Feuille d'exercices 6

1 Nombres premiers

Exercice 1. ***Postulat de Bertrand****: on va montrer que pour tout $n \geq 1$, il existe un nombre premier p tel que $n < p \leq 2n$.*

(1) Montrer que pour tout $m \geq 1$, on a

$$\prod_{m+1<p\leq 2m+1} p \leq C_{2m+1}^m \leq 2^{2m}$$

Pour tout x soit $q = 2m+1$ le plus grand nombre premier tel que $q \leq x$. Montrer que

$$\prod_{p\leq x} p = \prod_{p\leq q} p \leq 4^{2m} \leq 4^{x-1}$$

(2) Montrer que $n!$ s'écrit sous la forme $p^{v_p(n)}m$ avec p ne divisant pas m et

$$v_p(n) = \sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor$$

que l'on appelle la valuation p-adique de n. En déduire que la valuation p-adique de C_{2n}^n est

$$\sum_{k\geq 1} \lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor) \leq \max\{r : p^r \leq 2n\}$$

(3) Montrer que pour $p > \sqrt{2n}$, $v_p(C_{2n}^n) \leq 1$ et que pour $\frac{2n}{3} < p \leq n$, $v_p(C_{2n}^n) = 0$.

(4) Pour $n \geq 3$, montrer que $\frac{4^n}{2n} \leq C_{2n}^n$ et en déduire que

$$4^n \leq (2n)^{1+\sqrt{2n}} \prod_{\sqrt{2n}<p\leq \frac{2n}{3}} p \prod_{n<p\leq 2n} p$$

(5) On suppose qu'il n'y a pas de nombre premier p tel que $n < p \leq 2n$. En déduire que $4^{n/3} \leq (2n)^{1+\sqrt{2n}}$. En utilisant la relation $a + 1 < 2^a$, en déduire que $n < 4000$.

(6) Conclure en considérant la suite

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

(7) Montrer que pour $n \geq 4000$, on a

$$\prod_{n<p\leq 2n} p \geq 2^{n/30}$$

et en déduire qu'il y a au moins $\log_{2n}(2^{n/30} = \frac{1}{30}\frac{n}{\log_2 n+1}$ nombres premiers dans l'intervalle compris entre n et $2n$.

(8) Pouvez-vous commenter ce dernier résultat?

Exercice 2. *Pour tout $x \in \mathbb{R}_+$, on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.*

(1) Montrer que pour tout $k \in \mathbb{N}$, $\pi(2^{k+1}) \leq 2^k$.

(2) *Soit $p \leq 2n$ et r tel que $p^r \leq 2n < p^{r+1}$. Montrer que $v_p(C_{2n}^n) \leq r$ puis que*

$$\prod_{n<p\leq 2n} p \mid C_{2n}^n \mid \prod_{p^r \leq 2n < p^{r+1}} p^r$$

En déduire que $n^{\pi(2n)-\pi(n)} < C_{2n}^n \leq (2n)^{\pi(2n)}$.

(3) *Prouver que $2^n \leq C_{2n}^n \leq 2^{2n}$ et en déduire en prenant $n = 2^k$ que:*

$$k\big(\pi(2^{k+1}) - \pi(2^k)\big) < 2^{k+1}$$

et que $2^k \leq (k+1)\pi(2^{k+1})$.

(4) *Montrer que pour tout entier k:*

$$\frac{1}{2}\frac{2^{k+1}}{k+1} \leq \pi(2^{k+1}) \leq 3\frac{2^{k+1}}{k+1}$$

(5) *Soit $n > 1$ et k tel que $2^k \leq n < 2^{k+1}$. Montrer que*

$$\frac{\log 2}{4}\frac{n}{\log n} \leq \pi(n) \leq 6\log 2\frac{n}{\log n}$$

(6) *Application: montrer que*

$$\sum_{p\leq n} \frac{\log p}{p} = \log n + \mathcal{O}(1)$$

2 Courbes elliptiques: hors programme, cette section introduit à un des domaines actuellement les plus actifs de la théorie des nombres

Exercice 1. *Une fonction f est dite **elliptique** par rapport à un réseau Λ si c'est une fonction méromorphe sur $\mathbb{C}$ qui est Λ-périodique, i.e.*

$$f(z+\omega) = f(z)$$

pour tout $z \in \mathbb{C}$ et tout $\omega \in \Lambda$.

(1) *Montrer que f est Λ-périodique si et seulement si $f(z+\omega_1) = f(z) = f(z+\omega_2)$ pour tout $z \in \mathbb{C}$ avec $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Par ailleurs si f n'a pas de poles, montrer que f est constante.*

(2) *Soit f une fonction elliptique par rapport à Λ et soit P un parallélogramme fondamental.*

(i) *On suppose que f n'a pas de poles sur le bord ∂P de P. Montrer alors que la somme des résidus de f dans P est égale à 0.*

(ii) *On suppose que f n'a ni zéros ni poles sur ∂P. On note a_i les zéros et poles de f dans P et on note m_i la multiplicité de f en a_i. Montrer que*

$$\sum_i m_i = 0$$

$$\sum_i m_i a_i \equiv 0 \mod \Lambda$$

(3) *On considère la fonction $\mathfrak{P}$ de Weierstrass:*

$$\mathfrak{P}_\Lambda(x) = x^{-2} + \sum_{\omega\in\Lambda-0} [(x-\omega)^{-2} - \omega^{-2}]$$

(i) *Montrer que pour tout $s > 2$ la somme $\sum_{\omega\in\Lambda-0} \frac{1}{|\omega|^s}$ converge.*

(ii) *En déduire que la série qui définit $\mathfrak{P}$ converge uniformément sur tout compact de $\mathbb{C}$ ne contenant pas les points du réseau Λ.*

(iii) *En considérant $\mathfrak{P}'(x) = -2\sum_{x\in\Gamma}(x-\omega)^{-3}$, montrer que $\mathfrak{P}$ est elliptique par rapport à Λ.*

(4) *L'ensemble des fonctions elliptiques par rapport à Λ est un corps sur $\mathbb{C}$; on veut montrer que celui-ci est engendré par $\mathfrak{P}$ et $\mathfrak{P}'$.*

(i) *Soit f elliptique paire et soit $u \equiv -u \mod \Lambda$ avec $u \not\equiv 0 \mod \Lambda$. Montrer que $g(z) := \mathfrak{P}(z) - \mathfrak{P}(u)$ a un zéro d'ordre 2. En déduire que f a un zéro d'ordre pair en u. Traitez le cas de $u \equiv 0 \mod \Lambda$ en considérant $g = 1/\mathfrak{P}$.*

(ii) *Soit $(u_i)_{1\leq i\leq r}$ un famille de points contenant un représentant de chaque classe $(u, -u) \mod \Lambda$ où f a un pole ou un zéro autre que la classe de Λ. On pose*

$$m_i = \mathrm{ord}_{u_i} f \text{ si } 2u_i \not\equiv 0 \mod \Lambda$$

$$m_i = \frac{1}{2}\mathrm{ord}_{u_i} f \text{ si } 2u_i \equiv 0 \mod \Lambda$$

Montrer, en utilisant le théorème de Liouville, que f est égal à une constante fois $\prod_{i=1}^r [\mathfrak{P}(z)-\mathfrak{P}(u_i)]^{m_i}$.

(iii) *En déduire que $\mathbb{C}(\mathfrak{P})$ est le corps des fonctions elliptiques paires par rapport à Λ, puis que $\mathbb{C}(\mathfrak{P}, \mathfrak{P}')$ est le corps des fonctions elliptiques par rapport à Λ.*

(5) *On veut montrer que les points $(\mathfrak{P}(z), \mathfrak{P}'(z))$ appartiennent à une cubique d'équation $y^2 = 4x^3 - g_2x - g_3$ avec $\Delta = g_2^3 - 27g_3^2 \neq 0$.*

(i) *Montrer que*

$$\mathfrak{P}(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{2n+2}(\Lambda)z^{2n}$$

avec $s_n(\Lambda) = s_n = \sum_{\omega\neq 0}\frac{1}{\omega^m}$.

(ii) *En posant $g_2 = 60s_4$ et $g_3 = 140s_6$, montrer que $(\mathfrak{P}(z), \mathfrak{P}'(z))$ appartiennent à une cubique d'équation $y^2 = 4x^3 - g_2x - g_3$.*

(iii) *On pose $e_1 = \mathfrak{P}(\omega_1/2)$, $e_2 = \mathfrak{P}(\omega_2)$ et $e_3 = \mathfrak{P}(\frac{\omega_1+\omega_2}{2})$. Montrer que modulo Γ, $\mathfrak{P}'$ a trois racines simples à savoir $\omega_1/2$, $\omega_2/2$ et $(\omega_1+\omega_2)/2$. En déduire que*

$$(\mathfrak{P}')^2 = 4(\mathfrak{P}-e_1)(\mathfrak{P}-e_2)(\mathfrak{P}-e_3)$$

avec $\Delta = g_2^3 - 27g_3^2 \neq 0$.

(iv) *En déduire que*

$$x = \frac{1}{2}\int_{\infty}^{\mathfrak{P}(x)}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy \mod \Gamma$$

avec $\omega_1 = \int_{\infty}^{e_1}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$ et $\omega_2 = \int_{e_1}^{e_2}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$.

(v) *Montrer que l'équation $y^2 = x^3 - x$ correspond au réseau $\mathbb{Z}^2$ en utilisant l'égalité*

$$\omega_1 = \int_0^1 (x-x^2)^{-1/2}dx = \int_1^{\infty}(x^3-x)^{-1/2}dx = \omega_2/i$$

que l'on montrer via le changement de variable $x \mapsto 1/x$.

Exercice 2. ***Loi d'addition*** *Etant donné des nombres complexes g_2, g_3 on peut se demander s'il existe un réseau pour lequel ce sont les invariants associés comme dans l'exercice précédent. La réponse est oui. On considère la courbe projective A d'équation*

$$uy^2 = 4x^3 - g_2xu^2 - g_3u^3$$

de point infini $(0, 0, 1)$ qui est l'image des points de Λ par l'application $z \mapsto (1, \mathfrak{P}(z), \mathfrak{P}'(z))$.

(1) *Montrer que l'application ci-dessus induit une bijection* $\mathbb{C}/\Lambda - 0 \longrightarrow A_{\mathbb{C}} - \{\infty\}$, *où* $A_{\mathbb{C}}$ *désigne les points complexes de la cubique* A.

(2) *L'ensemble* $\mathbb{C}/\Lambda$ *est naturellement muni d'une structure de groupe; on veut exprimer celle-ci sur* $A_{\mathbb{C}}$. *Nous allons montrer que si* $P_1 = (1, x_1, y_1)$ *et* $P_2 = (1, x_2, y_2)$ *alors* $P_3 = P_1 + P_2 = (1, x_3, y_3)$ *s'exprime avec des fonctions rationnelles en* x_1, x_2, y_1, y_2. *Géométriquement on procède comme dans le dessin suivant: la droite* (P_1P_2) *intersecte* $A_{\mathbb{C}}$ *en un troisième point* $Q_3 = -P_3$ *et* P_3 *est le symétrique de* Q_3 *par rapport à l'axe des* x.

(i) *Soient* $u_1, u_2 \in \mathbb{C} - \Lambda$ *et supposons* $u_1 \not\equiv u_2 \mod \Lambda$. *Soient* $a, b \in \mathbb{C}$ *tels que*

$$\mathfrak{P}'(u_1) = a\mathfrak{P}(u_1) + b$$

$$\mathfrak{P}'(u_2) = a\mathfrak{P}(u_2) + b$$

Montrer que $g(z) = \mathfrak{P}'(z) - a\mathfrak{P}(z) - b$ *a 3 zéros comptés avec leur multiplicités. A quelle condition n'a-t-ont que 2 zéros distincts?*

(ii) *On suppose que gz a 3 zéros distincts. En notant* u_3 *le troisième, montrer que* $u_3 \equiv -(u_1 + u_2) \mod \Lambda$. *En déduire que*

$$x_3 = -x_1 - x_2 + \frac{1}{4}\Big(\frac{y_1 - y_2}{x_2 - x_2}\Big)^2.$$

(iii) *Pour* $u_1 \equiv u_2 \mod \Lambda$ *montrer que*

$$\mathfrak{P}(2u) = -2\mathfrak{P}(u) + \frac{1}{4}\Big(\frac{\mathfrak{P}"(u)}{\mathfrak{P}'(u)}\Big)^2.$$

Exercice 3. ***Une introduction à la géométrie algébrique***

(1) *En vous appuyant sur la classification des coniques projectives de* $\mathbb{P}^2_{\mathbb{R}}$, *montrez qu'une conique non dégénérée* C *non vide de* $\mathbb{P}^2_{\mathbb{R}}$ *est projectivement équivalente à la courbe* $XZ = Y^2$.

Montrez que cette courbe admet un paramétrage par $\mathbb{P}^1_{\mathbb{R}}$ *via l'application qui à* (U, V) *associe* (U^2, UV, V^2). *Quelle est l'application inverse?*

(2) ***Cas simples du théorème de Bézout***

(i) *Soit*

$$F(U, V) = a_d U^d + a_{d-1} U^{d-1} V + \cdots + a_0 V^d$$

un polynôme homogène non nul de degré d *en 2 variables à coefficients dans un corps* k. *On lui associe le polynôme en une variable* $f(u) = F(u, 1)$ *et on définit la multiplicité d'un zéro* (u, v) *de* F *dans* $\mathbb{P}^1_k$ *comme la multiplicité de* u/v *dans* f *si* $v \neq 0$ *et sinon en* $(1, 0)$ *comme l'entier* $d - \deg f$.

Montrer que F *a au plus* d *zéros dans* $\mathbb{P}^1_k$ *comptés avec multiplicités.*

(ii) *Soit* $L \subset \mathbb{P}^2_k$ *une droite et* $D \subset \mathbb{P}^2_k$ *une courbe définie par une équation* $G(X, Y, Z) = 0$ *où* G *est un polynôme homogène de degré* d *en* X, Y, Z. *On suppose* $L \nsubseteq D$. *Montrer que le cardinal de* $L \cap D$ *est inférieur ou égal à* d.

(iii) *Même hypothèse qu'en (ii) en remplaçant* L *par une conique non dégénérée* C: *montrer que le cardinal de* $C \cap D$ *est inférieur ou égal à* $2d$.

Remarque: On peut définir une notion de multiplicité d'une intersection en un point de sorte que les résultats précédents soient vrais en comptant avec multiplicité. En outre si k *est algébriquement clos, on a alors égalité. Le théorème de Bézout concerne des courbes* C *et* D *de degré* n *et* m: *leur intersection est alors* nm, *en comptant les multiplicités et en travaillant sur un corps algébriquement clos.*

(3) ***L'espace des coniques*** *Dans la suite on note* $S_d(k)$ *l'espace des polynômes homogènes de degré* d *à coefficients dans* k, *en les variables* X, Y, Z. *Etant donnés des points* $P_1, \cdots, P_r$ *de* $\mathbb{P}^2_k$, *on notera* $S_d(P_1, \cdots, P_n)$ *le sous-ensemble de* $S_d(k)$ *constitué des éléments* F *qui s'annulent sur les* P_i.

(i) *Soient $P_1, \cdots, P_5 \in \mathbb{P}^2_{\mathbb{R}}$ des points distincts tels que 4 quelconques ne sont pas colinéaires. Montrer qu'il existe au plus une conique passant par ces 5 points.*

(ii) *Soit $n \geq 5$ et soient $P_1, \cdots, P_n$ des points tels que 4 quelconques ne sont jamais colinéaires. Montrer alors que l'ensemble des formes quadratiques qui s'annulent sur ces poitns est de dimension $6 - n$.*

(iii) ***Un pinceau de coniques*** *est une famille de la forme*

$$C_{\lambda,\mu} := (\lambda Q_1 + \mu Q_2 = 0)$$

où Q_1 et Q_2 sont des coniques. On suppose que le pinceau possède au moins une conique dégénérée, montrer alors qu'elle en possède au plus 3. En outre si $k = \mathbb{R}$, montrer que le pinceau admet toujours une conique dégénérée.

(4) ***Cubiques: exemples***

(i) *On considère la cubique de $\mathbb{R}^2$ définie par l'équation $y^2 = X^3 + x^2$. Donnez en une paramétrisation.*

(ii) *Même question avec la cubique $y^2 = x^3$.*

(iii) *Soit k un corps de caractéristique différente de 2 et soit $\lambda \in k$ avec $\lambda \neq 0, 1$. Montrer que pour si $f, g \in k(t)$ sont tels que $f^2 = g(g-1)(g-\lambda)$ alors $f, g \in k$. Quelle interprétation en donnez-vous sur la cubique $y^2 = x(x-1)(x-\lambda)$?*

(5) ***Cas simples du Nullstellensatz****: soit k un corps infini et soit $F \in S_d(k)$ un polynôme homogène de degré d à coefficients dans k en les variables X, Y, Z.*

(i) *Soit $L \subset \mathbb{P}^2_k$ une droite. Montrer que si F s'annule sur L alors $F = HF'$ où H est une équation de L et $F' \in S_{d-1}(k)$. En déduire que si $P_1, \cdots, P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1, \cdots, P_a \in L$ et $P_{a+1}, \cdots, P_n \notin L$ avec $a > d$, alors*

$$S_d(P_1, \cdots, P_n) = HS_{d-1}(P_{a+1}, \cdots, P_n)$$

(ii) *Soit $C \subset \mathbb{P}^2_k$, une conique non dégénérée et non vide. Montrer que si F s'annule sur C alors $F = QF'$ où Q est une équation de C et $F' \in S_{d-2}(k)$. En déduire que si $P_1, \cdots, P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1, \cdots, P_a \in C$ et $P_{a+1}, \cdots, P_n \notin C$ avec $a > 2d$, alors*

$$S_d(P_1, \cdots, P_n) = QS_{d-2}(P_{a+1}, \cdots, P_n)$$

(iii) *Soient $P_1, \cdots, P_8 \in \mathbb{P}^2_k$ des points distincts tels que 4 quelconques ne sont pas colinéaires et que 7 quelconques ne sont pas sur une conique non dégénérée. Montrer alors que $\dim S_3(P_1, \cdots, P_8) = 2$.*

Indication*: on traitera séparément le cas où 3 points quelconques ne sont pas colinéaires et 6 quelconques ne sont pas sur une conique non dégénérée.*

(iv) *Soient C_1, C_2 deux coniques dont l'intersection est 9 points distincts. Montrer que toute conique D qui passe par 8 d'entre eux passe aussi par le neuvième.*

(6) ***Loi d'addition sur une conique****: soit $k \subset \mathbb{C}$ et $C \subset \mathbb{P}^2_k$ une cubique d'équation $F = 0$. On suppose que F est irréductible et que pour tout point $P \in C$, il existe une unique droite $L \subset \mathbb{P}^2_k$ telle que P est un zéro multiple de $F_{|L}$. On fixe un point $O \in C$ et on considère la construction suivante:*

Construction*: (a) Soit $A \in C$ et soit $\bar{A}$ le troisième point d'intersection de C avec la droite OA.*

(b) Pour $A, B \in C$ soit R le troisième point d'intersection de AB avec C et on définit $A + B$ comme étant égal à $\bar{R}$.

On veut montrer que l'on définit ainsi une loi de groupe abélien sur C avec O comme élément neutre.

(i) *Montrer que la construction précédente est bien définie.*

(ii) *Montrer que O est bien un élément neutre et que la loi est commutative.*

(iii) Montrer que l'inverse de A est le troisième point d'intersection de $\bar{O}A$ avec C.

(iv) ***Associativité****: soient A, B, C trois points de C; la construction de $(A+B)+C = \bar{S}$ utilise les 4 droite (cf. la figure (1)):*

$$L_1 = ABR, \quad L_2 = RO\bar{R}, \quad L_3 = C\bar{R}S, \quad L_4 = SO\bar{S}$$

La construction de $(B+C)+A = \bar{S}'$ utilise les 4 droites

$$M_1 = BCQ, \quad M_2 = QO\bar{Q}, \quad M_3 = A\bar{Q}S', \quad M_4 = S'O\bar{S}'$$

Il s'agit de prouver $\bar{S} = \bar{S}'$ ou de manière équivalente $S = S'$. On considère les deux cubiques

$$D_1 = L_1 + M_2 + L_3 \qquad D_2 = M_1 + L_2 + M_3$$

de sorte que

$$C \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\} \qquad C \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S'\}$$

Conclure en supposant les 9 points $\{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$ distincts.

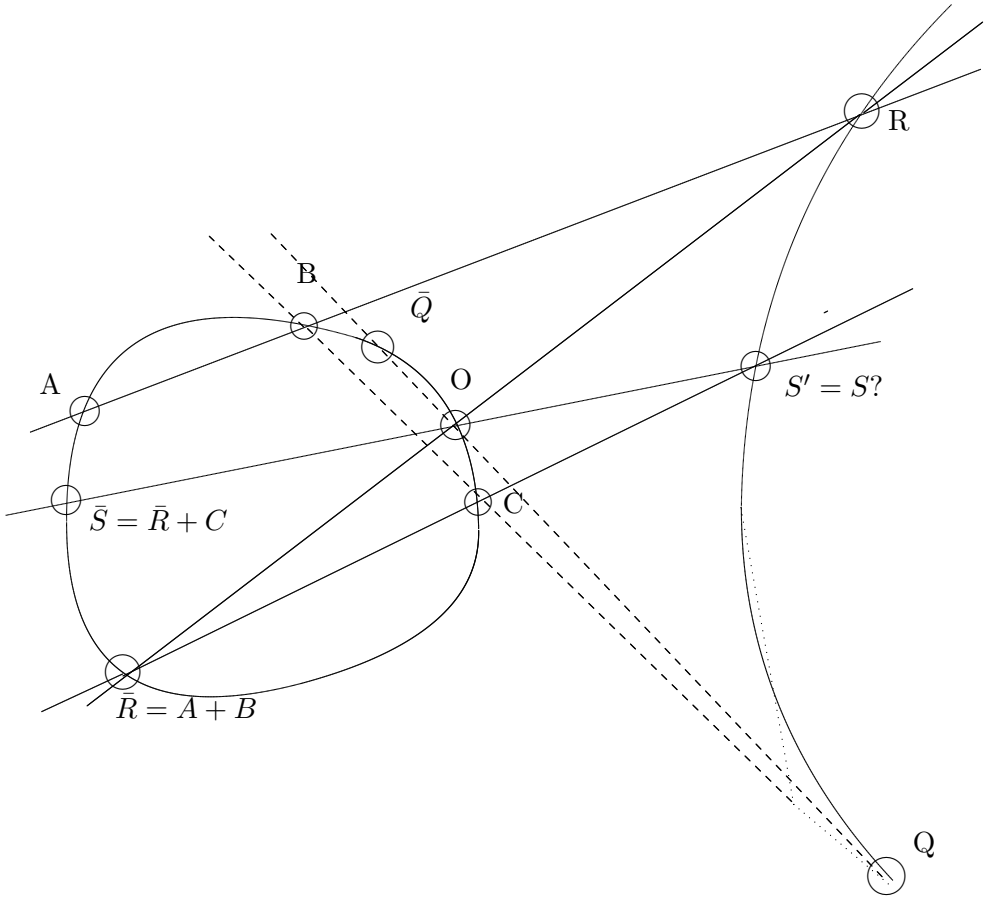

Figure 1: Loi d'addition sur une courbe elliptique

(v) Conclure dans le cas général en utilisant un argument de continuité et en utilisant l'hypothèse $k \subset \mathbb{C}$. Remarque: On peut montrer le cas général pour tout k avec une bonne notion de multiplicité, ou bien en utilisant la topologie de Zariski.

(vi) Soit $C \subset \mathbb{P}^2_k$ une cubique possédant un point d'inflexion P. Montrer qu'un changement de coordonnées dans $\mathbb{P}^2_k$ permet de se ramener à une équation de la forme ***normale****, i.e.*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Indication*: choisissez les coordonnées telles que $P = (0, 1, 0)$ et la droite d'inflexion $Z = 0$.*

(vii) ***Loi de groupe simplifiée****: on considère une cubique sous forme normale et on prend* $O = (0, 1, 0)$ *comme élément neutre. Montrer que l'on a les propriétés suivantes et retrouver la loi de groupe donnée par les fonctions de Weierstrass.*

(a) $C = \{O\} \cup C_0$*, où* $C_O : (y^2 = x^3 + ax + b)$ *est un courbe affine;*

(b) les droites passant par O *sont les droite projectives* $X = \lambda Z$ *et donc les droites affines* $x = \lambda$*;*

(c) $-P = \bar{P}$*.*

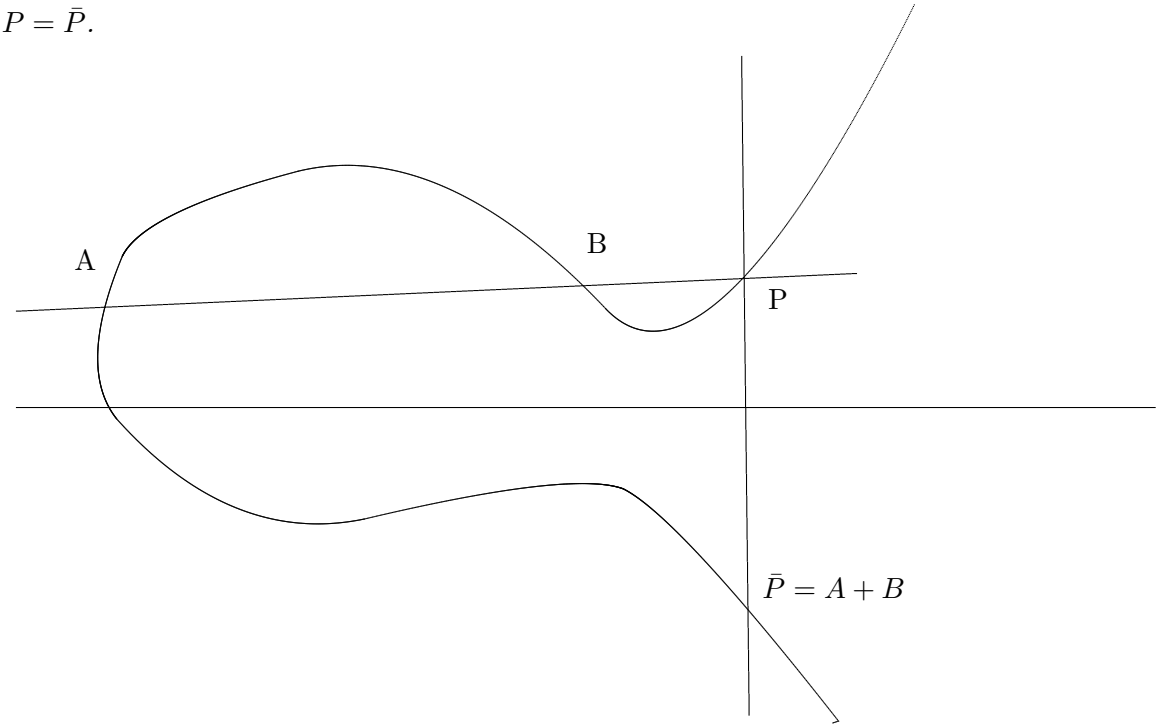

Figure 2: Loi d'addition simplifiée

Remarque: Essayez de prouver ***le théorème de l'hexagone de Pascal****: Soit un hexagone* $ABCDEF$ *dans* $\mathbb{P}_k^2$ *dont les paires de cotés opposés se rencontrent aux points* P, Q, R*. On suppose les 9 points et les 6 droites distinctes. Montrer alors que*

$$ABCDEF \text{ sont sur une même conique non dégénérée} \Leftrightarrow PQR \text{ sont colinéaires}$$

Exercice 4. ***Méthode de factorisation de Lenstra****:*

- *On choisit une courbe elliptique au hasard à coefficients dans* $\mathbb{Z}$ *avec un point* P *sur celle-ci. On considère alors la loi de groupe sur cette courbe modulo* n*.*
- *On calcule* $eP = (u, x, y)$ *dans ce groupe où* e *est un produit de petit nombres premiers pris à de petites puissances comme dans la méthode* $p - 1$ *de Pollard.*
- *On calcule le pgcd de* u *(ou du dénominateur de* x*) avec* n*.*
- *Si on trouve* 1*, alors on essaye avec une nouvelle courbe elliptique et un autre point.*

Commentez cet algorithme et expliquez en quoi il est plus souple que celui de Pollard.
Remarque: L'ordre d'une courbe elliptique prise au hasard sur $\mathbb{Z}/p\mathbb{Z}$ *varie de manière alléatoire entre* $p + 1 - 2\sqrt{p}$ *et* $p + 1 + 2\sqrt{p}$*.*

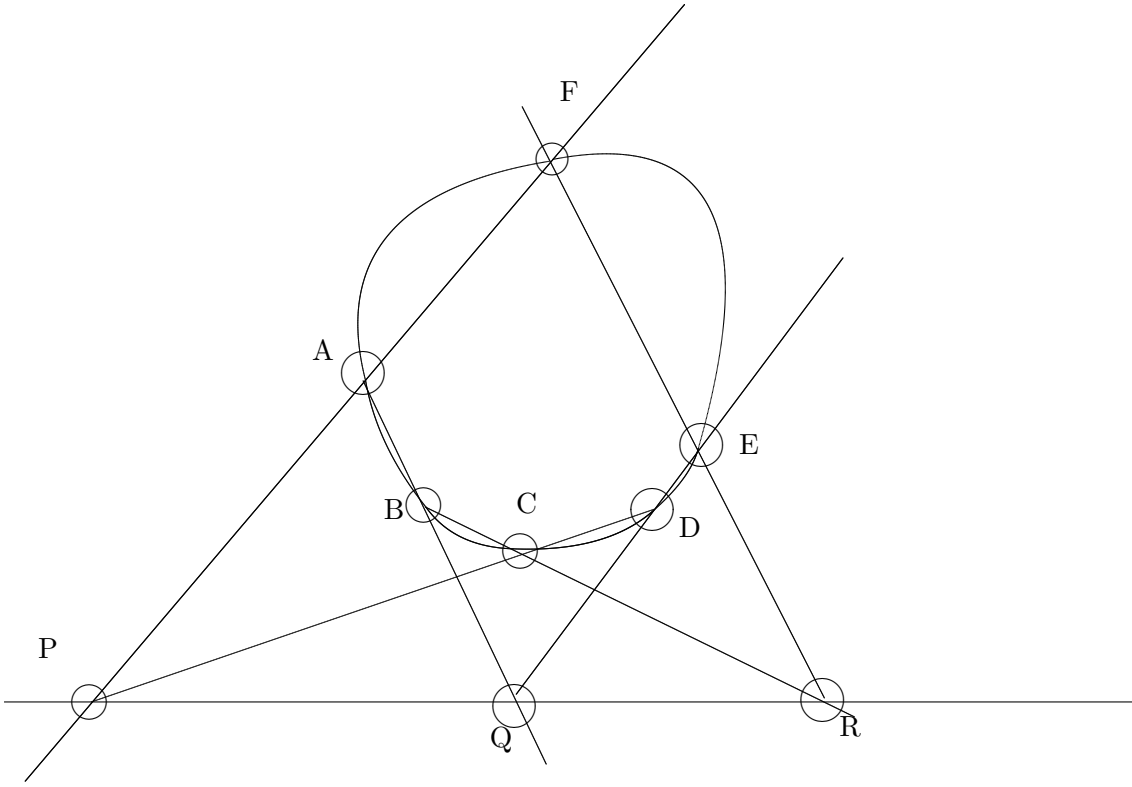

Figure 3: L'hexagone de Pascal