y]$ de la forme $aX + bY$. Précisément :

$$\left(\frac{\partial f}{\partial X}\right)_P (X - a) + \left(\frac{\partial f}{\partial Y}\right)_P (Y - b).$$

Noter que dans le cas $K = \mathbb{R}$, ces définitions coïncident bien avec celles du cours de calcul différentiel.

Exemple. Considérons la courbe $C : Y^2 = X^3 + aX + b$, où a, b appartiennent à un corps k supposé de caractéristique différente de 2. En un point singulier (x, y) de C on a :

$$2y = 0, \quad 3x^2 + a = 0, \quad y^2 = x^3 + ax + b.$$

D'où $y = 0$ et x est une racine double du polynôme $X^3 + aX + b$. Donc C est non-singulière si et seulement si $X^3 + aX + b$ n'a pas de racine double (dans \bar{k}), donc si et seulement si son discriminant $4a^2 + 27b^2$ est non nul.

Soit $P = (a, b) \in C_f(K)$. Tout polynôme de $k[X, Y]$ s'écrivant (de manière unique) comme somme de polynômes homogènes de degrés croissants, on a :

$$f(X, Y) = f_1(X - a, Y - b) + \cdots + f_n(X - a, Y - b),$$

où f_i est homogène de degré i en $X - a$ et $Y - b$ (il s'agit du développement de Taylor formel de f). En particulier, $f_1(X, Y) = \left(\frac{\partial f}{\partial X}\right)_P (X - a) + \left(\frac{\partial f}{\partial Y}\right)_P (Y - b)$. Si donc P est singulier, alors

$$f(X, Y) = f_m(X - a, Y - b) + \text{termes de plus haut degré},$$

où $m \geq 2$ et $f_m \neq 0$. On dit alors que P est un K -point de C de *multiplicité* m . Si $m = 2$, on dit que P est un *point double*. On peut même raffiner la terminologie ; on a besoin d'un lemme :

Lemme 2.2.1. *Les polynômes irréductibles homogènes de $\bar{k}[X, Y]$ sont les polynômes homogènes de degré un.*

En effet, utilisant l'homogénéité de $f \in \bar{k}[X, Y]$ pour l'écrire comme un polynôme $g(T)$ en $T = X/Y$ (on divise par une puissance convenable de Y , travaillant dans $\bar{k}(Y)[X]$), ce dernier polynôme se décompose en produit de facteurs $\alpha T + \beta$ de degré un dans $\bar{k}[T]$. En multipliant par la même puissance de Y , on obtient un produit de facteurs $\alpha Y + \beta X$. Ces polynômes sont irréductibles dans $\bar{k}[X, Y] = (\bar{k}[X])[Y]$ car ils sont irréductibles dans $(\bar{k}(X))[Y]$ (puisque de degré un) et primitifs en X (i.e. en tant que polynômes en Y à coefficients dans $\bar{k}[X]$).

Pour simplifier les écritures, supposons que le point singulier P soit $(a, b) = (0, 0)$. Alors $f_m(X) = \prod d_i^{r_i}$ dans $\bar{k}[X, Y]$, où les d_i sont homogènes de degré un. Les droites $D_i : d_i = 0$ sont appelées *les droites tangentes* à C en P ; D_i a pour multiplicité r_i . On dit que la singularité est *ordinaire* en P si les droites tangentes sont toutes distinctes (i.e. toutes de multiplicité un). Un point double ordinaire est appelé un *noeud*. Sinon, on dit que le point double est une *pointe*.

Exemple. La courbe $Y^2 = X^3 + aX^2$ est singulière en $(0, 0)$. Si $a \neq 0$, ce point est un noeud et les deux tangentes en $(0, 0)$ sont $Y = \pm\sqrt{a}X$ (elles sont définies sur k si et seulement si a est un carré de k). Si $a = 0$, le point singulier est une pointe (il n'y a qu'une seule tangente : $Y = 0$).

2.2.2. Courbes projectives planes

Définition 2.2.2. *Une courbe projective plane $C = C_F$ définie sur k est la donnée (à multiplication près par un élément de K^\times) d'un polynôme homogène $F \in k[X, Y, Z]$*

que l'on suppose sans facteur multiple dans sa décomposition en irréductibles dans $\bar{k}[X, Y, Z]$. Les K -points de C_F ou points K -rationnels, pour $K \supset k$ un corps, sont les zéros de F dans $\mathbb{P}^2(K)$:

$$C_F(K) = \{(x : y : z) \in \mathbb{P}^2(K) \mid F(x, y, z) = 0\}.$$

On dit souvent que $F = 0$ est une équation de la courbe et écrit $C : F = 0$. Remarquer que l'homogénéité de F implique que

$$F(\lambda x, \lambda y, \lambda z) = \lambda^{\deg(F)} F(x, y, z)$$

de sorte que ça a bien un sens de parler des points de $\mathbb{P}^2(k)$ qui annulent F (bien qu'évaluer F en un point de $\mathbb{P}^2(k)$ n'ait aucun sens!)

Le degré de F est appelé *degré de la courbe* C_F . Une courbe de degré un est par définition une droite projective plane, de degré deux une *conique* (projective plane), de degré trois une *cubique* (projective plane).

Exemple. La courbe $C : Y^2 Z = X^3 + aXZ^2 + bZ^3$ est une cubique projective plane. Avec les notations de l'annexe B.1, $C \cap U_0$ est la courbe affine plane $C_0 : v^2 = u^3 + au + b$ tandis que $C \cap D_\infty(k)$ est réduit au point $(0 : 1 : 0)$, appelé «point à l'infini».

Utilisant la décomposition $\mathbb{P}^2 = U_0 \cup U_1 \cup U_2$ (cf B.1), on voit qu'une courbe projective plane C_F est toujours l'union de trois courbes affines planes (les $C_i = C \cap U_i$). Si l'on garde la même lettre pour les coordonnées affines sur les U_i , alors C_0 est d'équation $F(X, Y, 1) = 0$; de même, $C_1 : F(X, 1, Z) = 0$ et $C_2 : F(1, X, Z) = 0$. Dans l'exemple précédent, C est l'union de $C_0 : Y^2 = X^3 + aX + b$ et $C_1 : Z = X^3 + aXZ^2 + bZ^3$ (cet exemple ne reflète pas le cas général : ici deux courbes affines suffisent ; en effet, C_1 contient le point à l'infini $(0 : 1 : 0)$).

Définition 2.2.3. On dit que P est un point singulier de C_F s'il vérifie

$$F(P) = 0 = \left(\frac{\partial F}{\partial X} \right)_P = \left(\frac{\partial F}{\partial Y} \right)_P = \left(\frac{\partial F}{\partial Z} \right)_P.$$

Si P est non-singulier alors la droite projective plane

$$D : \left(\frac{\partial F}{\partial X} \right)_P X + \left(\frac{\partial F}{\partial Y} \right)_P Y + \left(\frac{\partial F}{\partial Z} \right)_P Z = 0$$

est appelée *tangente* à C_F en P .

Cette définition est justifiée par le fait suivant : P est singulier si et seulement si il l'est en tant que point de l'une (et donc toutes!) des courbes affines C_i à laquelle il appartient. S'il est non singulier, alors $D_i = D \cap U_i$ est la tangente à C_i en P . Démontrons cette assertion (on traitera le cas U_0) :

– notant $f(X, Y) = F(X, Y, 1)$, la courbe C_0 est d'équation $f = 0$. On pose $P = (a : b : 1)$. Comme

$$\left(\frac{\partial F}{\partial X} \right)_P = \left(\frac{\partial f}{\partial X} \right)_{(a,b)}, \quad \left(\frac{\partial F}{\partial Y} \right)_P = \left(\frac{\partial f}{\partial Y} \right)_{(a,b)},$$

il est clair que si P est un point singulier de C , alors il est également singulier en tant que point de C_0 .

- Réciproquement, si P est un point singulier de C_0 , il reste à montrer que $\left(\frac{\partial F}{\partial Z}\right)_P = 0$; cela résulte de l'identité d'Euler pour F , évaluée en P :

Lemme 2.2.2. *Soit F un polynôme homogène de degré d dans $k[X_1, \dots, X_n]$; on a l'identité dite «d'Euler» :*

$$dF = \sum_{i=1}^n X_i \frac{\partial F}{\partial X_i}.$$

Preuve : Puisque F est homogène :

$$F(TX_1, \dots, TX_n) = T^d F(X_1, \dots, X_n)$$

dans $k[X_1, \dots, X_n, T]$. En dérivant par rapport à T et en donnant à T la valeur 1, on trouve l'identité annoncée.

- Supposons maintenant que P est non-singulier; la tangente à C_0 en (a, b) est d'équation

$$\left(\frac{\partial F}{\partial X}\right)_P (X - a) + \left(\frac{\partial F}{\partial Y}\right)_P (Y - b) = 0.$$

Comparant avec l'équation

$$D \cap U_0 : \left(\frac{\partial F}{\partial X}\right)_P X + \left(\frac{\partial F}{\partial Y}\right)_P Y + \left(\frac{\partial F}{\partial Z}\right)_P Z = 0,$$

il suffit de montrer que

$$\left(\frac{\partial F}{\partial Z}\right)_P = -a \left(\frac{\partial F}{\partial X}\right)_P - b \left(\frac{\partial F}{\partial Y}\right)_P.$$

Cela résulte à nouveau de l'identité d'Euler.

Remarque. En vue de la recherche des éventuels points singuliers, une des quatre égalités dans la définition d'un point singulier est redondante : par exemple, si les trois dérivées partielles sont nulles en P , alors $F(P) = 0$ également, par l'identité d'Euler.

De même, la notion de multiplicité peut s'étendre aux courbes projectives en utilisant le fait que tout point P de C appartient à l'une au moins des courbes affines C_i . On vérifie que la multiplicité de P est la même dans chaque C_i , de sorte tout ça a bien un sens. Enfin, on peut démontrer qu'une transformation projective respecte les multiplicités.

Exemple. La cubique projective $C : Y^2Z = X^3 + aXZ^2 + bZ^3$, avec $\Delta = 4a^3 + 27b^2 \neq 0$, est non-singulière. En effet, sa partie affine C_0 est non-singulière (car $\Delta \neq 0$; déjà vu) et le point à l'infini $(0 : 1 : 0)$ est régulier car $\left(\frac{\partial F}{\partial Z}\right)_O = 1$ (ici, $F = Y^2Z - (X^3 + aXZ^2 + bZ^3)$).

Exemple. La cubique projective C_F définie par $F = X^3 + Y^3 + Z^3$ est non-singulière sur un corps de caractéristique différente de 3 : on calcule $\frac{\partial F}{\partial X} = 3X^2$ (même formule pour Y et Z); un point singulier vérifie donc $X = Y = Z = 0$, ce qui ne correspond à aucun point du plan projectif.

2.2.3. Morphismes entre courbes projectives planes

Soit C_F et C_G deux courbes projectives planes définies sur k , données par deux polynômes homogènes F et G de $k[X, Y, Z]$.

Définition 2.2.4. Une application rationnelle $\varphi : C_F \rightarrow C_G$ est la donnée de trois polynômes A, B, C de $k[X, Y, Z]$, homogènes de même degré (strictement positif), tel que, pour presque tout \bar{k} -point $(x : y : z)$ de C_F (i.e. tous les points sauf éventuellement un nombre fini), $(A(x, y, z) : B(x, y, z) : C(x, y, z))$ est bien défini en tant qu'élément de $\mathbb{P}^2(\bar{k})$ et appartient à $C_G(\bar{k})$. On note $\varphi = (A : B : C)$.

On dit que l'application rationnelle φ est birationnelle s'il existe une application rationnelle $\psi : C_G \rightarrow C_F$ telle que, pour presque tous les \bar{k} -points, les applications $\psi \circ \varphi$ et $\varphi \circ \psi$ sont définies et égales à l'identité.

Noter que la condition d'homogénéité assure que $(A(x, y, z) : B(x, y, z) : C(x, y, z))$ définit bien un point du plan projectif, dès que les trois polynômes ne s'annulent pas simultanément.

Comme deux triplets (x_1, x_2, x_3) et (x'_1, x'_2, x'_3) sont proportionnels si et seulement si $x_i x'_j = x'_i x_j$ pour tout $i \neq j$, on est amené à définir :

Définition 2.2.5. Deux applications rationnelles $\varphi = (A_1, A_2, A_3), \varphi' = (A'_1, A'_2, A'_3) : C_F \rightarrow C_G$ sont dites équivalentes si $A_i A'_j \equiv A'_i A_j \pmod{F}$ dans $k[X, Y, Z]$ pour tout $i \neq j$. On écrit $\varphi \sim \varphi'$.

En effet, deux telles applications équivalentes prennent alors la même valeur en tout \bar{k} -point P de C_F en lequel elles sont toutes les deux définies. Mais il se peut que l'une des deux soit définie en P et l'autre pas.

Définition 2.2.6. On dit qu'une application rationnelle $\varphi : C_F \rightarrow C_G$ est régulière en P s'il existe une application rationnelle $\varphi' \sim \varphi$ définie en P . On pose alors $\varphi(P) = \varphi'(P)$.

En particulier, $(AH : BH : CH) \sim (A : B : C)$ pour tout polynôme H (qui n'est pas multiple de F).

Exemple. Soit $C_F : X^2 + Y^2 = Z^2$ et $C_G : Z = 0$. Alors $\varphi = (X + Z : Y : 0)$ est une application rationnelle $C_F \rightarrow C_G$ régulière en tout \bar{k} -point de C_F .

En effet, soit $P = (x : y : z)$ un tel point ; $\varphi(P) = (x + z : y : 0)$ appartient à $C_G(\bar{k})$ dès que $(x + z, y) \neq (0, 0)$. Le problème se pose en $P = (-1 : 0 : 1)$: φ est-elle régulière en P ? Comme $(X + Z)(X - Z) \equiv (-Y)Y \pmod{F}$, alors $\varphi \sim (-Y : X - Z : 0)$ (ou par étapes : $\varphi \sim ((X + Z)(X - Z) : Y(X - Z) : 0) \sim (-Y^2 : Y(X - Z) : 0) \sim (-Y : X - Z : 0)$). On pose donc $\varphi(P) = (0 : 1 : 0)$.

Définition 2.2.7. Un morphisme $\varphi : C_F \rightarrow C_G$ est une application rationnelle régulière en tout point de $C_F(\bar{k})$. S'il existe un morphisme $\psi : C_G \rightarrow C_F$ tel que $\psi \circ \varphi$ et $\varphi \circ \psi$ sont égales à l'identité sur $C_F(\bar{k})$ et $C_G(\bar{k})$, alors on dit que φ est un isomorphisme.

Exemple. Poursuivant avec l'exemple précédent, on vérifie que $\psi = (X^2 - Y^2 : 2XY : X^2 + Y^2)$ est une application rationnelle $C_G \rightarrow C_F$ régulière en tout point et qu'elle fournit un inverse à φ . Autrement dit, la conique projective C_F est isomorphe à la droite projective C_G .

2.3. Courbes elliptiques et loi de groupe

2.3.1. Définition d'une courbe elliptique

Rappelons la définition, dorénavant éclaircie : une courbe elliptique définie sur un corps k est une cubique projective plane non-singulière C définie sur k , munie d'un point $O \in C(k)$.

Il reste à comprendre le rôle du point O (ce sera le neutre pour la loi de groupe sur C que l'on va définir). Mais avant, on aimerait «simplifier» autant que possible l'équation d'une courbe elliptique, en restant dans la même «classe d'isomorphisme». C'est le rôle de l'équation de Weierstrass.

On appelle *équation de Weierstrass (courte)* une équation de la forme $Y^2Z = X^3 + aXZ^2 + bZ^3$. On écrit souvent $y^2 = x^3 + ax + b$ (la déshomogénéisée en Z obtenue en remplaçant Z par 1), pour simplifier, sachant que l'on retrouve l'équation initiale en homogénéisant, c'est-à-dire en multipliant chaque terme par une puissance de Z (minimale afin que tous les termes soient de même degré, en l'occurrence 3). De plus, $y^2 = x^3 + ax + b$ est l'équation de la «partie affine» notée C_0 de la cubique de Weierstrass $C : Y^2Z = X^3 + aXZ^2 + bZ^3$, la partie «à l'infini» se réduisant au point $(0 : 1 : 0)$ (déjà vu). Donc C est connue dès que l'on connaît C_0 . La donnée $(C, (0 : 1 : 0))$ définit une courbe elliptique sur k (on choisira toujours pour O le point à l'infini, dans le cas d'une cubique de Weierstrass).

Par ailleurs, on dit que deux courbes elliptiques (C, O) et (C', O') définies sur k sont *isomorphes* s'il existe un isomorphisme $\phi : C \rightarrow C'$ de courbes projectives planes vérifiant $\phi(O) = O'$.

On admettra la proposition suivante :

Proposition 2.3.1. *Soit k un corps de caractéristique différente de 2 et 3. Toute courbe elliptique (C', O') définie sur k est isomorphe à une courbe elliptique (C, O) , où C est donnée par une équation de Weierstrass courte et où $O = (0 : 1 : 0)$ est le point à l'infini.*

En fait, il existe un algorithme permettant de résoudre ce problème. Maple sait donc le faire.

Remarque. Sans l'hypothèse sur la caractéristique, on montre qu'on peut toujours se ramener à une équation de Weierstrass (longue) $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

La question naturelle qui se pose est alors la suivante : cette équation de Weierstrass est-elle «canonique» ?

Proposition 2.3.2. *On suppose toujours que k est de caractéristique différente de 2 et 3. Deux courbes elliptiques $C_{(a,b)}$ et $C_{(a',b')}$ sont isomorphes si et seulement si il existe $c \in k^\times$ tel que $a' = c^4a$ et $b' = c^6b$. L'isomorphisme est alors $(x : y : z) \mapsto (c^2x : c^3y : z)$.*

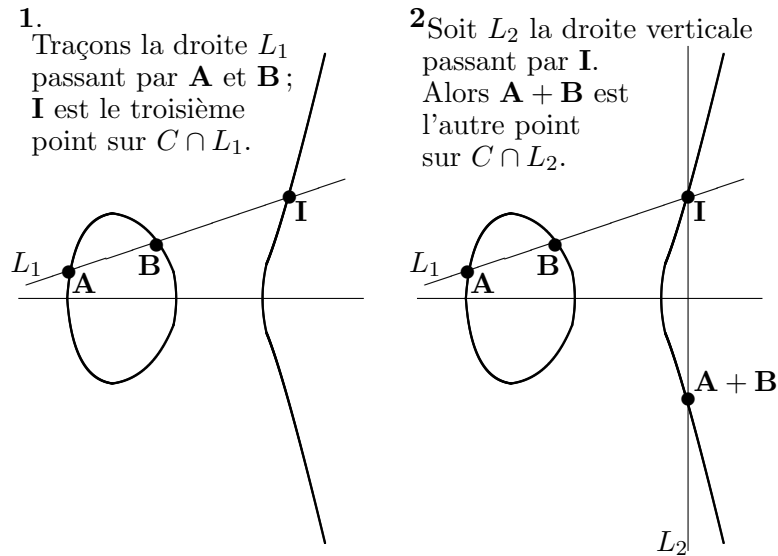
Il est clair que cette condition est suffisante. Nous admettrons qu'elle est également nécessaire.

2.3.2. La loi de groupe

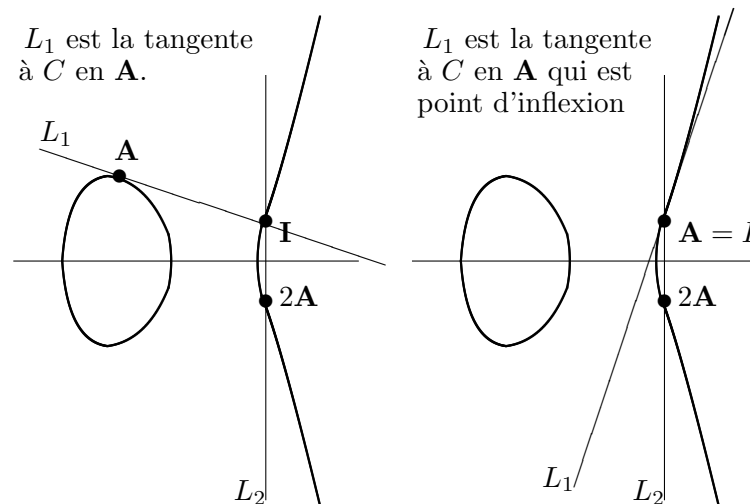
On suppose donc que k est un corps de caractéristique différente de 2 et 3 et se donne une courbe elliptique $C : y^2 = x^3 + ax + b$ (avec $4a^3 + 27b^2 \neq 0$ et $O = (0 : 1 : 0)$ le point à l'infini).

Pour n'importe quelle extension $K \supset k$ et A, B deux K -points de C , on veut définir la somme $A + B$, de sorte que $(C(K), +)$ forme un groupe abélien, de neutre O . La construction est la suivante ; elle procède par «cordes et tangentes» :

(a) Cas $A \neq B$:



(b) Cas où $A = B$:



Noter que la tangente est bien définie, car la courbe est non-singulière.

Ces constructions ont-elles un sens ? Il s'agit de vérifier :

- que I est bien défini (i.e. que la droite L_1 coupe bien C en un «troisième point»)
- que $A + B$ appartient à $C(K)$.

Remarque. L'addition des points est donc un moyen de fabriquer des points rationnels, lorsque l'on en connaît déjà un ou deux.

Qu'une droite rencontre une cubique (projective) en trois points (comptés avec «multiplicité») est un cas particulier du «théorème de Bezout» :

Théorème 2.3.1 (Bezout). *Si C et D sont deux courbes projectives planes de degrés c et d n'ayant pas une infinité de points en commun (c'est le cas par exemple si $C = D$), alors $\#(C(K) \cap D(K)) \leq cd$. Lorsque K est algébriquement clos, alors on a l'égalité $\sum_{P \in C(K) \cap D(K)} i(P, C \cap D) = cd$, où $i(P, C \cap D)$ désigne la multiplicité d'intersection de C et D en P .*

Nous allons démontrer ce théorème et définir la multiplicité d'intersection, du moins dans le cas qui nous intéresse. Ainsi C est une cubique d'équation $F(X, Y, Z) = 0$, pour F un polynôme homogène de degré 3 et D est une droite $aX + bY + cZ = 0$. Quitte à permuter les indéterminées, nous supposons que $a \neq 0$; en un point d'intersection, on a donc $F(-(bY + cZ)/a, Y, Z) = 0$. C'est un polynôme homogène de degré 3 de $k[Y, Z]$ (ce n'est pas le polynôme nul, sinon $aX + bY + cZ$ diviserait F ; la droite D serait incluse dans C , ce qui est contraire à l'hypothèse), qui s'écrit donc :

$$\alpha_1 Y^3 + \alpha_2 Y^2 Z + \alpha_3 Y Z^2 + \alpha_4 Z^3 = 0.$$

Si K est algébriquement clos, on a déjà vu que les polynômes homogènes irréductibles de $K[Y, Z]$ sont ceux de degré un. On pourra dans ce cas écrire :

$$(b_1 Y + c_1 Z)(b_2 Y + c_2 Z)(b_3 Y + c_3 Z) = 0$$

(rappelez-vous : on travaille dans $K(Z)[Y]$ et écrit

$$\alpha_1 \left(\frac{Y}{Z}\right)^3 + \alpha_2 \left(\frac{Y}{Z}\right)^2 + \alpha_3 \left(\frac{Y}{Z}\right) + \alpha_4$$

en tant que produit de facteurs de degré un en $T = \frac{Y}{Z}$). Par définition, la multiplicité d'intersection en $P = ((bc_1 - cb_1)/a : -c_1 : b_1)$ est le nombre de fois que le facteur $(b_1 Y + c_1 Z)$ apparaît dans cette décomposition. On a donc exactement trois solutions, comptées avec multiplicité. Enfin, lorsque K n'est pas algébriquement clos, $K \subset \bar{K}$, et le résultat pour \bar{K} donne l'inégalité pour K .

Remarque. On peut aussi définir la multiplicité d'intersection en travaillant sur une partie affine de la courbe C : par exemple, si $P \in U_0$, i.e. $P = (x_0 : y_0 : 1)$, on cherche la multiplicité d'intersection de $D_0 : a(x - x_0) + b(y - y_0) = 0$ et de $C_0 : f(x, y) = 0$, où $f(x, y) = F(x, y, 1)$. Comme précédemment, on peut supposer $a \neq 0$, de sorte qu'en un point d'intersection, on a $f(x_0 - \frac{b}{a}(y - y_0), y) = 0$. Dans $\bar{k}[y]$, ce polynôme s'écrit

$$\alpha_1 y^3 + \alpha_2 y^2 + \alpha_3 y + \alpha_4 = (b_1 y + c_1)(b_2 y + c_2)(b_3 y + c_3).$$

Par définition, la multiplicité d'intersection en P est le nombre de fois où apparaît le facteur $y - y_0$. Noter cependant que la somme des multiplicité d'intersection des points sur $C_0 \cap D_0$ n'est plus nécessairement trois : il se peut que ce polynôme en y

soit de degré strictement inférieur à trois (il se peut que C et D se coupent également à l'infini !)

Par ailleurs, écrivant

$$f(x, y) = F_1(x - x_0, y - y_0) + F_2(x - x_0, y - y_0) + F_3(x - x_0, y - y_0),$$

où F_i est homogène de degré i , rappelons que le plus petit i tel que $F_i \neq 0$ est la multiplicité de P sur C . Que peut-on dire concernant ces deux notions de multiplicité ? Remplaçant $x - x_0$ par $-\frac{b}{a}(y - y_0)$ dans cette égalité, la multiplicité d'intersection en (x_0, y_0) est par définition la puissance maximale de $(y - y_0)$ que l'on peut mettre en facteur. On se rend ainsi compte que :

- Lorsque D_0 n'est pas la tangente en P , alors la multiplicité d'intersection en P vaut un (car P est non-singulier) ;
- La multiplicité d'intersection en P est supérieure ou égale à la multiplicité de P sur C ;
- En particulier, lorsque D_0 coïncide avec la tangente, alors la multiplicité d'intersection est supérieure ou égale à 2, donc vaut 2 ou 3. La connaissance de F_2 permet de statuer : on regarde si $F_2(-\frac{b}{a}(y - y_0), y - y_0) = 0$.

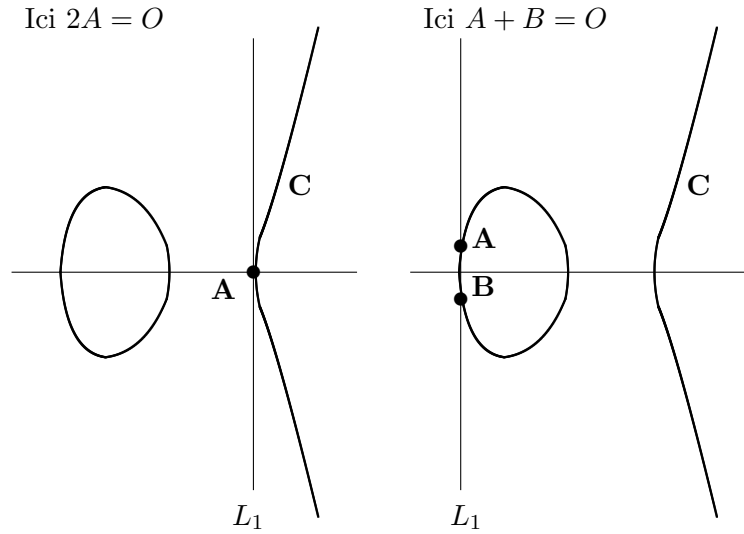
Définition 2.3.1. *Un point P non-singulier d'une courbe projective plane C est appelé un point d'inflexion de C lorsque la multiplicité d'intersection en P de C et de la tangente à C en P est supérieure ou égale à trois.*

Par exemple, le point à l'infini O de $C : Y^2Z = X^3 + aXZ^2 + bZ^3$ est un point d'inflexion : la droite à l'infini $D : Z = 0$ intersecte C en un seul point, qui est donc de multiplicité trois. On le voit également via les équations : en remplaçant Z par 0, on trouve $X^3 = 0$.

Notant I le «troisième» point d'intersection de C avec la droite L_1 (qui est la droite passant par A et B , ou la tangente à C en A si $A = B$), alors par construction, $A + B$ est le «troisième» point d'intersection de C avec la droite L_2 , qui est la droite passant par O et I (l'équation affine $x = x_0$ devient $X - x_0Z = 0$).

Remarque. C'est de cette manière que l'on définit la loi de groupe sur une courbe elliptique quelconque (i.e. pas nécessairement une cubique de Weierstrass et O un point rationnel quelconque).

On comprend alors les cas particuliers suivants :



Dans ces deux cas, $I = O$; on prend alors pour L_2 la tangente à C en O , qui coupe C en O uniquement. Ainsi, dans les constructions du (a) et (b), on voit que $I + (A + B) = O$, ou encore que $I = -(A + B)$. A supposer que la loi soit bien associative (ce qu'il faudra démontrer), on peut écrire $A + B + I = O$. En résumé, on voit que (et cette propriété caractérise la loi de groupe) :

Soit A, B et I trois points de C . Alors $A + B + I = O$ si et seulement si A, B et I sont alignés

En effet, $A + B + I = 0$ équivaut à $I = -(A + B)$. Or on vient de remarquer que par construction le point $-(A + B)$ est tel que A, B et $-(A + B)$ sont alignés.

Remarque. Dans la formulation de l'encadré, si un point est répété plusieurs fois alors il est sous-entendu que l'on prenne en compte les multiplicités : par exemple, « A, A et $I \neq A$ sont alignés» signifie qu'il existe une droite passant par A et I telle que les multiplicités d'intersection avec la courbe sont respectivement 2 et 1.

Notons la formule très simple pour l'inverse :

$$\text{Si } P = (x : y : z) \text{ alors } -P = (x : -y : z).$$

En effet, cela correspond à A, B et O alignés, donc A et B sur une même droite verticale ; or l'équation de C_0 est $y^2 = x^3 + ax + b$.

Remarque. Les formules encadrées sont spécifiques à une courbe elliptique sous forme de Weierstrass (avec O le point à l'infini).

En particulier, $-P = P$, i.e. P est d'ordre deux, si et seulement si $y = 0$. Les points d'ordre deux sont donc les $(x : 0 : 1)$ où x est racine de $X^3 + aX + b$. En rajoutant O , on obtient un groupe d'ordre 4 (en se plaçant sur \bar{k}), qui est donc isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (en effet, ce ne peut être $\mathbb{Z}/4\mathbb{Z}$ car tous les éléments distincts de O sont d'ordre deux). On vient de déterminer la 2-torsion du groupe abélien $C(\bar{k})$.

Montrons maintenant que si A et B sont K -rationnels, alors il en est de même de $A + B$. Par construction, il suffit de montrer que le troisième point I sur la droite L_1

est K -rationnel. On revient alors à l'intersection d'une cubique et d'une droite, qui est donnée par

$$\alpha_1 \left(\frac{Y}{Z}\right)^3 + \alpha_2 \left(\frac{Y}{Z}\right)^2 + \alpha_3 \left(\frac{Y}{Z}\right) + \alpha_4 = \left(b_1 \left(\frac{Y}{Z}\right) + c_1\right) \left(b_2 \left(\frac{Y}{Z}\right) + c_2\right) \left(b_3 \left(\frac{Y}{Z}\right) + c_3\right) = 0.$$

Il résulte des relations entre coefficients et racines du polynôme $\alpha_1 T^3 + \alpha_2 T^2 + \alpha_3 T + \alpha_4 \in k[T]$, que si toutes ses racines, sauf l'une, appartiennent à K , alors la dernière racine appartient à K également. Soit $I = (x : y : z)$; si $z = 0$, alors $x = -(by + cz)/a = -(b/a)y$, donc $I = (-b : a : 0)$ est même k -rationnel. Sinon, $z \neq 0$ et l'on a vu que $y/z \in K$. Comme $x/z = (-b(y/z) + c)/a$, alors $I = (x/z : y/z : 1)$ est bien K -rationnel.

Le rôle de A et B étant symétrique, la commutativité est évidente. Il reste à démontrer l'associativité : $(J + K) + L = J + (K + L)$ pour tout triplet de points (J, K, L) de $C(K)$. Nous écrirons en TP les formules explicites donnant les coordonnées de $A + B$ en fonction de celles de A et B ; c'est alors une simple vérification (un peu fastidieuse, d'où le recours à Maple qui calculera pour nous). Signalons qu'il existe des preuves plus élégantes; l'une d'entre elles fait un usage intensif du théorème de Bezout cité précédent.

Considérons maintenant deux courbes elliptiques $C_{(a,b)}$ et $C_{(a',b')}$ qui sont isomorphes, l'isomorphisme étant donné par $\phi : (x : y : z) \mapsto (c^2 x : c^3 y : z)$ (en particulier $\phi(O) = O$). A-t-on alors un isomorphisme de groupes abéliens? La réponse est oui : comme une droite $\alpha_1 X + \alpha_2 Y + \alpha_3 Z = 0$ passant par A et B est transformée en la droite $\alpha_1 c^{-2} X + \alpha_2 c^{-3} Y + \alpha_3 Z = 0$ passant par $\phi(A)$ et $\phi(B)$ (avec respect des multiplicités d'intersection), il résulte de la construction géométrique définissant la loi de groupe que $\phi(A + B) = \phi(A) + \phi(B)$.

Remarque. Un isomorphisme entre deux courbes elliptiques (C', O') et (C, O) induit toujours un isomorphisme de groupes abéliens. Lorsque l'isomorphisme est une transformation projective, c'est évident (pour les mêmes raisons que précédemment : une telle transformation transforme une droite en une droite et on démontre qu'elle respecte les multiplicités d'intersection). Le cas général est plus délicat à démontrer.

Enfin, si l'on se donne une cubique *singulière* $C : y^2 = x^3 + ax + b$ (donc $4a^3 + 27b^2 = 0$), peut-on définir une loi de groupe sur l'ensemble des points non singuliers (comme le polynôme $x^3 + ax + b$ possède au plus une racine multiple, il y a un seul point singulier)? Il s'agit de montrer que si A et B sont non-singuliers, alors le troisième point d'intersection I de la droite L_1 avec C est encore non singulier. Si $A \neq B$, cela résulte du fait que la multiplicité d'intersection de L_1 et C en chacun des points est un. En effet, non avons vu que cette multiplicité d'intersection (sauf avec la tangente) vaut un si et seulement si le point est non singulier. Si par contre $A = B$, auquel cas L_1 est la tangente en A , alors la multiplicité d'intersection en A est soit 2, auquel cas celle de I sera 1 (donc I est régulier), soit 3, auquel cas $I = A$ est encore non-singulier. La réponse est oui.

2.4. Points rationnels et théorème de Mordell

Soit $C : F(X, Y, Z) = 0$ une courbe projective plane définie sur \mathbb{Q} . Les deux questions fondamentales de la «géométrie diophantienne» sont les suivantes :

- Est-ce que C possède un point rationnel, c'est-à-dire un \mathbb{Q} -point ?
- Si la réponse est oui, peut-on «paramétrer» ces points rationnels ?

De plus, on aimerait disposer d'un algorithme pour répondre de manière effective à ces questions. Est-ce le cas ? C'est une troisième question.

2.4.1. Cas des courbes de degré inférieur ou égal à deux

Le cas d'une courbe de degré un est immédiat : une droite $D : aX + bY + cZ = 0$ avec a, b et c trois rationnels non tous nuls (par exemple $c \neq 0$) admet toujours un point rationnel et l'application

$$(x : y) \mapsto (x : y : -\frac{a}{c}x - \frac{b}{c}y)$$

établit une bijection entre $\mathbb{P}^1(\mathbb{Q})$ et $D(\mathbb{Q})$.

Qu'en est-il d'une courbe C de degré deux, i.e. une conique, définie par une forme quadratique $F(X, Y, Z)$ en trois variables à coefficients rationnels ?

Tout d'abord, on opère une réduction, en relation avec la *classification des formes quadratiques sur un corps k de caractéristique différente de deux* : la conique étant définie par

$$F(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0,$$

on considère la matrice

$$B = \frac{1}{2} \begin{pmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{pmatrix}$$

de la forme bilinéaire associée ; ainsi $F(X, Y, Z) = {}^tV B V$, où ${}^tV = (XYZ)$. Calculant les dérivées partielles, on voit que les points singuliers de C sont exactement les $(x : y : z)$ tels que $B^t(xyz) = 0$ (il résulte de l'identité d'Euler qu'un point P annulant les trois dérivées partielles est bien sur la courbe). Comme le vecteur nul est interdit (il ne correspond pas à un point de \mathbb{P}^2), on voit que la conique projective est non-singulière si et seulement si $\det B \neq 0$, donc si et seulement si B est de rang trois. Par définition, cela équivaut à dire que la forme quadratique est non dégénérée.

Comme B est une matrice symétrique sur le corps k (de caractéristique différente de deux), nous savons qu'elle est diagonalisable sur k (c'est le corollaire matriciel du théorème d'existence d'une base orthogonale pour la forme quadratique F) : il existe $G \in \text{GL}_3(k)$ telle que ${}^tG B G = D = \text{diag}(\alpha, \beta, \gamma)$ est diagonale. Cela permet d'écrire $F = \alpha L_1^2 + \beta L_2^2 + \gamma L_3^2$, où les L_i sont trois formes linéaires $L_i = g_{i1}X + g_{i2}Y + g_{i3}Z$ données par la matrice ${}^tG = (g_{ij})$. L'application $(x : y : z) \mapsto (L_1(x, y, z) : L_2(x, y, z) : L_3(x : y : z))$ définit une bijection de \mathbb{P}^2 dans lui-même, qui induit une bijection entre les K -points des coniques C et $C' : \alpha X^2 + \beta Y^2 + \gamma Z^2 = 0$ pour tout corps $K \supset k$. Il suffira donc d'étudier C' .

Dire que $C' : \alpha X^2 + \beta Y^2 + \gamma Z^2 = 0$ est non-singulière est équivalent à $\alpha\beta\gamma \neq 0$. Les cas dégénérés sont les suivants :

- B est de rang deux ; comme $\ker B$ est de dimension un, il y a un unique point singulier P . On se ramène à $C' : \alpha X^2 + \beta Y^2 = 0$ qui se décompose dans $\bar{k}[X, Y]$ en

$(\alpha_1 X + \beta_1 Y)(\alpha_1 X - \beta_1 Y)$: autrement dit, C' est l'union de deux droites (définies sur une extension de k) passant par P .

- B est de rang un : on se ramène alors à $C' : \alpha X^2 = 0$. Autrement dit, C' est une droite double définie sur k dont tous les points sont singuliers.

Remarque. Le fait qu'une conique non-dégénérée est non singulière peut être également vu comme une conséquence du théorème de Bezout : en effet, si P a pour multiplicité $m > 1$, alors la multiplicité d'intersection en P de C avec une droite quelconque passant par P et un second point Q de C est supérieure ou égal à m , donc à deux. Cela serait en contradiction avec le théorème de Bezout : $I(P, C \cap (PQ)) + I(Q, C \cap (PQ)) \geq 2 + 1 = 3$. Noter que le théorème de Bezout s'applique bien parce que la droite (PQ) n'est pas incluse dans C , justement parce que la conique est non-dégénérée.

Revenons maintenant au cas de la caractéristique 0 : C est donnée par une équation $aX^2 + bY^2 + cZ^2 = 0$, où a, b et c appartiennent à un corps k contenant \mathbb{Q} .

- Si $k = \mathbb{C}$, il est possible d'écrire $a = \alpha^2$, $b = \beta^2$ et $c = \gamma^2$, de sorte qu'en remplaçant X par αX , Y par βY et Z par γZ , on se ramène à $X^2 + Y^2 + Z^2 = 0$. Il n'y a essentiellement qu'un seul type de conique non-singulière dans $\mathbb{P}^2(\mathbb{C})$.
- Si $k = \mathbb{R}$, il faut tenir compte du signe des coefficients : il y a deux types, à savoir $X^2 + Y^2 - Z^2 = 0$ et $X^2 + Y^2 + Z^2 = 0$ (dont le second n'a pas de \mathbb{R} -points).
- Si $k = \mathbb{Q}$, on se ramène au cas où a, b et c sont des entiers relatifs non nuls (quitte à multiplier par un entier) premiers entre eux deux à deux et sans facteur carré (i.e. $p \mid x \Rightarrow p^2 \nmid x$, $x = a, b, c$) : si $d = \text{pgcd}(a, b) > 1$, on réécrit l'équation $(\frac{a}{d})X^2 + (\frac{b}{d})Y^2 + cdZ_1^2 = 0$, où $Z_1 = \frac{1}{d}Z$; si $d^2 \mid a$, alors notre équation est équivalente à $(\frac{a}{d^2})X^2 + bY_1^2 + cZ_1^2 = 0$, où $Y_1 = \frac{1}{d}Y$ et $Z_1 = \frac{1}{d}Z$.

Remarque. Dans le cas des coniques affines réelles, on distingue les ellipses, les hyperboles et les paraboles. Cette distinction disparaît dans le cas projectif (i.e. les courbes projectives correspondantes sont isomorphes en tant que courbes projectives planes définies sur \mathbb{R}).

- Le cas de l'ellipse affine se ramène par transformation affine au cercle $x^2 + y^2 = 1$, donc à $X^2 + Y^2 - Z^2 = 0$ en homogénéisant. Ici, la droite à l'infini $Z = 0$ ne coupe pas la conique (du moins, si l'on regarde les \mathbb{R} -points).
- Le cas de l'hyperbole affine se ramène à $x^2 - y^2 = 1$, donc à $X^2 - Y^2 - Z^2 = 0$ en homogénéisant. La droite à l'infini coupe la conique en les deux points $(1 : \pm 1 : 0)$ (avec une multiplicité d'intersection égale à un). Ces deux points sont à relier aux axes de l'hyperbole d'équation $y = \pm x$.
- Le cas de la parabole $y = x^2$, donc $YZ - X^2 = 0$. La droite $Z = 0$ coupe la conique en le point $(0 : 1 : 0)$ (avec une multiplicité d'intersection égale à deux).
Noter que $YZ - X^2 = -X^2 + [\frac{1}{2}(Y + Z)]^2 - [\frac{1}{2}(Y - Z)]^2$.

En résumé, les trois cas correspondent aux différentes façons, pour la droite à l'infini, de couper la conique.

Etudions maintenant les questions diophantiennes, pour une conique projective supposée non dégénérée. D'emblée, remarquons qu'il n'est pas vrai qu'une telle conique admet toujours un point rationnel :

Exemple. La courbe $C : X^2 + Y^2 + Z^2 = 0$ n'a pas de point rationnel : $C(\mathbb{Q}) = \emptyset$ car $C(\mathbb{R}) = \emptyset$.

Exemple. La conique $C : X^2 + Y^2 - 3Z^2 = 0$ est également dépourvue de point rationnel. En effet, si $(x : y : z) \in C(\mathbb{Q})$, on peut tuer les dénominateurs de façon à écrire $(x : y : z) = (x_1 : y_1 : z_1)$, où (x_1, y_1, z_1) est un triplet primitif d'entiers. Or les seuls carrés de \mathbb{F}_3 sont $\bar{0}$ et $\bar{1}$: on ne peut avoir $\bar{x}_1^2 + \bar{y}_1^2 = \bar{0}$ dans \mathbb{F}_3 que si $\bar{x}_1 = \bar{y}_1 = \bar{0}$. Alors 3^2 diviserait $3z_1^2$, donc 3 diviserait aussi z_1 , d'où la contradiction.

Les deux exemples précédents sont en fait étroitement liés. Pour le voir, il faut comprendre le rôle que joue \mathbb{R} vis à vis de \mathbb{Q} : par construction, \mathbb{R} est le complété de \mathbb{Q} pour la valeur absolue archimédienne $|\bullet|$. Or il existe d'autres corps, tout aussi importants que \mathbb{R} , obtenus en complétant \mathbb{Q} par rapport aux valeurs absolues p -adiques $|\bullet|_p$, pour chaque nombre premier p : ce sont les corps p -adiques \mathbb{Q}_p (voir l'annexe B.2). En fait, dans le second exemple, on a montré que $C(\mathbb{Q}_3) = \emptyset$: s'il y avait une solution $(x : y : z) \in C(\mathbb{Q}_3)$, quitte à multiplier par une puissance convenable de 3, on obtiendrait une solution (primitive) dans $C(\mathbb{Z}_3)$, c'est-à-dire un système compatible de solutions dans $\mathbb{Z}/3^n\mathbb{Z}$ pour tout n . Or on a montré qu'il n'y a pas de solution $(x_2 : y_2 : z_2)$ dans $\mathbb{P}^2(\mathbb{Z}/3^2\mathbb{Z})$ qui relève une solution $(x_1 : y_1 : z_1) = (\bar{0} : \bar{0} : z_1)$, $z_1 \neq \bar{0}$ dans $\mathbb{P}^2(\mathbb{Z}/3\mathbb{Z})$: on aurait $x_2 = \bar{0}$ ou $\pm\bar{3}$ dans $\mathbb{Z}/9\mathbb{Z}$ car x_2 relève x_1 (idem pour y_2), d'où $\bar{0} = \bar{3}z_2$. Puis $z_2 = \bar{0}$ ou $\pm\bar{3}$, auquel cas z_2 ne relève pas z_1 .

Ces deux exemples illustrent donc l'assertion suivante : une condition nécessaire pour que C ait un point rationnel est d'avoir un point dans \mathbb{R} et un point dans \mathbb{Q}_p pour tout premier p ($\mathbb{Q} \subset \mathbb{R}$ et $\mathbb{Q} \subset \mathbb{Q}_p$!). Il est naturel de se demander si cette condition est également suffisante :

Théorème 2.4.1 (Legendre). *Une forme quadratique $F(X, Y, Z)$ à coefficients rationnels possède un zéro non trivial dans \mathbb{Q} si et seulement si elle possède un zéro non trivial dans \mathbb{R} et dans chaque \mathbb{Q}_p pour tout premier p .*

Remarque. Lorsque, pour une certaine famille de polynômes, chaque polynôme possède un zéro dans \mathbb{Q} si et seulement si il possède un zéro dans \mathbb{R} et dans chaque \mathbb{Q}_p , on dit que le «principe de Hasse» est vérifié par cette famille de polynômes. Ainsi les coniques vérifient le principe de Hasse.

Bien sûr, ce n'est pas en ces termes que Legendre (1752-1833) a énoncé son résultat, puisque les nombres p -adiques ont moins de cent ans. L'énoncé de Legendre est le suivant :

Théorème 2.4.2 (Legendre). *Soit a, b et c trois entiers relatifs premiers entre eux deux à deux, sans facteur carré (i.e. $p \mid n \Rightarrow p^2 \nmid n$) et dont l'un au plus est négatif. Il existe une solution non-triviale à l'équation en entiers $ax^2 + by^2 + cz^2 = 0$ si et seulement si $abc < 0$ et chacune des trois congruences suivantes :*

$$t^2 \equiv -bc \pmod{a}, \quad u^2 \equiv -ac \pmod{b}, \quad v^2 \equiv -ab \pmod{c}$$

possède une solution.

Remarque. En pratique, il suffira donc d'étudier trois congruences du type $x^2 \equiv y \pmod{m}$, d'inconnue x , pour conclure à l'existence ou non de points rationnels. Décomposant m en produit de nombre premiers : $m = \prod_{i=1}^r p_i$ (les p_i tous distincts : m est supposé sans facteur carré), on sait de plus, d'après le lemme Chinois, que $x^2 \equiv y \pmod{m}$

possède une solution si et seulement si toutes les congruences $x^2 \equiv y \pmod{p_i}$. En effet, une égalité $\bar{x}^2 = \bar{y}$ dans $\mathbb{Z}/m\mathbb{Z}$ correspond, via l'isomorphisme $\mathbb{Z}/m\mathbb{Z} \simeq \prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z}$, à $(x_1, \dots, x_r)^2 = (x_1^2, \dots, x_r^2) = (y_1, \dots, y_r)$. Il suffit donc de vérifier que y est un carré modulo chacun des p_i , par le calcul du symbole de Legendre $\left(\frac{y}{p_i}\right)$.

Preuve :

- Quitte à permuter éventuellement x, y et z , on peut supposer que $a > 0$ et $b > 0$.
- C'est une condition nécessaire : s'il existe une solution non triviale, soit (x, y, z) une solution primitive de l'équation. Il est clair que $cz^2 = -(ax^2 + by^2) < 0$ donc que $c < 0$. Par ailleurs, x, y et z sont premiers entre eux deux à deux : en effet, si $p \mid x$ et $p \mid y$ alors $p^2 \mid cz^2$; comme $p \nmid z$, on aurait donc $p^2 \mid c$, ce qui contredit l'hypothèse que c est sans facteur carré. Puis x et y sont premiers avec c (et permutations circulaires) : par exemple, si $p \mid x$ et $p \mid c$ alors $p \mid by^2$, ce qui est impossible car $\text{pgcd}(b, c) = \text{pgcd}(x, y) = 1$.

Soit p un nombre premier divisant a ; on calcule le symbole de Legendre :

$$\left(\frac{b}{p}\right) = \left(\frac{by^2}{p}\right) = \left(\frac{-ax^2 - cz^2}{p}\right) = \left(\frac{-cz^2}{p}\right) = \left(\frac{-c}{p}\right).$$

Ainsi $\left(\frac{-bc}{p}\right) = \left(\frac{b}{p}\right)^2 = +1$. D'après le théorème chinois, $-bc$ est un carré modulo a . Les autres congruences se démontrent de la même manière (permutation circulaire des inconnues x, y et z et des coefficients a, b et c).

- C'est une condition suffisante :
 - tout d'abord, on se ramène au cas où $ab, -ac$ et $-bc$ sont trois entiers naturels supérieurs ou égaux à deux : si $a = -c = 1$, $(1, 0, 1)$ est solution ; si $b = -c = 1$, $(0, 1, 1)$ est solution. Enfin, si $a = b = 1$, on peut prendre $z = 1$ et écrire c comme somme de deux carrés : puisque $-1 = -ab$ est un carré modulo c , c'est un carré modulo tout diviseur premier p de c , donc tout tel p vérifie $p \equiv 1 \pmod{4}$. C'est exactement la condition nécessaire et suffisante vue au premier chapitre pour une écriture $c = x^2 + y^2$.
 - Soit $f(X, Y, Z) = aX^2 + bY^2 + cZ^2 \in \mathbb{Z}[X, Y, Z] =: A$; montrons que l'on peut écrire $f(X, Y, Z) \equiv g(X, Y, Z)h(X, Y, Z) \pmod{abc}$ (ou encore $\bar{f} = \bar{g}\bar{h}$, égalité dans $A/(abc) \simeq (\mathbb{Z}/abc\mathbb{Z})[X, Y, Z]$), où g et h sont deux polynômes homogènes de degré un : on a

$$af(X, Y, Z) \equiv a^2X^2 + abY^2 \equiv a^2X^2 - t^2Y^2 \equiv (aX + bY)(aX - bY) \pmod{c},$$

donc f factorise modulo c en un produit de deux facteurs linéaires ; de même modulo a et b . On utilise alors le lemme chinois, appliqué à l'anneau A : via $A/(abc) \simeq A/(a) \times A/(b) \times A/(c)$, on construit g et h à partir des facteurs linéaires modulo a, b et c .

- Utilisant un argument de comptage (principe des tiroirs), nous montrons qu'il existe une racine non triviale de f modulo abc : considérons les triplets d'entiers (x, y, z) tels que

$$0 \leq x \leq \sqrt{-bc}, \quad 0 \leq y \leq \sqrt{-ac}, \quad 0 \leq z \leq \sqrt{ab}.$$

Il y en a

$$(1 + [\sqrt{-bc}])(1 + [\sqrt{-ac}])(1 + [\sqrt{ab}]) > \sqrt{-bc}\sqrt{-ac}\sqrt{ab} = -abc = \#\mathbb{Z}/abc\mathbb{Z};$$

donc $(x, y, z) \mapsto g(x, y, z) \pmod{abc}$ n'est pas injective : il existe deux tels triplets (x_i, y_i, z_i) , $i = 1, 2$, distincts, tels que $g(x_1, y_1, z_1) \equiv g(x_2, y_2, z_2) \pmod{abc}$. Posons $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$ et $z_0 = z_1 - z_2$; alors (x_0, y_0, z_0) n'est pas le triplet nul, mais il vérifie $g(x_0, y_0, z_0) \equiv 0 \pmod{abc}$, donc également $f(x_0, y_0, z_0) \equiv 0 \pmod{abc}$.

- Nous avons $x_0 \leq [\sqrt{-bc}] < \sqrt{-bc}$ car $-bc$ n'est pas un carré; de même, $y_0 < \sqrt{-bc}$ et $z_0 < \sqrt{ab}$, d'où les inégalités $0 \leq ax_0^2 < -abc$, $0 \leq by_0^2 < -abc$ et $abc < cz_0^2 \leq 0$. Il en résulte l'encadrement $abc < f(x_0, y_0, z_0) < -2abc$. Donc $f(x_0, y_0, z_0) = 0$ ou $-abc$. Dans le premier cas, c'est terminé; dans le second, le triplet $(x, y, z) = (x_0z_0 + by_0, y_0z_0 - ax_0, z_0^2 + ab)$ vérifie

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 + c(z_0^2 + ab)^2 = (z_0^2 + ab)(ax_0^2 + by_0^2 + cz_0^2 + abc) = 0.$$

Enfin, expliquons pourquoi le premier énoncé, que j'attribue également à Legendre, est bien équivalent au théorème que nous venons de démontrer. Il s'agit de montrer que les conditions du théorème 2.4.1 sont suffisantes (i.e. entraînent l'existence d'un zéro rationnel non trivial); nous allons voir qu'elles impliquent les conditions du théorème 2.4.2.

- La condition $abc < 0$ est clairement équivalente à celle d'une solution réelle (non triviale) : si a, b et c sont de même signe, disons positif, l'équation $cz^2 = -(ax^2 + by^2)$ ne possède pas de solution réelle; dans le cas contraire, on en trouve toujours une.
- Notons $\Delta = 8abc$ le discriminant de la forme quadratique $F = aX^2 + bY^2 + cZ^2$ (c'est le déterminant de la matrice B considérée plus haut). Rappelons que par hypothèse a, b et c sont des entiers relatifs non nuls premiers entre eux deux à deux et sans facteur carré. Réduisant les coefficients modulo un premier p , on considère la forme quadratique $\bar{F} = \bar{a}X^2 + \bar{b}Y^2 + \bar{c}Z^2$ sur le corps \mathbb{F}_p . Son discriminant est $\bar{\Delta}$. Donc lorsque p ne divise pas Δ , alors \bar{F} est non-dégénérée et la conique $\bar{C}_p : \bar{F} = 0$ est non-singulière. On a besoin de quelques lemmes.

Lemme 2.4.1. *Une forme quadratique $F(X, Y, Z)$ de rang 3 définie sur un corps fini (de caractéristique $p \neq 2$) est toujours singulière : il existe un triplet (x, y, z) différent du triplet nul tel que $F(x, y, z) = 0$.*

En effet, on se ramène à $F(X, Y, Z) = aX^2 + bY^2 + cZ^2$ et utilise alors un argument de comptage : on choisit $z = 1$ et cherche (x, y) tel que $ax^2 = -c - by^2$. Or il y a $(p-1)/2$ carrés dans \mathbb{F}_p^\times , donc $\{ax^2\}$ et $\{c - by^2\}$ sont deux ensembles de cardinal $(p+1)/2$, qui par conséquent ne peuvent être disjoints, car \mathbb{F}_p est de cardinal p .

Le passage de \mathbb{F}_p à \mathbb{Q}_p s'effectue via le «lemme de Hensel» (également rencontré au premier semestre, dans le cas d'une seule variable!) : un triplet solution de $\bar{F}(X, Y, Z) = 0$ dans $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ se relève en un triplet solution de $F(X, Y, Z) = 0$ dans \mathbb{Z}_p .

Lemme 2.4.2 (Hensel). *Soit $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ et $\underline{a} \in \mathbb{Z}^n$ tel que pour un certain $m \geq 0$ et un $r \geq 1$,*

$$f(\underline{a}) \equiv 0 \pmod{p^{2m+r}}$$

mais que pour un i

$$\left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}} \not\equiv 0 \pmod{p^{m+1}}.$$

Alors il existe un $\underline{b} \in \mathbb{Z}_p^n$ tel que $f(\underline{b}) \equiv 0 \pmod{p^{2m+r+1}}$ et $\underline{b} \equiv \underline{a} \pmod{p^{m+r}}$. De plus,

$$\left(\frac{\partial f}{\partial X_i} \right)_{\underline{b}} \not\equiv 0 \pmod{p^{m+1}}.$$

Preuve : on considère le développement

$$f(X_1, \dots, X_n) = f(a_1, \dots, a_n) + \sum_{i=1}^n \left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}} (X_i - a_i) + \text{termes de plus haut degré.}$$

Posons $b_i = a_i + h_i p^{m+r}$, où $h_i \in \mathbb{Z}$. Alors :

$$f(b_1, \dots, b_n) = f(a_1, \dots, a_n) + \sum_{i=1}^n \left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}} h_i p^{m+r} + \text{termes divisibles par } p^{2m+r+1}.$$

Il faut choisir les h_i tels que

$$f(a_1, \dots, a_n) + \sum_{i=1}^n \left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}} h_i p^{m+r}$$

soit divisible par p^{2m+r+1} . Par hypothèse, nous savons qu'il existe un $k \leq m$ tel que p^k divise $\left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}}$ pour tout i mais p^{k+1} ne les divise pas tous. Il suffit que les h_i vérifient

$$\frac{f(a_1, \dots, a_n)}{p^{m+k+r}} + \sum_{i=1}^n \frac{\left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}}}{p^k} h_i \equiv 0 \pmod{p},$$

condition que l'on peut toujours satisfaire en prenant $h_i = 0$ sauf pour un indice i tel que $\frac{\left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}}}{p^k}$ est inversible modulo p . Enfin, comme $\underline{b} = \underline{a} + \underline{h} p^{m+r}$, alors

$$\left(\frac{\partial f}{\partial X_i} \right)_{\underline{b}} = \left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}} + p^{m+r} \left(\frac{\partial f}{\partial X_i} \right)_{\underline{h}}$$

par linéarité de la dérivation ; on voit que $\left(\frac{\partial f}{\partial X_i} \right)_{\underline{b}} \equiv \left(\frac{\partial f}{\partial X_i} \right)_{\underline{a}} \pmod{p^{m+r}}$, d'où résulte $\left(\frac{\partial f}{\partial X_i} \right)_{\underline{b}} \not\equiv 0 \pmod{p^{m+1}}$ tout comme pour \underline{a} .

Corollaire. *Sous les hypothèses du lemme précédent avec $r = 1$, il existe un $\underline{b} \in \mathbb{Z}_p^n$ tel que $f(\underline{b}) = 0$ et $\underline{b} \equiv \underline{a} \pmod{p^{m+1}}$.*

Preuve : appliquant le lemme précédent avec $r = 1$, on trouve $\underline{a}_{2m+2} \in \mathbb{Z}^n$ tel que $\underline{a}_{2m+2} \equiv \underline{a} \pmod{p^{m+1}}$ et $f(\underline{a}_{2m+2}) \equiv 0 \pmod{p^{2m+2}}$. On applique alors le lemme à \underline{b} avec $r = 2$ pour construire \underline{a}_{2m+3} , etc. La suite (\underline{a}_{2m+r}) , où $r \geq 2$, vérifie $f(\underline{a}_{2m+r}) \equiv 0 \pmod{p^{2m+r}}$ et $\underline{a}_{2m+r+1} \equiv \underline{a}_{2m+r} \pmod{p^{m+r}}$. Comme $|\underline{a}_{2m+s} - \underline{a}_{2m+r}|_p \leq p^{-(m+r)}$ pour $s \geq r \geq 2$, la suite (\underline{a}_{2m+r}) est de Cauchy dans \mathbb{Z}_p^r , donc converge vers un $\underline{b} \in \mathbb{Z}_p^r$.

Comme $f : \mathbb{Z}_p^r \rightarrow \mathbb{Z}_p$ est une fonction polynôme, c'est une application continue pour la topologie p -adique, donc

$$f(\underline{b}) = f(\lim_r \underline{a}_{2m+r}) = \lim_r f(\underline{a}_{2m+r}) = 0.$$

Le lemme de Hensel s'applique ici, pour tout premier $p \nmid \Delta$, avec $m = 0$ car la conique \bar{C}_p est non-singulière (cf lemme 2.4.1). L'existence d'une solution non triviale dans les \mathbb{Q}_p , pour $p \nmid \Delta$ est donc automatique. Par conséquent, l'essence des conditions du théorème 2.4.1 se situe dans les conditions d'existence pour $p \mid \Delta = 8abc$ (bien que cette remarque soit inutile pour la démonstration du théorème 2.4.1, elle est essentielle à la compréhension de l'équivalence entre les deux théorèmes).

- Supposons que $p \mid a$; notre équation s'écrit $pa'X^2 + bY^2 + cZ^2 = 0$, où $p \nmid a'bc$. Soit (x, y, z) une solution non triviale dans \mathbb{Q}_p ; quitte à multiplier par une puissance convenable de p , on peut supposer que $(x, y, z) = (x_n, y_n, z_n)_{n \geq 1}$ est un triplet primitif de \mathbb{Z}_p . Alors le triplet (x_1, y_1, z_1) de $\mathbb{Z}/p\mathbb{Z}$ vérifie $y_1 \neq 0, z_1 \neq 0$ et $\bar{b}y_1^2 + \bar{c}z_1^2 = 0$. En effet, si $y_1 = z_1 = 0$, parce que (x_2, y_2, z_2) relève (x_1, y_1, z_1) et que $pa'x_2^2 + by_2^2 + cz_2^2 = 0$ dans $\mathbb{Z}/p^2\mathbb{Z}$, alors p diviserait un représentant \tilde{x}_2 de x_2 et l'on aurait $x_1 = 0$ également, ce qui contredirait la primitivité du triplet.

Regardons maintenant à quelle condition $\bar{b}Y^2 + \bar{c}Z^2 = 0$ possède une solution non triviale dans \mathbb{F}_p . Comme un élément non nul est inversible, c'est équivalent à dire que $-\bar{b}\bar{c}^{-1}$ est un carré de \mathbb{F}_p , ou encore, en multipliant par \bar{c}^2 , que $-bc$ est un carré modulo p . Finalement, demander qu'il existe une solution dans \mathbb{F}_p pour tous les $p \mid a$ est équivalent par le lemme Chinois (et parce que a est sans facteur carré) à demander que $-bc$ est un carré modulo a . On retrouve les conditions de Legendre. Finalement, on a montré que les conditions de Legendre sont équivalentes à l'existence d'un \mathbb{R} -point et d'un \mathbb{Q}_p -point pour tout premier p , d'où le principe de Hasse pour les coniques projectives (non dégénérées).

- Petite remarque : qu'en est-il du cas $p = 2$ (cas restant, pour $p \mid \Delta$)? On peut démontrer que l'existence d'une solution non triviale dans \mathbb{R} et tous les \mathbb{Q}_p , *sauf* l'un (qui peut être \mathbb{R} ou l'un des \mathbb{Q}_p), implique l'existence d'une solution non triviale dans tous les complétés de \mathbb{Q} . Cela explique pourquoi le cas $p = 2$ ne donne pas de condition nécessaire supplémentaire.

Répondons à la seconde question : comment décrire l'ensemble des points rationnels (à supposer que ce dernier soit non vide). Partons de $P_0 \in C(\mathbb{Q})$; d'après le théorème de Bezout, une droite (à pente rationnelle) passant par P_0 qui n'est pas la tangente en P_0 recoupe la courbe en un seul autre point (qui sera également rationnel). Dans le cas de la tangente en P_0 , ce point P_0 est le «second» point d'intersection (compté avec multiplicité). Finalement, on obtient une bijection entre l'ensemble des points rationnels et l'ensemble des droites passant par P_0 , donc avec $\mathbb{P}^1(\mathbb{Q})$.

Exemple. Si l'on choisit $P_0 = (-1 : 0 : 1)$ sur la courbe $C : X^2 + Y^2 = Z^2$, une droite passant par P_0 a pour équation $bX - aY + bZ = 0$ ($a, b \in \mathbb{Q}$ non tous les deux nuls). Si $a \neq 0$, on multiplie l'équation par a^2 et remplace aY par $b(X + Z)$: on obtient $(a^2 + b^2)X^2 + 2b^2XZ + (b^2 - a^2)Z^2 = 0$. Comme P_0 vérifie cette équation, nous savons que l'on peut mettre $X + Z$ en facteur, d'où $(X + Z)((a^2 + b^2)X + (b^2 - a^2)Z) = 0$. Prenant $X = a^2 - b^2$ et $Z = a^2 + b^2$, on trouve $Y = 2ab$. Le second point d'intersection est donc $(a^2 - b^2 : 2ab : a^2 + b^2)$. Lorsque $a = 0$, on remplace Z par $-X$ et trouve $Y^2 = 0$,

d'où le point $(-1 : 0 : 1)$. La formule précédente donne donc encore le bon résultat dans le cas $a = 0$. En conclusion, la bijection recherchée est $(a : b) \mapsto (a^2 - b^2 : 2ab : a^2 + b^2)$, de $\mathbb{P}^1(\mathbb{Q})$ sur $C(\mathbb{Q})$. Notons qu'il s'agit là de la paramétrisation rationnelle du cercle déjà invoquée lors de la résolution de l'équation de Fermat pour $n = 2$ (on a une bijection entre l'ensemble des triplets Pythagoriciens primitifs et l'ensemble $C(\mathbb{Q})$) : notre courbe est incluse entièrement dans le sous-espace affine $U_0 = \{(x : y : z), z \neq 0\}$ (il n'y a pas de point rationnel à l'infini), donc il suffit de considérer $C_0 : x^2 + y^2 = 1$.

Il reste la question subsidiaire : nous disposons déjà d'un algorithme permettant de décider de l'existence d'un point rationnel (cf remarque après l'énoncé du théorème de Legendre). Mais peut-on déterminer algorithmiquement un tel point ? La preuve du théorème de Legendre apporte une réponse : il suffit de tester tous les triplets (x, y, z) tels que $0 \leq x \leq \sqrt{-bc}, 0 \leq y \leq \sqrt{-ac}$ et $0 \leq z \leq \sqrt{ab}$. Cette méthode n'est cependant guère performante. L'algorithme suivant, dû à Legendre également, est meilleur (bien que l'on puisse encore l'améliorer !) :

- On se ramène à une équation du type $X^2 - aY^2 = bZ^2$, où a et b sont des entiers relatifs non nuls sans facteur carré (non nécessairement premiers entre eux). Par symétrie, on peut supposer $0 < |a| \leq |b|$. Nous cherchons un triplet primitif solution. L'idée est de se ramener à une équation de la même forme avec des nouveaux coefficients a et b tels que la quantité $|a| + |b|$ est strictement plus petite qu'à l'étape précédente. Ce processus de descente nous ramène au cas où $|a| = 1$ ou $|b| = 1$, qui se résout trivialement.
- On suppose donc $|b| \geq 2$; on résout alors la congruence $u^2 \equiv a \pmod{b}$ et choisit une solution u telle que $|u| \leq |b|/2$. Posons $u^2 - a = bt$. On a $|t| = |u^2 - a|/|b| < |b|$ car $|u^2 - a| \leq b^2/4 + |b| < b^2$ lorsque $|b| \geq 2$. On considère alors la nouvelle équation $X_1^2 - aY_1^2 = tZ_1^2$.
- Il reste à expliquer comment on déduit d'une solution non triviale (x_1, y_1, z_1) de $X_1^2 - aY_1^2 = tZ_1^2$ une solution non triviale (x, y, z) de $X^2 - aY^2 = bZ^2$: les formules sont les suivantes :

$$x = ux_1 - ay_1, \quad y = x_1 - uy, \quad z = tz_1.$$

Comme $u^2 \neq a$ puisque a est sans facteur carré, (x, y, z) est non triviale. Un petit calcul montre qu'il s'agit bien d'une solution. En fait, posant $z = tz_1$, les formules pour x et y proviennent de la remarque suivante : il faut que

$$bz^2 = (bt)(tz_1^2) = (u^2 - a)(x_1^2 - ay_1^2) = x^2 - ay^2;$$

travaillant dans $\mathbb{Q}(\sqrt{a})$, il suffit que

$$(u + \sqrt{a})(x_1 - y_1\sqrt{a}) = x + y\sqrt{a}.$$

Exercice. Appliquer l'algorithme de Legendre à l'équation $11X^2 + 13Y^2 = 19Z^2$.

2.4.2. Cas des courbes elliptiques

Soit C une cubique non-singulière définie sur \mathbb{Q} . Alors C est une courbe elliptique si et seulement si elle possède un point rationnel. La question naturelle est de savoir si

le principe de Hasse s'applique pour les cubiques non-singulières. La réponse est non : on peut démontrer que la courbe $3X^3 + 4Y^3 = 5Z^3$ n'admet pas de point rationnel, bien qu'elle admette un point réel et un point dans chaque corps p -adique.

Supposons maintenant que C soit une courbe elliptique ; comment pouvons-nous décrire l'ensemble $C(\mathbb{Q})$? Mordell a démontré en 1922 le résultat suivant :

Théorème 2.4.3. *Soit C une courbe elliptique définie sur \mathbb{Q} . Il existe un nombre fini de points de C à coordonnées dans \mathbb{Q} à partir desquels tous les autres points à coordonnées dans \mathbb{Q} peuvent être obtenus par des constructions successives de cordes et de tangentes.*

En fait, Mordell n'avait pas réalisé que $C(\mathbb{Q})$ constituait un groupe (ce qui a compliqué un peu sa preuve). En termes de la théorie des groupes, on énonce plutôt :

Théorème 2.4.4 (Mordell). *Soit C une courbe elliptique définie sur \mathbb{Q} . Alors $C(\mathbb{Q})$ est un groupe abélien de type fini.*

On peut donc écrire

$$C(\mathbb{Q}) = \mathbb{Z}^r \oplus C(\mathbb{Q})_{tors},$$

où $C(\mathbb{Q})_{tors}$ désigne le sous-groupe de torsion (c'est un groupe fini) et r , qui est le rang de la partie libre \mathbb{Z}^r du \mathbb{Z} -module $C(\mathbb{Q})$, est par définition le *rang de la courbe elliptique* C .

Quelques mots de la preuve du théorème de Mordell : les deux ingrédients essentiels sont les suivants :

- On démontre que le quotient $C(\mathbb{Q})/2C(\mathbb{Q})$ est fini ; si l'on prend un système de représentants (P_1, \dots, P_m) des classes, alors $P \in C(\mathbb{Q})$ peut s'écrire $P = P_i + 2P'$, pour un certain i et $P' \in C(\mathbb{Q})$. On réitère alors l'opération sur P' et ainsi de suite.
- Intuitivement, P' est «plus petit» que P ; ainsi, en un nombre fini d'étape, on est ramené à un $P^{(k)}$ «petit» et les «petits points rationnels» sont en nombre fini. Plus précisément, on définit la *hauteur* d'un point $P = (x : y : 1)$ comme étant $H(P) = \max(|m|, |n|)$, où $x = m/n$ avec m et n premiers entre eux (et $H(O) = 1$ dans le cas du neutre O). C'est la hauteur qui va diminuer à chaque étape du processus de descente. De plus, $\{P \in C(\mathbb{Q}) | H(P) \leq C\}$, pour C un réel quelconque, est fini : en effet, les rationnels x s'écrivant m/n avec m et n des entiers relatifs bornés, sont en nombre fini.

La question concerne désormais l'existence d'algorithmes permettant de déterminer le rang d'une courbe elliptique ainsi que la partie de torsion. Nous allons énoncer à la fin de ce chapitre le «théorème de Nagell-Lutz» qui permet de calculer $E(\mathbb{Q})_{tors}$ (et que vous appliquerez en TP). Concernant la détermination du rang, il n'existe pas d'algorithme non-conjectural (c'est-à-dire dont on sache prouver qu'il donne effectivement le bon résultat) le calculant dans tous les cas ; nous en dirons un peu plus en évoquant la conjecture de Birch et Swinnerton-Dyer. En fait, on ne sait même pas démontrer qu'il existe des courbes elliptiques de rang arbitraire (c'est-à-dire aussi grand que l'on veut). Par contre, on peut donner un listing des différents $E(\mathbb{Q})_{tors}$ susceptibles d'apparaître. Outre le rang, on aimerait disposer d'un système de générateurs ; les algorithmes répondant à ce problème pour une courbe elliptique quelconque ne sont pas

très performants : pour commencer, on recherche systématiquement un certain nombre de points rationnels de petite hauteur.

2.4.3. Et en degré supérieur ?

Mordell a conjecturé qu'une courbe projective plane non singulière de degré supérieur ou égal à quatre n'admet qu'un nombre fini de points à coordonnées dans \mathbb{Q} . Cette célèbre conjecture de Mordell a été démontrée par Faltings en 1983, ce qui lui valut la médaille Fields...

2.5. Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

2.5.1. Théorème de Hasse

Soit C une courbe elliptique définie sur un corps fini \mathbb{F}_q de caractéristique p (i.e. $q = p^r$). Lorsque $p > 2$, elle possède une équation de Weierstrass $y^2 = f(x)$ où f est un polynôme de degré trois de $\mathbb{F}_q[X]$; lorsque $p > 3$, on peut se ramener à une équation courte $y^2 = x^3 + ax + b$. Pour $p = 2$, on doit considérer une équation de Weierstrass longue.

Comme \mathbb{F}_q est un corps fini, le groupe $E(\mathbb{F}_q)$ est fini. Plus précisément, $\mathbb{P}^2(\mathbb{F}_q)$ possède $(q^3 - 1)/(q - 1)$ points, donc E possède au plus $1 + q + q^2$ points. On peut affiner cette majoration : pour chaque valeur de x , il y a au plus deux valeurs de y pour lesquelles (x, y) appartient à $E(\mathbb{F}_q)$, puisque $y^2 = f(x)$; d'où la majoration $\#E(\mathbb{F}_q) \leq 2q + 1$ (en comptant le point à l'infini). En fait, il s'avère que le nombre de x pour lesquels $f(x)$ est un carré est environ égal au nombre de x pour lesquels $f(x)$ n'est pas un carré, de sorte que le nombre de \mathbb{F}_q -points est environ $q + 1$. Le théorème suivant précise cela :

Théorème 2.5.1 (Hasse). *Soit E une courbe elliptique définie sur le corps fini \mathbb{F}_q ; alors :*

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

Autrement dit, le nombre de \mathbb{F}_q -points est compris entre $q + 1 - 2\sqrt{q} = (1 - \sqrt{q})^2$ et $(1 + \sqrt{q})^2$.

Exemple. La courbe E définie sur \mathbb{F}_3 par l'équation $y^2 = f(x) = x^3 - x + 1$ est non singulière car le discriminant est $\Delta = -23 \neq 0$ dans \mathbb{F}_3 . Comme $f(1) = f(-1) = f(0) = 1$ dans \mathbb{F}_3 , qui est un carré, il y a six points affines donc sept points en tout. Cela correspond à la borne supérieure de l'estimation de Hasse qui nous dit que E possède entre un et sept points. Comme 7 est premier, $E(\mathbb{F}_3)$ est donc un groupe cyclique d'ordre 7; on peut vérifier que $P = (0, 1)$ est un générateur.

2.5.2. Réduction modulo p

Rappelons qu'un point de $\mathbb{P}^2(\mathbb{Q})$ peut s'écrire, de façon unique au signe près, sous la forme $(x : y : z)$, où (x, y, z) est un triplet primitif d'entiers. Cela permet de définir, pour p un nombre premier, une application $\mathbb{P}^2(\mathbb{Q}) \rightarrow \mathbb{P}^2(\mathbb{F}_p)$ par $(x : y : z) \mapsto (\bar{x}, \bar{y}, \bar{z})$, où la barre désigne la réduction des entiers modulo p .

D'autre part, soit C une courbe projective plane donnée par un polynôme $F \in \mathbb{Q}[X, Y, Z]$; quitte à multiplier F par un entier (non nul) convenable, on peut supposer que les coefficients de F sont entiers et premiers dans leur ensemble. Alors, réduisant tous les coefficients modulo p , on obtient un polynôme homogène $\bar{F} \in \mathbb{F}_p[X, Y, Z]$ de même degré que F . La courbe projective plane, définie sur \mathbb{F}_p , ainsi obtenue s'appelle la *réduction de C modulo p* ; on la note \bar{C}_p .

Remarque. Lorsque C est une courbe elliptique sous forme de Weierstrass $y^2 = x^3 + ax + b$, où a et b sont rationnels, on effectue le changement de variables $x \rightsquigarrow x/c^2$ et $y \rightsquigarrow y/c^3$ (de sorte que la forme de Weierstrass est conservée tout en restant dans la même classe d'isomorphisme), l'entier c étant choisi tel que les nouveaux a et b soient entiers (et souvent, on demande que $|\Delta|$ soit minimal, où Δ est le nouveau discriminant).

Finalement, si $P \in C(\mathbb{Q})$, on peut considérer \bar{P} ; il est clair que \bar{P} appartient à $\bar{C}_p(\mathbb{F}_p)$. Cela définit une application $C(\mathbb{Q}) \rightarrow \bar{C}_p(\mathbb{F}_p)$.

La proposition suivante dit que cette application de réduction est, dans le cas des courbes elliptiques, un morphisme de groupes pour presque tous les premiers p :

Proposition 2.5.1. *Soit E une courbe elliptique définie sur \mathbb{Q} par une équation de Weierstrass $y^2 = f(x)$, où $f(x)$ est un polynôme de degré trois de $\mathbb{Z}[x]$ de discriminant Δ . Pour tous les nombres premiers p ne divisant pas 2Δ , l'application de réduction $E(\mathbb{Q}) \rightarrow \bar{E}_p(\mathbb{F}_p)$ est un morphisme de groupes.*

En effet, si p ne divise pas 2Δ , alors la cubique \bar{E}_p est non-singulière; c'est donc une courbe elliptique dont le point à l'infini est encore $(0 : 1 : 0)$ et sa loi de groupe est, comme pour E , définie par :

$$P_1 + P_2 + P_3 = O \text{ si et seulement si } P_1, P_2 \text{ et } P_3 \text{ sont alignés}$$

(avec la convention habituelle sur les multiplicités). Le résultat provient alors du fait que les droites se réduisent modulo p en des droites et que les multiplicités d'intersection sont également conservées par réduction.

2.5.3. Fonction L de Hasse-Weil et conjecture de Birch et Swinnerton-Dyer

Soit E une courbe elliptique définie sur \mathbb{Q} . On définit une fonction $L(E, s)$ de la variable complexe s par la formule suivante :

$$L(E, S) = \prod_p \frac{1}{1 + (N_p - p - 1)p^{-s} + p^{-2s}},$$

où $N_p = \#\bar{E}_p$. Cette formule est correcte pour les premiers p ne divisant pas 2Δ ; les facteurs correspondant à ces «mauvais p » diffèrent légèrement : on dispose de formules explicites que je ne donne pas ici. On démontre que ce produit infini converge absolument pour $\Re(s) > 3/2$. C'est la fonction L de Hasse-Weil associée à la courbe elliptique E . Depuis Wiles qui a démontré la conjecture de Taniyama-Shimura-Weil (d'où résulte le théorème de Fermat), nous savons que la fonction L se prolonge en une fonction méromorphe sur \mathbb{C} tout entier. En particulier, on peut considérer sa valeur au point $s = 1$.

Conjecture (Birch et Swinnerton-Dyer). $L(E, 1) = 0$ si et seulement si le rang de E est supérieur ou égal à un.

Remarque. En fait, cet énoncé est une version faible de la conjecture de Birch et Swinnerton-Dyer, qui prédit très exactement que le rang r de la courbe elliptique est égal à l'ordre du zéro de la fonction méromorphe $L(E, s)$ en $s = 1$. Cette conjecture vaut un million de dollars ! Sa profondeur et sa beauté est de relier une quantité analytique (on dit que l'ordre d'annulation de la fonction L en $s = 1$ est le «rang analytique» de la courbe elliptique) et un nombre r lié à la géométrie de la courbe et sa structure algébrique : elle affirme l'étonnante égalité du rang analytique et du rang algébrique.

En pratique, r est donc le plus petit entier ρ tel que la dérivée ρ -ième $L^{(\rho)}(E, s)$ ne s'annule pas en $s = 1$. Cependant, il est difficile de décider numériquement de l'annulation d'une telle fonction. L'algorithme de détermination du rang, dû à Manin, fait intervenir outre la conjecture de Birch et Swinnerton-Dyer d'autres ingrédients de nature algébrique. Un autre algorithme, dû à Cremona, n'utilise pas la conjecture de Birch et Swinnerton-Dyer ; c'est l'algorithme le plus «performant» à ce jour, mais il n'aboutit pas toujours (à la différence de l'algorithme conjectural précédent).

2.6. Courbes elliptiques et nombres congruents

On rappelle qu'un *nombre congruent* est un entier naturel qui représente l'aire d'un triangle rectangle dont les côtés sont rationnels.

Proposition 2.6.1. *Soit n un entier naturel ; les propositions suivantes sont équivalentes :*

- (i) $n = \frac{1}{2}ab$, pour un triplet Pythagoricien rationnel (a, b, c) ;
- (ii) il existe trois carrés rationnels en progression arithmétique de raison n ;
- (iii) la courbe elliptique C_n donnée par l'équation de Weierstrass $y^2 = x^3 - n^2x$ possède un point rationnel distinct des solutions triviales $(\pm n, 0)$, $(0, 0)$ (qui correspondent aux points d'ordre 2) et du point à l'infini.

Preuve :

- (i) \Rightarrow (ii) : posant $x = (\frac{c}{2})^2$, on a $(\frac{a-b}{2})^2 = \frac{a^2+b^2}{4} - \frac{ab}{2} = x - n$ et $(\frac{a+b}{2})^2 = x + n$.
- (ii) \Rightarrow (i) : la progression arithmétique étant $x - n, x, x + n$, les nombres $a = \sqrt{x+n} + \sqrt{x-n}$, $b = \sqrt{x+n} - \sqrt{x-n}$ et $c = 2\sqrt{x}$ sont rationnels et vérifient $a^2 + b^2 = c^2$.
- (ii) \Rightarrow (iii) : notant toujours $x - n, x, x + n$ les trois carrés rationnels, leur produit $x^3 - n^2x$ est alors un carré, disons y^2 . Le point (x, y) appartient donc à C_n ; ce n'est aucun des points cités : en effet, la progression arithmétique est à termes positifs et ce ne peut être $0, n, 2n$ car $2n$ n'est pas un carré rationnel lorsque n est un carré rationnel.
- (iii) \Rightarrow (ii) : Soit P un point rationnel de C_n qui ne correspond pas à une solution triviale. Alors $y \neq 0$ donc P n'est pas d'ordre deux ; comme $2P \neq O$, on peut donc écrire $2P = (x', y')$. Il résulte du lemme suivant que $x', x' - n$ et $x' + n$ sont des carrés rationnels.

Lemme 2.6.1. *Soit E une courbe elliptique définie sur un corps k de caractéristique différente de 2 par une équation de Weierstrass $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ où les*

racines α_i du trinôme appartiennent à k . Alors un point $P = (x_0, y_0) \neq O$ appartient à $2E(k)$ si et seulement si les $x_0 - \alpha_i$ sont tous les trois des carrés de k .

Démontrons le lemme :

- On peut supposer que $x_0 = 0$. En effet, effectuant le changement de variable $x' = x - x_0$, un point $P' = (0, y_0) \neq O$ de $E' : y^2 = (x' - \alpha'_1)(x' - \alpha'_2)(x' - \alpha'_3)$ appartient à $2E'(k)$ si et seulement si P appartient à $2E(k)$ (simple translation de la figure ; or l'addition est définie géométriquement). De même, les $x_0 - \alpha_i$ sont des carrés si et seulement si les $0 - \alpha'_i$ le sont.
- S'il existe $Q \in E(k)$ tel que $2Q = P$, alors il existe exactement quatre tels points Q . En effet, comme la multiplication par 2 est un morphisme, on trouve toutes les solutions en rajoutant à une solution particulière les éléments du noyau, c'est-à-dire O et les points $(\alpha_i, 0)$ d'ordre 2. On pose donc $Q_i = Q + (\alpha_i, 0)$.
- Géométriquement, ces quatre points s'interprètent comme suit : $2Q = P$ s'écrit $2Q + (-P) = O$; c'est équivalent, par la définition géométrique de l'addition, à demander que la tangente à E en Q passe par $-P$. L'équation d'une droite D passant par $-P = (0, -y_0)$ est de la forme $y = px - y_0$; on veut que la multiplicité d'intersection en un k -point $Q = (x_1, y_1)$ de $E \cap D$ soit deux, donc que l'équation

$$(px - y_0)^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3, \quad (*)$$

où les σ_i sont les fonctions symétriques en les racines α_i , possède une racine double x_1 dans k (l'autre racine étant $x_0 = 0$). Explicitement, en regardant le coefficient en x^2 , on trouve $x_1 = (\alpha_1 + \alpha_2 + \alpha_3 + p^2)/2$, donc x_1 appartient à k si p appartient à k (et réciproquement, puisque la pente d'une droite passant par deux points k -rationnels appartient à k).

- Simplifions l'équation (*) : comme $\sigma_3 = \alpha_1 \alpha_2 \alpha_3 = -y_0^2$ (car $(0, y_0)$ appartient à E), on trouve après simplification par x :

$$x^2 - (p^2 + \sigma_1)x + (2py_0 + \sigma_2) = 0.$$

Le trinôme admet une racine double si et seulement si son discriminant est nul, i.e. :

$$\Delta = (p^2 + \sigma_1)^2 - 4(2py_0 + \sigma_2) = 0.$$

Le problème est donc ramené à montrer que ce polynôme de degré quatre en p admet une (et donc quatre) racine(s) dans k si et seulement si les $-\alpha_i$ sont des carrés dans k .

- Les σ_i s'expriment en fonction des α_i ; cependant, Δ fait également intervenir y_0 qui lui ne s'exprime pas en fonction des α_i (mais $y_0^2 = -\sigma_3$ oui !). On introduit alors des β_i (pris dans une clôture algébrique de k) tels que $\beta_i^2 = -\alpha_i$ et que $y_0 = \beta_1 \beta_2 \beta_3$. Cette dernière condition peut toujours être remplie : si $\alpha_i \neq 0$, alors il existe deux choix pour β_i qui diffèrent par un signe ± 1 et il s'agit d'ajuster les signes, sachant que si l'un des α_i est nul, le β_i correspondant est nul et la relation est trivialement vérifiée. Un tel triplet de β_i étant déterminé, les autres triplets convenables sont les :

$$(\beta_1, -\beta_2, -\beta_3) \quad (-\beta_1, \beta_2, -\beta_3) \quad (-\beta_1, -\beta_2, \beta_3)$$

(avec éventuelle redondance si des α_i sont nuls).

- Maintenant, tous les coefficients de Δ sont des polynômes symétriques en les β_i ; ils peuvent donc s'écrire en terme des fonctions symétriques élémentaires σ'_i en les β_i . Précisément :

$$\begin{aligned}\sigma_1 &= -\beta_1^2 - \beta_2^2 - \beta_3^2 = -(\sigma'_1)^2 + 2\sigma'_2; \\ \sigma_2 &= \beta_1^2\beta_2^2 + \beta_1^2\beta_3^2 + \beta_2^2\beta_3^2 = (\sigma'_2)^2 - 2\sigma'_1\sigma'_3; \\ y_0 &= \sigma'_3.\end{aligned}$$

Ainsi :

$$\Delta = (p^2 - (\sigma'_1)^2 + 2\sigma'_2)^2 - 4((\sigma'_2)^2 - 2\sigma'_1\sigma'_3 + 2p\sigma'_3).$$

- On voit que $p_1 = \sigma'_1 = \beta_1 + \beta_2 + \beta_3$ est racine évidente. Comme on aurait pu faire trois autres choix de signes pour les β_i , les trois autres racines correspondent à ces choix ; ce sont $p_2 = \beta_1 - \beta_2 - \beta_3$, $p_3 = -\beta_1 + \beta_2 - \beta_3$ et $p_4 = -\beta_1 - \beta_2 + \beta_3$. Comme $\beta_1 = (p_1 + p_2)/2$, $\beta_2 = (p_1 + p_3)/2$ et $\beta_3 = (p_1 + p_4)/2$, on voit que les p_i appartiennent à k si et seulement si les β_i appartiennent à k , donc si et seulement si les $-\alpha_i$ sont des carrés de k . Cela démontre la proposition.

Le lien entre nombres congruents et courbes elliptiques est dorénavant établi : le problème se ramène à l'étude du groupe de Mordell-Weil $\mathbb{C}_n(\mathbb{Q})$. Notamment, on se demande s'il existe d'autres points, outre les quatre points $(0, 0)$, $(\pm n, 0)$ et O (point à l'infini) qui forment un sous-groupe isomorphe au groupe abstrait $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Nous allons montrer que la partie de torsion $\mathbb{C}_n(\mathbb{Q})_{tors}$ se réduit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, d'où résulte la :

Proposition 2.6.2. *Un entier naturel non nul n est congruent si et seulement si la courbe elliptique $C_n : y^2 = x^3 - n^2x$ est de rang supérieur ou égal à un.*

L'idée est d'utiliser les applications de réduction $\pi_p : C_n(\mathbb{Q}) \rightarrow \bar{C}_n(\mathbb{F}_p)$ qui, pour $p \nmid 2\Delta$ (c'est-à-dire p premier impair et $p \nmid n$), sont des morphismes de groupe. On espère, connaissant les $\bar{C}_n(\mathbb{F}_p)$ pour différents p , regrouper ces informations afin d'en déduire $C_n(\mathbb{Q})_{tors}$. Par exemple, si l'on sait de plus que π_p est injective sur la partie de torsion, alors l'image de $C_n(\mathbb{Q})_{tors}$ par π_p est un sous-groupe de $\bar{C}_n(\mathbb{F}_p)$ isomorphe à $C_n(\mathbb{Q})_{tors}$, d'où la relation suivante entre les cardinaux : $\#C_n(\mathbb{Q})_{tors} \mid \#\bar{C}_n(\mathbb{F}_p)$.

Nous avons besoin de deux lemmes :

Lemme 2.6.2. *Soit p un nombre premier tel que $p \nmid n$ et $p \equiv 3 \pmod{4}$. Alors $\#\bar{C}_p(\mathbb{F}_p) = p + 1$.*

Preuve : Nous avons trois points correspondant à $y = 0$, à savoir $(\pm n, 0)$ et $(0, 0)$. Il reste donc $p - 3$ valeurs possibles pour x , et pour chaque valeur on se demande si $f(x) = x^3 - n^2x$ est un carré modulo p . Comme $p \equiv 3 \pmod{4}$, nous savons que -1 n'est pas un carré modulo p ; par conséquent, l'application $x \mapsto -x$ change le signe du résidu quadratique. Ainsi l'ensemble $\{f(x), f(-x) = -f(x)\}$ contient-il exactement un carré modulo p ; il lui correspond deux points de $\bar{C}_p(\mathbb{F}_p) : (x, \pm\sqrt{f(x)})$ ou $(-x, \pm\sqrt{f(-x)})$. On obtient une telle paire de \mathbb{F}_p -points pour chaque paire $\{x, -x\}$, donc $p - 3$ \mathbb{F}_p -points. En rajoutant les trois points précédents et le point à l'infini, on obtient le chiffre annoncé.

Lemme 2.6.3. Soient P_1 et P_2 deux points d'une courbe C définie sur \mathbb{Q} et $\pi_p : C(\mathbb{Q}) \rightarrow \bar{C}(\mathbb{F}_p)$ l'application de réduction modulo un nombre premier p . Alors $\pi_p(P_1) = \pi_p(P_2)$ si et seulement si p divise le produit vectoriel de P_1 et P_2 (en tant que vecteurs de \mathbb{R}^3).

Preuve : Ecrivons $P_i = (x_i : y_i : z_i)$ ($i = 1, 2$) où les coordonnées projectives sont entières et premières dans leur ensemble.

- Supposons que p divise le produit vectoriel de P_1 et P_2 et montrons que $\pi_p(P_1) = \pi_p(P_2)$. On raisonne par disjonction de cas : si p divise x_1 , alors il divise également x_2 . En effet, p divise $x_2z_1 - x_1z_2$ et $x_1y_2 - x_2y_1$ par hypothèse et il ne divise pas simultanément y_1 et z_1 ; pour fixer les idées, on supposera que $p \nmid y_1$. Par hypothèse, p divise également $y_1z_2 - y_2z_1$; donc $p \nmid y_2$ et $\pi_p(P_1) = (0 : \bar{y}_1 : \bar{z}_1) = (0 : \bar{y}_2\bar{y}_1 : \bar{y}_2\bar{z}_1) = (0 : \bar{y}_1\bar{y}_2 : \bar{y}_1\bar{z}_2) = (0 : \bar{y}_2 : \bar{z}_2) = \pi_p(P_2)$. Si par contre p ne divise pas x_1 , alors il ne divise pas x_2 et $\pi_p(P_1) = (\bar{x}_1 : \bar{y}_1 : \bar{z}_1) = (\bar{x}_2\bar{x}_1 : \bar{x}_2\bar{y}_1 : \bar{x}_2\bar{z}_1) = (\bar{x}_1\bar{x}_2 : \bar{x}_1\bar{y}_2 : \bar{x}_1\bar{z}_2) = (\bar{x}_2 : \bar{y}_2 : \bar{z}_2) = \pi_p(P_2)$. Dans les deux cas, $\pi_p(P_1) = \pi_p(P_2)$.
- Réciproquement, supposons que $\pi_p(P_1) = \pi_p(P_2)$. Comme p ne divise pas simultanément x_1 , y_1 et z_1 , nous supposons pour fixer les idées que $p \nmid x_1$. Alors p ne divise pas x_2 , puisque $(\bar{x}_2 : \bar{y}_2 : \bar{z}_2) = (\bar{x}_1 : \bar{y}_1 : \bar{z}_1)$. Ainsi $(\bar{x}_2\bar{x}_1 : \bar{x}_2\bar{y}_1 : \bar{x}_2\bar{z}_1) = \pi_p(P_1) = \pi_p(P_2) = (\bar{x}_1\bar{x}_2 : \bar{x}_1\bar{y}_2 : \bar{x}_1\bar{z}_2)$ dans $\mathbb{P}^2(\mathbb{F}_p)$. Comme les premières coordonnées coïncident, il en est de même des deux autres. Donc p divise $x_2z_1 - x_1z_2$ et $x_1y_2 - x_2y_1$. En particulier, si p divise y_1 , alors il divise également y_2 , donc aussi $y_1z_2 - y_2z_1$. Si par contre il ne divise pas y_1 , alors le même raisonnement que pour x_1 montre la divisibilité de $y_1z_2 - y_2z_1$ par p . On a démontré que p divise le produit vectoriel de P_1 et P_2 .

Corollaire. Soit C une courbe elliptique définie sur \mathbb{Q} . L'application de réduction $\pi_p : C(\mathbb{Q})_{tors} \rightarrow \bar{C}(\mathbb{F}_p)$ est injective pour tous les nombres premiers p sauf un nombre fini d'entre eux.

En effet, $C(\mathbb{Q})_{tors}$ est un groupe fini ; il n'y a qu'un nombre fini de premiers p divisant les coordonnées des produits vectoriels que l'on peut fabriquer avec les points de torsion.

Remarque. On verra plus loin que l'application de réduction $\pi_p : C(\mathbb{Q})_{tors} \rightarrow \bar{C}(\mathbb{F}_p)$ est toujours injective pour $p \nmid 2\Delta$. Le lemme élémentaire précédent suffit pour l'instant à nos besoins.

Combinant les deux lemmes, on en déduit que $\#C(\mathbb{Q})_{tors} \mid p + 1$ pour presque tous les nombres premiers $p \equiv 3 \pmod{4}$, ou encore que presque tous les nombres premiers $p \equiv 3 \pmod{4}$ vérifient $p \equiv -1 \pmod{\#C(\mathbb{Q})_{tors}}$. Par l'absurde, si $\#C(\mathbb{Q})_{tors} \neq 4$, soit il existerait un diviseur impair m de $\#C(\mathbb{Q})_{tors}$, soit $C(\mathbb{Q})_{tors}$ serait d'ordre 2^s , avec $s \geq 3$, auquel cas $m = 8$ diviserait $\#C(\mathbb{Q})_{tors}$. Si $m = 8$, considérons les nombres premiers $p \equiv 3 \pmod{8}$: ils seraient en nombre fini, puisque tous les $p \equiv 3 \pmod{4}$, sauf un nombre fini, vérifieraient $p \equiv -1 \pmod{8}$ (car $8 \mid \#C(\mathbb{Q})_{tors}$). Si m est impair et $3 \nmid m$, on considère les premiers $p \equiv 3 \pmod{4m}$, sinon les $p \equiv 7 \pmod{12}$; dans chaque cas, le modulo divise $\#C(\mathbb{Q})_{tors}$ (et $(3, 4m) = 1 = (7, 12)$), de sorte que ces nombres premiers seraient également en nombre fini. On aboutit à une contradiction avec le :

Théorème 2.6.1 (de la progression arithmétique de Dirichlet). *Soit $m \geq 1$, et soit a tel que $(a, m) = 1$. L'ensemble des nombres premiers p tels que $p \equiv a \pmod{m}$ est infini.*

Le lecteur intéressé trouvera dans [Se] Chapitre VI une démonstration.

La dernière étape consiste à trouver un critère efficace pour déterminer si la courbe elliptique $C_n : y^2 = x^3 - n^2x$ n'est pas de rang nul. Etant données les difficultés liées au calcul du rang en général, cette étape s'annonce délicate. Effectivement, nous dirons juste, de manière vague, qu'aux courbes elliptiques C_n on associe des «formes modulaires» qui admettent un développement de Fourier, dont le n^e terme s'exprime en fonction de $L(C_n, 1)$. Tunnel démontre ainsi :

Théorème 2.6.2 (Tunnel, 1983). *Soit n un entier naturel impair (resp. pair) sans facteur carré tel que n soit congruent. Alors*

$$\#\{(x, y, z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2} \#\{(x, y, z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 8z^2\}$$

(resp.

$$\#\{(x, y, z) \in \mathbb{Z}^3 \mid \frac{n}{2} = 4x^2 + y^2 + 32z^2\} = \frac{1}{2} \#\{(x, y, z) \in \mathbb{Z}^3 \mid \frac{n}{2} = 4x^2 + y^2 + 8z^2\}).$$

Réciproquement, si la conjecture de Birch et Swinnerton-Dyer est vraie pour la courbe elliptique $C_n : y^2 = x^3 - n^2x$, alors cette égalité implique que n est un nombre congruent.

Remarque. Un sens de la conjecture de Birch et Swinnerton-Dyer, pour une certaine classe de courbes elliptiques dont les C_n font partie, a été démontrée par Coates et Wiles. C'est pourquoi, dans l'énoncé du théorème de Tunnel, la référence à cette conjecture n'est faite qu'au niveau de la réciproque. Les détails se trouvent dans [Ko1].

2.7. Détermination de $E(\mathbb{Q})_{\text{tors}}$

2.7.1. Courbes elliptique sur \mathbb{Q}_p

Soit E une courbe elliptique définie sur \mathbb{Q}_p par une équation de Weierstrass $y^2 = x^3 + ax + b$. Après un éventuel changement de variable $x \rightsquigarrow x/c^2$ et $y \rightsquigarrow y/c^3$, on peut supposer que a et b appartiennent à \mathbb{Z}_p . Alors, via l'application $\mathbb{Z}_p \rightarrow \mathbb{F}_p \simeq \mathbb{Z}_p/p\mathbb{Z}_p$ de réduction modulo p appliquée aux coefficients, on obtient une courbe \bar{E}_p définie sur \mathbb{F}_p par une équation $y^2 = x^3 + \bar{a}x + \bar{b}$ (c'est une courbe elliptique lorsque $2\Delta \notin p\mathbb{Z}_p$). D'autre part, si $P = (x : y : z) \in \mathbb{P}^2(\mathbb{Q}_p)$, on représente P par son unique représentant $(x : y : z)$ où les trois coordonnées appartiennent à \mathbb{Z}_p et forment un triplet primitif (i.e. x, y et z n'appartiennent pas tous les trois à $p\mathbb{Z}_p$); cela définit une application $\mathbb{P}^2(\mathbb{Q}_p) \ni P \mapsto \bar{P} \in \mathbb{P}^2(\mathbb{F}_p)$ de réduction modulo p . Cette dernière induit une application $E(\mathbb{Q}_p) \rightarrow \bar{E}(\mathbb{F}_p)$.

Soit $\bar{E}_{ns}(\mathbb{F}_p)$ le groupe formé des \mathbb{F}_p -points non-singuliers de \bar{E}_p et $E^0(\mathbb{Q}_p)$ l'image réciproque de $\bar{E}_{ns}(\mathbb{F}_p)$ par l'application de réduction modulo p . Autrement dit,

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \bar{P} \text{ est non singulier}\}.$$

C'est un sous-groupe de $E(\mathbb{Q}_p)$ et l'application induite $\phi_p : E^0(\mathbb{Q}_p) \rightarrow \bar{E}_{ns}(\mathbb{F}_p)$ est un morphisme de groupes : cela provient du fait que la loi de groupe est définie géométriquement (et la réduction modulo p transforme une droite en une droite et conserve les multiplicités d'intersection). De plus, on peut toujours relever un \mathbb{F}_p -point non singulier de \bar{E}_p en un \mathbb{Q}_p -point de E : c'est le lemme de Hensel. En conclusion, ϕ_p est surjective. Soit $E^1(\mathbb{Q}_p)$ son noyau ; alors $E^0(\mathbb{Q}_p)/E^1(\mathbb{Q}_p) \simeq \bar{E}_{ns}(\mathbb{F}_p)$.

Soit $P = (x : y : z)$ un élément de $E^1(\mathbb{Q}_p)$; comme $\bar{P} = (\bar{0} : \bar{1} : \bar{0})$, alors x et z sont divisibles par p mais pas y , qui est donc une unité de \mathbb{Z}_p . On définit alors

$$E^n(\mathbb{Q}_p) = \{P \in E^1(\mathbb{Q}_p) \mid \frac{x(P)}{y(P)} \in p^n \mathbb{Z}_p\}.$$

On vient de définir une chaîne de sous-groupes $E(\mathbb{Q}_p) \supset E^0(\mathbb{Q}_p) \supset E^1(\mathbb{Q}_p) \supset \dots$. On parle de «filtration de $E(\mathbb{Q}_p)$ » (de longueur infinie). Notons que \mathbb{Z}_p possède également une filtration par la valuation : $\mathbb{Z}_p = F^0 \supset F^1 = p\mathbb{Z}_p \supset F^2 = p^2\mathbb{Z}_p \supset \dots$ et $x \mapsto p^{-n}x \pmod p$ définit un isomorphisme entre F^n/F^{n+1} et \mathbb{F}_p . On démontre (voir [Ca] §11 par exemple) que l'application $P \mapsto p^{-n} \frac{x(P)}{y(P)} \pmod p$ définit un isomorphisme entre $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p)$ et le groupe additif \mathbb{F}_p pour $n \geq 1$.

La filtration précédente est la clef de la proposition suivante :

Proposition 2.7.1. *Le groupe $E^1(\mathbb{Q}_p)$ est sans torsion.*

En effet, soit P est un point de $E^1(\mathbb{Q}_p)$ d'ordre fini m . Nous allons traiter le cas où $p \nmid m$: soit n l'unique entier tel que $P \in E^n(\mathbb{Q}_p) \setminus E^{n+1}(\mathbb{Q}_p)$; alors l'image de P dans $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \simeq \mathbb{F}_p$ n'est pas 0, tandis que l'image de $mP = O$ est 0. Alors m serait un multiple de p , d'où la contradiction. Le cas où $p \mid m$ nécessite une analyse plus fine du comportement de l'addition des points par rapport à la filtration ; on aboutit également à une contradiction (cf [Ca] §11).

Corollaire. *Si $P = (x : y : 1) \in E(\mathbb{Q}_p)_{tors}$, alors $x, y \in \mathbb{Z}_p$.*

Preuve : nous allons montrer que si $P = (x : y : 1) \notin E^1(\mathbb{Q}_p)$, alors $x, y \in \mathbb{Z}_p$. Comme un point de torsion n'appartient pas à $E^1(\mathbb{Q}_p)$, cela démontre le corollaire. Nous procédons par contraposée et supposons que x ou y n'appartient pas à \mathbb{Z}_p . Alors, en multipliant par une puissance de p convenable, on écrit $P = (x' : y' : z')$, où le triplet est un triplet primitif d'éléments de \mathbb{Z}_p . Nécessairement, $z' \in p\mathbb{Z}_p$; notant $\bar{P} \in \bar{E}(\mathbb{F}_p)$ la réduction de P modulo p , on a $z(\bar{P}) = 0$, donc \bar{P} est le point à l'infini $(\bar{0} : \bar{1} : \bar{0})$. Par conséquent, P appartient bien à $E^1(\mathbb{Q}_p)$, ce qui démontre l'assertion.

Corollaire. *Si $P = (x : y : 1) \in E(\mathbb{Q})_{tors}$, alors $x, y \in \mathbb{Z}$.*

En effet, un tel point p appartient à tous les \mathbb{Z}_p . Autrement dit, la p -valuation de x et y est positive ou nulle pour tout premier p ; les rationnels x et y sont donc des entiers.

Les points de torsion ont donc des coordonnées entières (au sens de l'énoncé précédent). Ce corollaire est l'un des deux ingrédients essentiels de la preuve du théorème de Nagell-Lutz. Avant de citer et démontrer ce dernier, énonçons un dernier corollaire, utile parfois dans la recherche des points rationnels :

Corollaire. Soit p un nombre premier ne divisant pas 2Δ . Alors le morphisme $\pi_p : E(\mathbb{Q})_{tors} \rightarrow \bar{E}(\mathbb{F}_p)$ de réduction modulo p est injectif.

En effet, $E^1(\mathbb{Q}_p)$ est le noyau du morphisme $E(\mathbb{Q}) \rightarrow \bar{E}(\mathbb{F}_p)$; donc $\ker(\pi_p) = E^1(\mathbb{Q}_p) \cap E(\mathbb{Q})_{tors} = \{O\}$.

Il résulte de ce corollaire que $\#E(\mathbb{Q})_{tors} \mid \#\bar{E}(\mathbb{F}_p)$ pour tout premier $p \nmid 2\Delta$, fait déjà utilisé dans la résolution du problème des nombres congruents.

2.7.2. Théorème de Nagell-Lutz

Soit E une courbe elliptique définie sur \mathbb{Q} par une équation de Weierstrass $y^2 = f(x) = x^3 + ax + b$ de discriminant Δ . Avec le raisonnement habituel, on peut supposer que a et b sont des entiers relatifs. On dit qu'un point rationnel P de E a des «coordonnées entières» si $P = O$ ou $P = (x : y : 1)$ avec $x, y \in \mathbb{Z}$. On a vu qu'un point de torsion a des coordonnées entières (c'est le corollaire 2.7.1). On pourra donc lui appliquer le lemme suivant :

Lemme 2.7.1. Soit $P = (x, y)$ un point rationnel de E tel que P et $2P$ ont des coordonnées entières. Alors $y = 0$ ou $y^2 \mid \Delta$.

Preuve : Supposons que $y \neq 0$ et démontrons que $y^2 \mid \Delta$. Comme P n'est pas d'ordre deux (car $y \neq 0$), on peut écrire $2P = (x_1, y_1)$. Par hypothèse, x, y, x_1 et y_1 sont des entiers. D'après les formules de duplication (vues en TP), $x_1 = \alpha^2 - 2x$, où $\alpha = \frac{f'(x)}{2y}$ est la pente de la tangente en P . Ainsi α est un rationnel dont le carré est entier : c'est donc un entier. Par conséquent, $2y$ divise $f'(x)$; en particulier, $y \mid f'(x)$.

D'autre part, il résulte de la théorie générale du résultant et du discriminant (voir par exemple [Ca] §16) que le discriminant Δ appartient à l'idéal de $\mathbb{Z}[x]$ engendré par $f(x)$ et $f'(x)$: autrement dit, on peut écrire $\Delta = r(x)f(x) + s(x)f'(x)$ dans $\mathbb{Z}[x]$. Sans faire appel à loc. cit., le lecteur pourra vérifier l'égalité suivante : $4a^3 + 27b^2 = [-27(x^3 + ax - b)](x^3 + ax + b) + [(3x^2 + 4a)(3x^2 + a)](3x^2 + a)$. Comme $y^2 = f(x)$, alors y^2 divise à la fois $f(x)$ et $f'(x)^2$. La relation précédente montre que y^2 divise Δ .

Nous venons de démontrer le :

Théorème 2.7.1 (Nagell-Lutz). Soit E une courbe elliptique définie sur \mathbb{Q} par une équation de Weierstrass $y^2 = x^3 + ax + b$, où a et b sont deux entiers relatifs, et soit $P \neq O$ un point rationnel d'ordre fini. Alors $P = (x, y)$ a des coordonnées entières vérifiant ou bien $y = 0$ ou bien $y^2 \mid \Delta = 4a^3 + 27b^2$.

Remarque. La réciproque n'est pas vraie : un point $P = (x : y : 1)$ peut vérifier les conditions du théorème sans être un point de torsion pour autant.

L'intérêt en pratique du théorème de Nagell-Lutz pour la recherche des points de torsion est évident : il fournit directement un algorithme de recherche de ces points.

- On décompose l'entier Δ et recherche tous les entiers y tels que $y^2 \mid \Delta$.
- Pour chaque y trouvé (ainsi que $y = 0$), on résout $f(x) = y^2$, où $f(x) = x^3 + ax + b$: un entier x solution divisera $b - y^2$, d'où à nouveau un nombre fini de possibilités.

- On a ainsi obtenu une liste finie de points rationnels incluant tous les points de torsion. Il reste à déterminer lesquels sont d'ordre fini. Pour cela, on calcule les nP , où $n \geq 2$, jusqu'à ce que l'on trouve O ou bien que l'on aboutisse à un nP qui n'est pas dans la liste. En effet, si P est d'ordre infini, alors les nP sont tous distincts, donc on sortira bien de la liste finie. Alternativement, on peut calculer les itérés jusqu'à obtenir O ou un nP dont les coordonnées ne sont pas entières : en effet, si tous les itérés avaient des coordonnées entières, on pourrait leur appliquer le lemme 2.7.1 ; il n'y en aurait donc qu'un nombre fini.

Vous menerez cette démarche en TP sur des cas concrets.

2.7.3. Théorème de Mazur

Examinons sur quelques exemples la structure du groupe $E(\mathbb{Q})_{tors}$:

Exemple. Soit $E : y^2 = x^3 + 3$. On calcule $\Delta = 3^5$.

1. Première méthode : $p = 5$ et $p = 7$ ne divisent pas 2Δ et l'on dénombre facilement $\#\bar{E}(\mathbb{F}_5) = 6$ et $\#\bar{E}(\mathbb{F}_7) = 13$. Comme $\#E(\mathbb{Q})_{tors}$ divise à la fois 6 et 13, qui sont premiers entre eux, on voit que O est le seul point de torsion. En particulier, cela montre que $(1, 2) \in E(\mathbb{Q})$ est d'ordre infini, donc E est de rang strictement positif.
2. Seconde méthode : d'après le théorème de Nagell-Lutz, on sait que $y \in \{0, \pm 1, \pm 3, \pm 9\}$. Ensuite, il faut que $x \mid 3 - y^2$; on vérifie que ces x ne conviennent pas en traitant tous les cas possibles. Alternativement, on peut argumenter comme suit : $y = 0$ et $y = \pm 1$ ne donnent clairement aucun point rationnel ; si $3 \mid y$, alors $3 \mid x$ également, puis $3 = y^2 - x^3$ serait divisible par 9, d'où la contradiction.

Exemple. Soit $E : y^2 = x^3 + x$. On calcule $\Delta = 2^2$.

1. Première méthode : on calcule $\#\bar{E}(\mathbb{F}_3) = 4$, $\#\bar{E}(\mathbb{F}_5) = 4$, $\#\bar{E}(\mathbb{F}_7) = 8$. C'est insuffisant pour conclure : on a $\#E(\mathbb{Q})_{tors} \in \{1, 2, 4\}$. Explicitons nos groupes finis :

$$\begin{aligned}\bar{E}(\mathbb{F}_3) &= \{\bar{O}, (\bar{0}, \bar{0}), (-\bar{1}, \bar{1}), (-\bar{1}, -\bar{1})\}, \\ \bar{E}(\mathbb{F}_5) &= \{\bar{O}, (\bar{0}, \bar{0}), (-\bar{2}, \bar{0}), (-\bar{2}, -\bar{0})\}.\end{aligned}$$

Comme les points d'ordre deux sont exactement les $\bar{P} = (x, y)$ ou $y = 0$, on voit que $\bar{E}(\mathbb{F}_3) \simeq \mathbb{Z}/4\mathbb{Z}$ alors que $\bar{E}(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Or $E(\mathbb{Q})_{tors}$ est isomorphe à un sous-groupe de chacun de ces deux groupes. Comme $(0, 0) \in E(\mathbb{Q})$ est d'ordre deux, alors $E(\mathbb{Q})_{tors} = \{O, (0, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

2. Seconde méthode : d'après Nagell-Lutz, $y \in \{0, \pm 1, \pm 2\}$. Il faut que $x \mid y^2$, d'où peu de cas à regarder...

Exemple. Soit $E : y^2 = x^3 - 43x + 166$. On calcule $\Delta = 2^{15} \cdot 13$. Nous combinons les deux méthodes :

- on calcule $\#\bar{E}(\mathbb{F}_3) = 7$, donc $E(\mathbb{Q})_{tors} = \{O\}$ ou $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$.
- appliquant Nagell-Lutz, on trouve facilement le point rationnel $P = (3, 8)$. On vérifie par le calcul qu'il est d'ordre 7.

La question naturelle qui se pose est la suivante : quels sont les groupes finis qui apparaissent en tant que sous-groupe de torsion des points rationnels des courbes elliptiques ? Le théorème de Mazur (démontré en 1977) y répond ; sa preuve est difficile et fait appel à des techniques qui dépassent de loin celles mises en oeuvre jusqu'à présent.

Théorème 2.7.2. *Soit E une courbe elliptique définie sur \mathbb{Q} . Alors $E(\mathbb{Q})_{tors}$ est isomorphe à l'un des groupes abstraits suivants : $\mathbb{Z}/n\mathbb{Z}$ (pour $1 \leq n \leq 10$), $\mathbb{Z}/12\mathbb{Z}$, ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ (pour $1 \leq n \leq 4$).*

Remarque. Toutes ces quinze possibilités apparaissent bien ; le lecteur trouvera à l'exercice 2.12 page 62 de [S-T] des exemples couvrant tous les cas énumérés.

A. Annexes au chapitre 1

A.1. Anneaux factoriels

Soit A un anneau intègre

Définition A.1.1. *Soit $a \in A - (A^\times \cup \{0\})$; on dit que a est irréductible si*

$$a = bc \Rightarrow b \in A^\times \text{ ou } c \in A^\times$$

et a est premier si

$$a \mid bc \Rightarrow a \mid b \text{ ou } a \mid c.$$

Définition A.1.2. *On dit que A est factoriel si tout élément $a \in A - (A^\times \cup \{0\})$ se décompose en produit d'irréductibles, et si la décomposition est unique à l'ordre près des facteurs, et à des éléments inversibles près.*

(pour avoir l'unicité, on choisit un système de représentants des irréductibles)

Remarque. Exemple d'anneau non factoriel : $A = \mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5}, a, b \in \mathbb{Z}\}$; on a $A^\times = \{\pm 1\}$ (en utilisant $N(z) = |z|^2$). Il y a deux décompositions de 6 en facteurs irréductibles :

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

De même, $\mathbb{C}[X, Y]/(Y^2 - X^3)$ n'est pas factoriel : l'image \bar{Y} de Y est un élément irréductible non premier.

Proposition A.1.1 (critère de factorialité). *A est factoriel si et seulement si les conditions suivantes sont satisfaites :*

- (i) *toute suite croissante d'idéaux principaux est stationnaire ($(a_1) \subset (a_2) \subset \dots (a_n) = (a_{n+1}) = \dots$: égalité à partir d'un certain rang)*
- (ii) *tout irréductible est premier*

((i) correspond en gros à l'existence d'une factorisation et (ii) à l'unicité)

Définition A.1.3. *On dit que A est Noethérien s'il vérifie l'une ou l'autre des conditions équivalentes suivantes :*

- (i) toute suite croissante d'idéaux est stationnaire
- (ii) tout idéal est de type fini

((i) du critère de factorialité est une condition plus faible que Noethérien)

Corollaire. *Tout anneau principal est factoriel.*

En effet, il vérifie (ii) de la définition d'un anneau Noethérien ; de plus, si p est irréductible, alors l'idéal (p) est maximal (utilise la primalité : si $(p) \subsetneq I = (\alpha)$, alors $\alpha \mid p$, ce qui contredit l'irréductibilité) ; il est donc premier, donc p est premier.

Rappel :

- I premier $\Leftrightarrow A/I$ est intègre et $\neq \{0\}$;
- I maximal $\Leftrightarrow A/I$ est un corps

Remarque. $K[X, Y]$, K un corps, est factoriel mais pas principal : l'idéal $(X) + (Y)$ n'est pas principal ; $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal, mais pas Euclidien.

Factorialité et anneaux de polynômes :

Proposition A.1.2. *Si A est factoriel, alors $A[X]$ aussi.*

(donc $K[X, Y] = (K[X])[Y]$ est factoriel)

A.2. Excursion au pays des corps de nombres

Les corps de nombres sont les extensions finies de \mathbb{Q} . Nous allons considérer au chapitre 1 les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$, qui sont reliés respectivement aux corps de nombres $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$.

Rappelons tout d'abord que si $K \subset L$ sont deux corps, on dit que K est un sous-corps de L et que L est une *extension* de K . On peut alors regarder L comme un K -espace vectoriel et la dimension $\dim_K(L)$ est par définition le *degré* de l'extension de corps, noté parfois $[L : K]$. Par exemple, $[\mathbb{C} : \mathbb{R}] = 2$ et $[\mathbb{C} : \mathbb{Q}] = \infty$.

Remarque. Si $F \subset K \subset E$ sont trois corps emboîtés, on peut démontrer la formule de transitivité du degré : $[E : F] = [E : K][K : F]$.

Soit $K \subset L$ une extension de corps et $\alpha \in L$.

Définition A.2.1. *On dit que α est algébrique sur K s'il existe $P \in K[X]$, $P \neq 0$ tel que $P(\alpha) = 0$. Sinon α est transcendant sur K .*

Par exemple, $\sqrt{2}, i$ sont algébriques sur \mathbb{Q} , tandis que π et e sont transcendants.

Une variante de la définition est la suivante : considérons le morphisme d'anneaux $\Psi_\alpha : K[X] \ni P \mapsto P(\alpha) \in L$. On note $K[\alpha]$ son image, qui est le plus petit anneau contenant K et α . On a :

- soit $\ker \Psi_\alpha = (0)$; alors α est transcendant sur K et $K[\alpha]$ est isomorphe à l'anneau de polynômes $K[X]$
- soit $\ker \Psi_\alpha = (P)$; alors α est algébrique sur K et $K[\alpha] \simeq K[X]/(P)$. Comme $K[\alpha] \subset L$ est intègre, l'idéal est premier donc P est irréductible. C'est par définition le *polynôme minimal de α sur K* (on le choisit unitaire).

On note $K(\alpha)$ le corps des fractions de $K[\alpha]$. C'est le plus petit corps contenant K et α .

Proposition A.2.1. *Les assertions suivantes sont équivalentes :*

- (i) α est algébrique sur K
- (ii) $K[\alpha] = K(\alpha)$
- (iii) $\dim_K K(\alpha) < \infty$ (et alors $[K(\alpha) : K]$ est le degré du polynôme minimal de α sur K)

(i) \Leftrightarrow (ii) :

- si α est algébrique sur K , $\ker \Psi_\alpha$ est un idéal premier donc maximal, car $K[X]$ est principal. Par conséquent, $K[\alpha] \simeq K[X]/(P)$ est un corps.
- si α est transcendant sur K , alors $K[\alpha] \simeq K[X]$ n'est pas un corps.

(i) \Leftrightarrow (iii) :

- si α est algébrique sur K et n est le degré du polynôme minimal P , alors $(1, X, \dots, X^{n-1})$ forme une base de $K[\alpha] \simeq K[X]/(P)$ (cf cours d'algèbre linéaire)
- si α est transcendant sur K , alors $K[\alpha] \simeq K[X]$ est de dimension infinie sur K .

Ainsi $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ sont des extensions finies de \mathbb{Q} , de degré 2, les polynômes minimaux de i et j étant $X^2 + 1$ et $X^2 + X + 1$ respectivement. En effet, ces polynômes sont irréductibles dans $\mathbb{Q}[X]$. On a la description suivante : $\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ (de même pour $\mathbb{Q}(j)$).

Enfin, $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont définis comme suit : on note $\mathbb{Z}[\alpha]$ l'image du morphisme d'anneaux $\mathbb{Z}[X] \ni P \mapsto P(\alpha) \in \mathbb{C}$. Ils jouent pour $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ respectivement le même rôle que joue \mathbb{Z} pour \mathbb{Q} . Ce sont les *anneaux des entiers* associés aux corps de nombres $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$.

Remarque. Si $K \supset \mathbb{Q}$ est un corps de nombres, l'anneau des entiers O_K de K est par définition l'ensemble des éléments de K qui sont *entiers* sur \mathbb{Z} , c'est-à-dire racine d'un polynôme *unitaire* à coefficients dans \mathbb{Z} . L'anneau des entiers est le coeur de la «théorie algébrique des nombres»; cet anneau n'est pas toujours principal (ce sera notre cas, pour les exemples précédents), mais il est possible de définir une «décomposition en idéaux premiers» qui remplace la décomposition en nombres premiers. Vous verrez cela dans le cours d'algèbre de maîtrise.

B. Annexes au chapitre deux

B.1. Le plan projectif

B.1.1. Définition

Soit k un corps. Le *plan projectif* sur k est

$$\mathbb{P}^2(k) = \{(x, y, z) \in k^3 \mid (x, y, z) \neq (0, 0, 0)\} / \sim$$

où $(x, y, z) \sim (x', y', z')$ si et seulement si $(x', y', z') = \lambda(x, y, z)$ pour $\lambda \in k^\times$. On écrit $(x : y : z)$ pour la classe de (x, y, z) (cette notation suggère que seul importe les quotients des coordonnées, i.e. y/x et z/x si $x \neq 0$, ou x/y et z/y si $y \neq 0$).

Soit $P \in \mathbb{P}^2(k)$; les triplets (x, y, z) représentant P se situent sur une même droite $D(P)$ passant par l'origine, et $P \mapsto D(P)$ définit une bijection entre $\mathbb{P}^2(k)$ et l'ensemble de ces droites.

Remarque. L'espace projectif $\mathbb{P}^n(k)$ se définit de manière similaire pour tout entier $n \geq 0$.

Soit $U_0 = \{(x : y : z) | z \neq 0\}$ et $D_\infty(k) = \{(x : y : z) | z = 0\}$. Alors

$$(x, y) \in \mathbb{A}^2(k) \mapsto (x : y : 1) \in U_0$$

définit une bijection (l'application réciproque est $(x : y : z) \mapsto (x/z, y/z)$) ainsi que

$$(x : y) \in \mathbb{P}^1(k) \mapsto (x : y : 0) \in D_\infty(k).$$

De plus, $\mathbb{P}^2(k) = U_0 \sqcup D_\infty(k)$: le plan projectif $\mathbb{P}^2(k)$ est l'union disjointe du «plan affine» U_0 et de la «droite à l'infini» D_∞ . Deux droites affines parallèles de U_0 se coupent en un point de D_∞ (et un seul) : on peut ainsi voir $\mathbb{P}^2(k)$ comme U_0 plus un point à l'infini par famille de droites parallèles. Sur U_0 , $u = x/z, v = y/z$ constitue un système de coordonnées affines.

Soient maintenant $U_1 = \{(x : y : z) | x \neq 0\}$ et $U_2 = \{(x : y : z) | y \neq 0\}$. Alors U_1 et U_2 peuvent également être vus de façon naturelle comme des plans affines : par exemple, on identifie U_1 et $\mathbb{A}^2(k)$ via $(x : 1 : z) \mapsto (x, z)$. Comme au moins l'un parmi x, y et z est non nul, on a $\mathbb{P}^2(k) = U_0 \cup U_1 \cup U_2$. On dit parfois que $\{U_0, U_1, U_2\}$ constitue une *atlas* du plan projectif, constitué des trois *cartes* U_i .

B.1.2. Transformations projectives

Une matrice M de $\mathrm{GL}_{n+1}(k)$ induit une application $\mathbb{P}^n(k) \rightarrow \mathbb{P}^n(k)$: puisque $Mv = 0$ si et seulement si $v = 0$, M agit sur $k^{n+1} \setminus \{(0, \dots, 0)\}$; comme $M(\lambda v) = \lambda M(v)$, elle «passe au quotient» pour la relation d'équivalence de colinéarité : si $v \sim v'$ alors $Mv \sim Mv'$.

Définition B.1.1. On appelle transformation projective une application $\mathbb{P}^n(k) \rightarrow \mathbb{P}^n(k)$ induite par un élément M de $\mathrm{GL}_{n+1}(k)$. L'ensemble des transformations projectives forme le groupe projectif, noté $\mathrm{PGL}_{n+1}(k)$.

Deux matrices M et M' induisent la même application si et seulement si elles diffèrent par multiplication par un scalaire : si $Mv \sim M'v$ pour tout v de $\mathbb{P}^n(k)$, ou encore $Mv = \lambda_v M'v$, on montre que λ_v ne dépend pas de v . Identifiant le sous-groupe de $\mathrm{GL}_{n+1}(k)$ constitué des matrices scalaires avec k^\times , on a donc $\mathrm{PGL}_{n+1}(k) \simeq \mathrm{GL}_{n+1}(k)/k^\times$.

Lemme B.1.1. Soient (P_1, P_2, P_3) et (Q_1, Q_2, Q_3) deux triplets de points non-colinéaires dans $\mathbb{P}^2(K)$. Alors il existe une unique transformation projective M vérifiant $MP_i = Q_i$ pour $i = 1, 2, 3$.

Lorsqu'une propriété est invariante par transformation projective, ce lemme permet de supposer qu'un point donné (ou triplet de points donnés) est $(0 : 0 : 1)$ (ou $(1 : 0 : 0)$, $(0 : 1 : 0)$ et $(0 : 0 : 1)$). On parle de «changement de coordonnées projectives» dans $\mathbb{P}^2(K)$.

B.2. Les nombres p -adiques

B.2.1. Motivation

L'entier 2 n'est pas un carré rationnel, mais si l'on passe de \mathbb{Q} à \mathbb{R} , l'équation $x^2 = 2$ possède deux solutions : $\pm\sqrt{2}$, où $\sqrt{2} = 1,414213\dots$. Cette écriture est l'écriture décimale de $\sqrt{2}$, tout réel pouvant s'écrire $x = \pm \sum_{k=-\infty}^n a_k 10^k$, où les $a_k \in \{0, \dots, 9\}$ (écriture unique, sauf pour les décimaux où $\dots c_n 000 \dots$ et $\dots (c_n - 1)999 \dots$ représentent le même nombre). On peut définir les réels de cette manière, l'inconvénient étant la définition des opérations.

Une autre façon de regarder le développement décimal de $\sqrt{2}$ est la suivante : on considère la suite (x_n) définie par $x_0 = 1$, $x_1 = 14/10$, $x_2 = 141/100$, etc... C'est une suite de Cauchy de rationnels qui n'admet pas de limite dans \mathbb{Q} mais converge vers $\sqrt{2}$ dans le corps complet \mathbb{R} . La définition moderne des réels passe par les suites de Cauchy : \mathbb{R} est le complété de \mathbb{Q} pour la valeur absolue archimédienne $|\bullet|$. Enfin, les rationnels x_n sont de approximations de $\sqrt{2}$ de plus en plus fines : $|\sqrt{2} - x_n| \leq 10^{-n}$.

Considérons maintenant la suite de congruences $x^2 \equiv 2 \pmod{7^n}$ pour $n = 1, 2, \dots$. Lorsque $n = 1$, on a deux solutions : $x = x_1 \equiv \pm 3 \pmod{7}$. Ce choix fait, les x_n ($n \geq 2$) sont uniquement déterminés : en effet, supposant x_n construit (et unique modulo 7^n), alors x_{n+1} vérifie également $x^2 \equiv 2 \pmod{7^n}$, donc $x_{n+1} \equiv x_n \pmod{7^n}$ par unicité. On écrit $x_{n+1} = x_n + c_n 7^n$ et $x_n^2 - 2 = d_n 7^n$; alors $x_{n+1}^2 - 2 \equiv x_n^2 - 2 + 2x_n c_n 7^n \pmod{7^{n+1}} \equiv d_n 7^n + 2x_n c_n 7^n \pmod{7^{n+1}}$. Il faut donc que $d_n + 2x_n c_n \equiv 0 \pmod{7}$, ce qui détermine c_n modulo 7 (x_n est inversible modulo 7), donc x_{n+1} modulo 7^{n+1} . Par exemple, si $x_1 = 3$, on trouve $c_n \equiv d_n \pmod{7}$, d'où la formule de récurrence $x_{n+1} \equiv x_n + x_n^2 - 2 \pmod{7^{n+1}}$.

Que se passe-t-il «à la limite», lorsque n tend vers l'infini ? La suite (x_n) possède-t-elle une limite ? D'une part, il n'existe pas d'entier x vérifiant $x^2 \equiv 2 \pmod{7^n}$ pour tout $n \geq 1$, car $x^2 - 2$ serait divisible par une puissance arbitraire de 7, ce qui n'est possible que si $x^2 - 2 = 0$. D'autre part, la série $\sum c_n 7^n$ (où $c_n \in \{0, \dots, 6\}$) ne converge pas dans \mathbb{R} , au sens usuel, pour la distance issue de la valeur absolue archimédienne.

Nous allons définir les «nombres p -adiques» (pour chaque nombre premier p). L'anneau \mathbb{Z}_p des entiers p -adiques contient \mathbb{Z} ; il est muni d'une distance, la «distance p -adique» issue de la «valeur absolue p -adique» $|\bullet|_p$. La série $\sum c_n 7^n$ converge pour la distance 7-adique; sa somme, notée x , est un entier 7-adique qui vérifie $x^2 = 2$ dans \mathbb{Z}_7 . L'écriture $x = \sum_{n=0}^{+\infty} c_n 7^n$ constitue le «développement 7-adique» de x .

Le corps \mathbb{Q}_p des nombres p -adiques est le corps des fractions de \mathbb{Z}_p ; il contient \mathbb{Q} . En fait, on peut également l'obtenir par «complétion» de \mathbb{Q} pour la distance p -adique.

B.2.2. Construction de \mathbb{Z}_p

On considère les $\mathbb{Z}/p^n\mathbb{Z}$; la projection $i_n : \mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ a pour noyau $p^n\mathbb{Z} \supset p^{n+1}\mathbb{Z}$, donc factorise à travers $\mathbb{Z} \rightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$. Les projections étant surjectives, on obtient des morphismes surjectifs $p_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$.

Définition B.2.1. \mathbb{Z}_p est la limite projective de ce système, c'est-à-dire l'ensemble des suites $(x_1, x_2, \dots, x_n, \dots) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \dots \times \mathbb{Z}/p^n\mathbb{Z} \dots$ qui vérifient $x_n = p_n(x_{n+1})$ pour tout $n \geq 1$.

On écrit $\mathbb{Z}_p = \varprojlim_{n \rightarrow +\infty} \mathbb{Z}/n\mathbb{Z}$. C'est un sous-ensemble de $\prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$, et en fait un sous-anneau pour les opérations héritées (car les projections sont des morphismes d'anneaux).

On a une inclusion naturelle $i : \mathbb{Z} \hookrightarrow \mathbb{Z}_p$: les morphismes i_n ($n \geq 1$) sont compatibles aux projections p_n (i.e. les idagrammes évidents commutent), donc définissent un morphisme i par la formule $i(x) = (i_n(x)) = (x \bmod p^n)$. Bien qu'aucun des i_n ne soit injectif, la résultante i est injective : si $i_n(x) = \bar{0}$ dans $\mathbb{Z}/p^n\mathbb{Z}$ pour tout n , alors p^n divise x pour tout n , d'où $x = 0$.

Développement p -adique d'un élément de \mathbb{Z}_p : soit $\underline{x} = (x_n) \in \mathbb{Z}_p$, où $x_n \in \mathbb{Z}/p^n\mathbb{Z}$, et soit \tilde{x}_n le représentant de x_n compris entre 0 et $p^n - 1$. Écrivons pour tout n l'entier \tilde{x}_n en base p : $\tilde{x}_n = c_0^{(n)} + c_1^{(n)}p + \cdots + c_{n-1}^{(n)}p^{n-1}$, où $c_i^{(n)} \in \{0, \dots, p-1\}$.

Lemme B.2.1. *Pour $i \leq n-1$, on a $c_i^{(n+1)} = c_i^{(n)}$.*

En effet, $x_{n+1} \equiv \tilde{x}_n \pmod{p^n}$ (puisque $x_n = p_n(x_{n+1})$) ; écrivant $x_{n+1} = \tilde{x}_n + p^n u$, on montre que $u \in \{0, \dots, p-1\}$: si $u < 0$, on aurait $x_{n+1} \leq \tilde{x}_n - p^n < 0$ et si $u \geq p$ alors $x_{n+1} \geq p^{n+1}$; c'est impossible. Donc $c_0^{(n)} + c_1^{(n)}p + \cdots + c_{n-1}^{(n)}p^{n-1} + up^n$ est l'écriture en base p de x_{n+1} ; on conclut par l'unicité de ce dernier.

Définition B.2.2. *On appelle développement p -adique de \underline{x} la suite infinie des chiffres $c_i : (c_0, c_1, \dots, c_n, \dots)$, $c_i \in \{0, p-1\}$. On note $\underline{x} = c_0 + c_1p + \cdots + c_np^n + \cdots$ (à prendre pour l'instant comme une écriture formelle).*

Nous venons d'associer à $\underline{x} \in \mathbb{Z}_p$ une suite infinie de chiffres. Réciproquement, étant donnée $(c_0, c_1, \dots, c_n, \dots)$, on lui associe $\underline{x} = (x_n) \in \mathbb{Z}_p$, où x_n est la classe de $c_0 + c_1p + \cdots + c_{n-1}p^{n-1}$ modulo p^n . Ces deux constructions sont réciproques l'une de l'autre : on peut se donner un entier p -adique par son développement p -adique.

B.2.3. Propriétés algébriques de \mathbb{Z}_p

Lemme B.2.2. *Soit $\underline{x} = (x_n) \in \mathbb{Z}_p$; alors \underline{x} est inversible dans \mathbb{Z}_p si et seulement si $x_1 \neq \bar{0}$.*

Preuve : le sens direct est évident ; étant donné un élément inversible $\underline{x} = (x_n)$ de \mathbb{Z}_p , la composante x_1 en particulier est inversible dans $\mathbb{Z}/p\mathbb{Z}$, donc non nulle. Réciproquement, soit \underline{x} tel que x_1 est inversible dans $\mathbb{Z}/p\mathbb{Z}$; nous noterons y_1 son inverse. Soit $y \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ et $p_n(y)$ son image par la projection $\mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$; on a le résultat général suivant :

Si $p_n(y)$ est inversible dans $\mathbb{Z}/p^n\mathbb{Z}$ alors y est inversible dans $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

En effet, les inversible de $\mathbb{Z}/p^n\mathbb{Z}$ sont les \bar{m} ou $(p, m) = 1$. Soit \tilde{y} un entier qui représente la classe y ; par hypothèse, la classe $p_n(y)$ de \tilde{y} modulo p^n est inversible, donc $(\tilde{y}, p) = 1$. Par conséquent, la classe y de \tilde{y} modulo p^{n+1} est également inversible.

Cela montre, de proche en proche, que les x_n sont inversibles dans $\mathbb{Z}/p^n\mathbb{Z}$; nous notons y_n les inverses. Montrons que $y_n = p_n(y_{n+1})$: appliquant p_n à l'égalité $x_{n+1}y_{n+1} = \bar{1}$, on obtient $x_np_n(y_{n+1}) = \bar{1}$ et conclut par l'unicité de l'inverse.

Lemme B.2.3. *Si \underline{x} n'est pas inversible dans \mathbb{Z}_p alors il existe $\underline{y} \in \mathbb{Z}_p$ tel que $\underline{x} = p\underline{y}$. Réciproquement, $p\underline{y}$ n'est pas inversible.*

Preuve : D'après le lemme précédent, si $\underline{x} = (x_n)$ n'est pas inversible, alors $x_1 = 0$. Le représentant de x_1 dans $\{0, \dots, p-1\}$ est donc $c_0 = 0$ et le développement p -adique s'écrit $c_1p + \dots + c_n p^n + \dots$ (somme «formelle»). L'entier p -adique \underline{y} dont le développement p -adique est $c_1 + \dots + c_n p^{n-1} + \dots$ vérifie $\underline{x} = p\underline{y}$: en effet, x_n est la classe de $c_1p + \dots + c_{n-1}p^{n-1}$ modulo p^n et y_n celle de $c_1 + \dots + c_{n-1}p^{n-2}$, donc $x_n = py_n$ pour tout n . Réciproquement, $p\underline{y} = (\bar{0}, \bar{p}y_1, \dots)$ n'est pas inversible.

Lemme B.2.4. *Tout $\underline{x} \in \mathbb{Z}_p \setminus \{0\}$ s'écrit de manière unique sous la forme $p^n \underline{y}$, où $n \in \mathbb{N}$ et $\underline{y} \in \mathbb{Z}_p^\times$.*

Preuve : Démontrons l'existence. Si $\underline{x} \in \mathbb{Z}_p^\times$, c'est terminé ; sinon, on écrit $\underline{x} = p\underline{x}_1$. Si \underline{x}_1 est inversible alors on a gagné, sinon on poursuit : $\underline{x} = p^2 \underline{x}_2$. Ainsi de suite ; le processus s'arrête bien : si l'on pouvait écrire $\underline{x} = p^n \underline{x}_n$ pour tout n , alors on aurait $\underline{x} = (\bar{0}, \dots, \bar{0}, \dots) = 0$. Pour démontrer l'unicité, on suppose que $p^n \underline{y} = p^m \underline{z}$ (avec $n \geq m$) : comme $\underline{z} = p^{n-m} \underline{y}$ est inversible, alors $n = m$; puis $\underline{y} = \underline{z}$.

Proposition B.2.1. *\mathbb{Z}_p est un anneau principal (donc factoriel) dont p est (aux associés près) l'unique élément irréductible. La décomposition précédente est la décomposition en produit d'irréductibles.*

Preuve : Démontrons que \mathbb{Z}_p est intègre : étant donnés \underline{x} et \underline{x}' deux éléments non nuls, il s'agit de montrer que $\underline{x}\underline{x}' \neq 0$. Pour cela, on écrit $\underline{x} = p^n \underline{y}$ et $\underline{x}' = p^{n'} \underline{y}'$, où \underline{y} et \underline{y}' sont inversibles, d'inverses \underline{z} et \underline{z}' . Alors $\underline{x}\underline{x}' = p^{n+n'} \underline{y}\underline{y}'$. Comme $(\underline{x}\underline{x}')(\underline{z}\underline{z}') = p^{n+n'} \neq 0$, nécessairement $\underline{x}\underline{x}' \neq 0$.

Soit maintenant I un idéal non nul de \mathbb{Z}_p . On note n le plus petit entier tel que $p^n \in I$; prenant $\underline{x} = p^m \underline{y}$ (\underline{y} inversible) dans I , alors $p^m = \underline{x}\underline{y}^{-1} \in I$, donc n est bien défini et l'on a $m \geq n$ par définition de n . Par conséquent \underline{x} est un multiple de p^n , ce qui montre que $I = (p^n)$.

Il reste à montrer que p est irréductible : si $p = \underline{x}\underline{x}'$, on écrit les décompositions $\underline{x} = p^n \underline{y}$ et $\underline{x}' = p^{n'} \underline{y}'$; alors $p = p^{n+n'} \underline{y}\underline{y}'$, donc $n + n' = 1$ par unicité. Par conséquent l'un des deux entiers est nul, donc l'un parmi \underline{x} et \underline{x}' est inversible.

Remarque. Tout idéal est donc de la forme (p^n) pour un certain entier n . L'idéal (p) est l'unique idéal premier non nul ; il est de plus maximal : on va voir que $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$, qui est un corps (ceci n'a rien d'étonnant : un idéal premier d'un anneau principal est maximal).

Lemme B.2.5. *La suite de morphismes*

$$0 \rightarrow \mathbb{Z}_p \xrightarrow{\alpha} \mathbb{Z}_p \xrightarrow{\beta} \mathbb{Z}/p^n\mathbb{Z} \rightarrow 0,$$

où α désigne la multiplication par p^n et $\beta : (x_n) \mapsto x_n$, est exacte. Autrement dit, α est injective, $\ker \beta = \text{Im } \alpha$ et β est surjective.

Preuve : L'injectivité de α provient du fait que \mathbb{Z}_p est intègre : si $p^n \underline{x} = 0$, alors $\underline{x} = 0$.

Démontrons que $\ker \beta \subset \text{Im } \alpha$: un élément $\underline{x} = (x_n)$ de $\ker \beta$ a ses n premières composantes nulles (puisque $x_n = \bar{0}$) ; son développement p -adique est donc de la forme $c_n p^n + c_{n+1} p^{n+1} + \dots$. Soit \underline{y} l'entier p -adique dont le développement est $c_n + c_{n+1} p + \dots$; on vérifie que $\underline{x} = p^n \underline{y}$. L'inclusion $\ker \beta \supset \text{Im } \alpha$ est évidente.

Enfin, β est surjective : étant donné $\lambda \in \mathbb{Z}/p^n \mathbb{Z}$, on pose $x_n = \lambda$, ce qui définit x_i pour $i < n$ ($x_{i-1} = p_{i-1}(x_i)$). On utilise la surjectivité des p_i pour définir les x_i lorsque $i > n$. On peut donc construire \underline{x} tel que $\beta(\underline{x}) = \lambda$.

Corollaire. $\mathbb{Z}_p/p^n \mathbb{Z}_p \simeq \mathbb{Z}/p^n \mathbb{Z}$.

En effet, $\ker \beta = \text{Im } \alpha = p^n \mathbb{Z}_p$.

B.2.4. Propriétés topologiques de \mathbb{Z}_p

Sur \mathbb{Z} , on dispose de la valuation p -adique v_p définie comme suit : $v_p(x)$ est la puissance de p qui apparaît dans la décomposition de $x \neq 0$ en produit de nombres premiers et $v_p(0) = +\infty$. On définit ensuite la valeur absolue p -adique par $|x|_p = a^{-v_p(x)}$, où $a > 1$ est un réel fixé ; souvent, on choisit $a = p$ (cette normalisation permet d'avoir la formule du produit : $|x| \prod_p |x|_p = 1$).

On vérifie facilement que $v_p(xy) = v_p(x) + v_p(y)$ et que $v_p(x+y) \geq \min(v_p(x), v_p(y))$ (avec égalité si $v_p(x) \neq v_p(y)$). Ainsi :

- $|x| \geq 0$ et $|x|_p = 0 \Leftrightarrow x = 0$;
- $|x+y|_p \leq \max(|x|_p, |y|_p)$ (inégalité *ultramétrique*, plus forte que l'inégalité triangulaire) ;
- $|xy|_p = |x|_p |y|_p$;

Les trois propriétés précédentes constituent la définition d'une valeur absolue (ultramétrique ou non-archimédienne).

Il résulte du lemme B.2.4 que la valuation v_p de \mathbb{Z} s'étend à \mathbb{Z}_p : écrivant $\underline{x} = p^n \underline{y}$, où $\underline{y} \in \mathbb{Z}_p^\times$, on pose $v_p(\underline{x}) = n$. Donc $|\bullet|_p$ se prolonge également en une valeur absolue sur \mathbb{Z}_p .

La distance p -adique est définie par $d_p(x, y) = |x - y|_p$. La topologie p -adique est la topologie provenant de la distance p -adique.

Le développement p -adique peut s'interpréter topologiquement :

Proposition B.2.2. Soit $\underline{x} \in \mathbb{Z}_p$ dont le développement p -adique est $c_0 + c_1 p + \dots + c_n p^n + \dots$. Alors $\underline{x} = \lim_{n \rightarrow +\infty} (c_0 + c_1 p + \dots + c_n p^n) = \sum_{i=0}^{+\infty} c_i p^i$.

Preuve : on a $|\underline{x} - (c_0 + c_1 p + \dots + c_n p^n)|_p \leq p^{-(n+1)}$; en effet, $\underline{y} = \underline{x} - (c_0 + c_1 p + \dots + c_n p^n)$ a un développement p -adique dont les n premiers termes sont nuls. Il s'écrit donc $\underline{y} = (y_k)$, avec $y_{n+1} = \bar{0}$; d'après le lemme B.2.5, il est divisible par p^{n+1} . Par conséquent, $v_p(y) \geq n+1$.

Corollaire. \mathbb{Z} est dense dans \mathbb{Z}_p .

En effet, on tronque le développement p -adique en gardant de plus en plus de chiffres.

Proposition B.2.3. La projection $\mathbb{Z}_p \xrightarrow{\pi_n} \mathbb{Z}/p^n \mathbb{Z}$ définie par $\underline{x} = (x_n) \mapsto x_n$ est continue (où $\mathbb{Z}/p^n \mathbb{Z}$ est munie de la topologie discrète).

Preuve : $\pi_n(n) = \pi_n(y)$ si et seulement si $\pi_n(x - y) = 0$, donc si et seulement si $x - y$ appartient à $p^n \mathbb{Z}_p$. Par conséquent, l'image réciproque d'un singleton $\{\lambda\}$ par π_n est $\bar{\lambda} + p^n \mathbb{Z}_p$, où $\bar{\lambda}$ représente λ . C'est un ouvert de \mathbb{Z}_p car c'est un translaté de $p^n \mathbb{Z}_p$ qui est ouvert. En effet, $p^n \mathbb{Z}_p = \{x : v_p(x) \geq n\} = \{x : v_p(x) > n-1\} = \{x : |x|_p < p^{-(n-1)}\}$. On voit que $p^n \mathbb{Z}_p$ est ouvert : c'est la boule ouverte de rayon $p^{-(n-1)}$ (et fermé également : c'est la boule fermée de rayon p^n).

Corollaire. \mathbb{Z}_p est totalement discontinu : ses composantes connexes sont des points.

En effet, si $\Omega \subset \mathbb{Z}_p$ est connexe, alors $\pi_n(\Omega)$ également ; donc $\pi_n(\Omega) = \{\lambda_n\}$. Soient \underline{x} et \underline{y} dans Ω ; alors $x_n = y_n = \lambda_n$ pour tout n , ce qui montre que $\underline{x} = \underline{y}$. Autrement dit, Ω est bien un singleton.

Théorème B.2.1. \mathbb{Z}_p est compact.

Preuve : soit (\underline{x}^k) une suite d'éléments de \mathbb{Z}_p ; il s'agit d'en extraire une sous-suite convergente.

- On regarde (x_1^k) comme suite de $\mathbb{Z}/p\mathbb{Z}$: ce dernier étant de cardinal fini, il existe α_1 tel que $S_1 = \{k \in \mathbb{N} : x_1^k = \alpha_1\}$ est infini.
- On regarde les x_2^k , pour $k \in S_1$: il existe $\alpha_2 \in \mathbb{Z}/p^2\mathbb{Z}$ tel que $S_2 = \{k \in S_1 : x_2^k = \alpha_2\}$ est infini. Remarquons que $p_1(\alpha_2) = \alpha_1$ car $\alpha_2 = x_2^k$ et $p_1(x_2^k) = x_1^k = \alpha_1$ puisque $k \in S_1$.
- On continue ainsi indéfiniment et considère $\underline{\alpha} \in \mathbb{Z}_p$. On extrait de la suite de départ une sous-suite (\underline{x}^{k_i}) , où $k_i \in S_i$ pour tout i . Alors \underline{x}^{k_i} tend vers $\underline{\alpha}$ lorsque i tend vers l'infini : en effet, $\pi_i(\underline{x}^{k_i} - \underline{\alpha}) = \bar{0}$ car $k_i \in S_i$; d'après le lemme B.2.5, on a donc $\underline{x}^{k_i} - \underline{\alpha} \in p^i \mathbb{Z}_p$. Par conséquent, $|\underline{x}^{k_i} - \underline{\alpha}|_p \leq p^{-i}$.

Corollaire. \mathbb{Z}_p est complet.

Remarque. Pour la topologie p -adique, une série $\sum u_n$ converge si et seulement si $u_n \rightarrow 0$. En effet, comme \mathbb{Z}_p est complet, on peut appliquer le critère de Cauchy. Or il résulte de l'inégalité ultramétrique que $|\sum_{n=q}^r u_n|_p \leq \max_{q \leq n \leq r} |u_n|_p$. Donc pour que la tranche de Cauchy devienne aussi petite que l'on veut lorsque p et q sont grands, il suffit que $|u_n|_p \rightarrow 0$.

B.2.5. Le corps \mathbb{Q}_p

Définition B.2.3. C'est le corps des fractions de \mathbb{Z}_p .

Puisque \mathbb{Z}_p contient \mathbb{Z} , il contient donc \mathbb{Q} . On dispose d'une valuation sur \mathbb{Q}_p : écrivant $x \in \mathbb{Q}_p \setminus \{0\}$ sous la forme $x = \frac{a}{b} = \frac{p^n u}{p^m v}$, on pose $v_p(x) = n - m$. On vérifie facilement que cette définition a bien un sens (donc ne dépend pas de la fraction choisie représentant x). Le même processus permet de prolonger la valuation p -adique de \mathbb{Z} en une valuation sur le corps des fractions \mathbb{Q} de \mathbb{Z} . On obtient donc une valeur absolue $|x|_p = p^{-v_p(x)}$ sur \mathbb{Q}_p , qui prolonge celle de \mathbb{Z}_p et celle de \mathbb{Q} .

Remarque. Le théorème d'Ostrowski dit que ce sont là, à équivalence près, toutes les valeurs absolues de \mathbb{Q} : une telle valeur absolue est soit $|\bullet|_p^\alpha$ (p premier) soit $|\bullet|^\alpha$, pour un certain réel positif α .

Voici quelques propriétés topologiques, où la topologie est définie par la distance p -adique :

Théorème B.2.2. *Le corps \mathbb{Q}_p est localement compact et complet. \mathbb{Z}_p en est un sous-anneau à la fois ouvert et fermé. \mathbb{Q} est dense dans \mathbb{Q}_p .*

Preuve : par translation, on se ramène à 0 (une translation est une application continue) : or \mathbb{Z}_p est compact, donc les $p^n\mathbb{Z}_p$ aussi (les homothéties sont continues). Ces derniers constituent une base de voisinages de 0. Une suite de Cauchy est bornée ; il existe donc $n \in \mathbb{Z}$ tel que le compact $p^n\mathbb{Z}_p$ contienne la suite toute entière. On pourra alors en extraire une sous-suite convergente, auquel cas notre suite de Cauchy qui admet une valeur d'adhérence est également convergente.

\mathbb{Z}_p est à la fois ouvert et fermé (c'est à la fois une boule ouverte et une boule fermée). Finalement, écrivant $x \in \mathbb{Q}_p$ sous la forme $x = p^n y$, où $n \in \mathbb{Z}$ et $y \in \mathbb{Z}_p$, on transforme via l'application $z \mapsto p^n z$ une suite d'entiers convergent vers y dans \mathbb{Z}_p en une suite de rationnels convergent vers x dans \mathbb{Q}_p , ce qui démontre la troisième assertion.

En particulier, \mathbb{Q}_p s'identifie au complété de \mathbb{Q} pour la valeur absolue p -adique.

Bibliographie

- [A] M. ARTIN, «*Algebra*», Prentice Hall, 1991.
- [Ca] J. W. S. CASSELS, «*Lectures on Elliptic Curves*», LMS, Student Texts 24, 1991.
- [Co] H. COHEN, «*A course in computational algebraic number theory*», GTM 138, Springer-Verlag, Berlin, 1993.
- [CCS] G. CORNELL, J. SILVERMANN, G. STEVENS, editors, «*Modular Forms and Fermat's Last Theorem*», Springer-Verlag, 1997.
- [Cx] D. COX, «*Primes of the form $x^2 + ny^2$* », Wiley, 1989.
- [D] J. DIEUDONNÉ, «*Pour l'honneur de l'esprit humain*», Hachette, 1987.
- [G] J. GOLDMAN, «*The Queen of Mathematics : An Historically Motivated Guide to Number Theory*», A. K. Peters, Ltd., 1997.
- [Gu] D. GUIN, «*Algèbre*», tomes 1 & 2, Belin, 1997.
- [H] Y. HELLEGOUARCH «*Invitation aux mathématiques de Fermat-Wiles*», Masson, Paris, 1997.
- [J] N. JACOBSON, «*Basic Algebra*», tomes I & II, Freeman and Company.
- [KKS] K. KATO, N. KUROKAWA, T. SAITO, «*Number Theory I, Fermat's dream*», Translations of Mathematical Monographs, AMS 2000.
- [Ko1] N. KOBLITZ, «*Introduction to Elliptic Curves and modular Forms*», GTM 97, Springer, Berlin, 1984.
- [Ko2] N. KOBLITZ, «*A course in number theory and cryptography*», GTM 114, Springer, Berlin, 1994.
- [L] S. LANG, «*Algebra*», third edition, Addison-Wesley, 1993.

- [P-R] B. PERRIN-RIOU, «*Algèbre, arithmétique et maple*», Cassini, Paris, 2000.
- [R] P. RIBENBOIM, «*13 Lectures on Fermat's Last Theorem*», Springer-Verlag, New-York, 1979.
- [Sa] P. SAMUEL, «*Théorie algébrique des nombres*», Hermann, Paris, 1971.
- [Se] J.-P. SERRE, «*Cours d'arithmétique*», Le mathématicien, PUF, Paris, 1977.
- [S-T] J. H. SIVERMAN, J. TATE, «*Rational Points on Elliptic Curves*», Springer, 1992.
- [Swin] H.P.F. SWINNERTON-DYER, «*A brief guide to algebraic number theory*», London Mathematical Society Student Texts 50, Cambridge University Press, Cambridge, 2001.