Courbes algébriques sur les corps finis
version préliminaire

Christian Pauly

avril 2006

Table des matières

Chapitre 1

Introduction

Le but de ce cours est de présenter la preuve de l'hypothèse de Riemann pour la fonction zêta associée à une courbe projective lisse définie sur un corps fini. Ce résultat est un cas particulier des conjectures d' André Weil, énoncé en 1949 dans son article [We], et démontré dans un contexte beaucoup plus général, par Pierre Deligne en 1973.

Pour les aspects cohomologiques des conjectures de Weil on pourra lire l'appendice C de [H]. Pour une introduction accessible au niveau M2 à la géométrie diophantienne on lira le texte introductif de B. Mazur [Ma].

E-mail : pauly@math.univ-montp2.fr

Chapitre 2

Théorie de Galois

Le but de ce chapitre est de rassembler tous les résultats de théorie de Galois, qui seront utilisés dans la suite de ce cours. On ne donnera que quelques preuves faciles. Pour les autres on pourra consulter les livres de référence, comme par exemple [C], [St], [Mal] ou [La]. Des cours en lignes sont également disponibles, par exemple [L] et [Mi].

Tous les corps apparaissant dans ce cours sont supposés commutatifs.

2.1 Extensions de corps

Soit k un corps et soit $i : \mathbb{Z} \to k$ le homomorphisme d'anneau qui envoie l'entier n sur $n \cdot 1$. Si i n'est pas injectif, on observe que l'idéal $\ker i$ est un idéal premier $p\mathbb{Z}$ pour un nombre premier p

Définition 2.1.1 *On dit que k est un corps de caractéristique 0 si i est injectif. On dit que k est un corps de caractéristique p si $\ker i = p\mathbb{Z}$.*

Soit K une extension de k, c'est-à-dire $k \subset K$.

Définition 2.1.2 *Un élément $x \in K$ est algébrique sur k s'il existe un polynôme non nul $P \in k[X]$ tel que $P(x) = 0$. Dans le cas contraire on dit que x est transcendant.*

Exemple.
Si $k = \mathbb{Q}$, le nombre $\sqrt{2}$ est algébrique, mais e et π sont transcendants.

Définition 2.1.3 *L'extension K/k est algébrique si tout élément $x \in K$ est algébrique sur k.*

Définition 2.1.4 *L'extension K/k est finie si la dimension de K comme k-espace vectoriel est finie. Dans ce cas on note $[K : k] = \dim_k K$.*

Exemples.

1. Soit $P \in k[X]$ un polynôme irréductible. Alors (voir ex...) l'idéal (P) est premier, donc maximal. Ainsi le quotient $K := k[X]/(P)$ est un corps, appelé le corps de rupture de P. C'est une extension algébrique finie de k. On a la relation

$$[K : k] = \deg P.$$

Si l'on note x la classe de l'indéterminée X modulo l'idéal (P) on a $K = k[x]$.

2. $k = \mathbb{F}_p(T^p)$ et $K = \mathbb{F}_p(T)$ où T est un élément transcendant sur le corps fini $\mathbb{F}_p$. Alors K est une extension algébrique de degré p sur k.
3. Soient K/k une extension et soient $x_1, x_2, \ldots, x_n \in K$. On note $k[x_1, x_2, \ldots, x_n]$ la k-algèbre engendrée par les x_i. Si tous les éléments x_i sont algébriques sur k alors l'algèbre $L = k[x_1, x_2, \ldots, x_n]$ est un corps et on a $[L : k] \leq \prod_i [k[x_i] : k]$ — exercice.

Définition 2.1.5 *Soit K/k une extension et $x \in K$ un élément algébrique. On appelle polynôme minimal de x sur k le générateur unitaire de l'idéal des polynômes dans $k[X]$ annulateurs de x. On notera* $\mathrm{Min}_k(x)$ *le polynôme minimal de x sur k.*

Définition 2.1.6 *Une clôture algébrique de k est une extension algébrique K tel que tout polynôme $P \in k[X]$ se scinde sur K, c'est-à-dire*

$$P(X) = \prod_{i=1}^{n} (X - a_i) \qquad avec \qquad a_i \in K.$$

Proposition 2.1.1 *Tout corps k admet une clôture algébrique.*

Proposition 2.1.2 *Deux clôtures algébriques de k sont k-isomorphes.*

Soit k un corps et $P \in k[X]$ un polynôme (pas nécessairement irréductible). En fixant une clôture algébrique $\overline{k}$ de k on peut écrire $P(X) = \prod_{i=1}^{n} (X - a_i)$ avec $n = \deg P$.

Définition 2.1.7 *On appelle corps de décomposition de P ou corps des racines de P le corps*

$$K_P := k[a_1, a_2, \ldots, a_n].$$

On vérifiera que K_P est une extension finie de k et que K_P ne dépend pas du choix de la clôture algébrique $\overline{k}$.

Exemples.

1. Soit $k = \mathbb{Q}$ et $P = X^5 - 2$. Alors $K_P = \mathbb{Q}[\sqrt[5]{2}, e^{\frac{2i\pi}{5}}]$.
2. Soit $k = \mathbb{Q}$ et $P = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \ldots + X^{p-1}$ pour p premier. Alors $K_P = \mathbb{Q}[e^{\frac{2i\pi}{p}}]$

Définition 2.1.8 *Soit K/k une extension algébrique finie. Un automorphisme de corps $\sigma : K \to K$ qui agit trivialement sur k, c'est-à-dire $\sigma(x) = x$ pour tout $x \in k$ est appelé un automorphisme de l'extension K/k. L'ensemble des automorphismes de l'extension K/k forme un groupe pour la composition, noté* $\mathrm{Aut}(K/k)$.

Remarques.

1. Soit $P \in k[X]$ et soit K_P son corps de décomposition. En général les corps K_P et $L := K[X]/(P)$ ne coincident pas ! Si l'on note a la classe de l'indéterminée X dans L le polynôme P se factorise $P(X) = (X - a)Q(X)$ dans $L[X]$, mais en général Q n'a pas toutes ses racines dans L

2. Soit $P \in k[X]$ et soit K_P son corps de décomposition. Si $x \in K_P$ est une racine de P, alors $\sigma(x)$ est aussi une racine de P pour tout automorphisme $\sigma \in \mathrm{Aut}(K_P/k)$. Cela résulte du calcul suivant. On note $P(X) = \sum_{i=1}^{n} a_i X^i$ avec $a_i \in k$.

$$P(\sigma(x)) = \sum_{i=1}^{n} a_i \sigma(x)^i = \sigma(\sum_{i=1}^{n} a_i x^i) = \sigma(P(x)) = 0.$$

Ainsi si l'on choisit un ordre sur les n racines de P (qu'on suppose toutes distinctes pour simplifier) on obtient un homomorphisme de groupe

$$\mathrm{Aut}(K_P/k) \hookrightarrow S_n,$$

qui est injectif : en effet, comme K_P est engendré par les racines de P la permutation induite sur les racines de P détermine l'automorphisme de l'extension K_P/k.

2.2 Extensions galoisiennes

Définition 2.2.1 *On dit qu'un polynôme $P \in k[X]$ est séparable si tous ses facteurs irréductibles n'ont que des racines simples dans une clôture algébrique de k.*

Définition 2.2.2 *On dit qu'une extension algébrique K/k est séparable si pour tout élément $x \in K$ le polynôme minimal $\mathrm{Min}_k(x) \in k[X]$ est séparable.*

Exemples.

1. Si la caractéristique de k est égale à 0, toute extension de k est séparable. En effet soit $P = \mathrm{Min}_k(x)$ un polynôme minimal. Si P a une racine double a, alors $P(a) = P'(a) = 0$. Ceci implique que le pgcd de P et P' n'est pas un polynôme constant, donc P n'est pas irréductible, contradiction.
2. Soit k_0 un corps de caractéristique $p > 0$ et soit T un élément transcendant sur k_0. On pose $k = k_0(T^p)$ et $K = k_0(T)$. Alors $[K : k] = p$ et $\mathrm{Min}_k(T) = X^p - T^p \in k[X]$. Ce polynôme n'est pas séparable, car il s'écrit $X^p - T^p = (X - T)^p$ dans $K[T]$. Par conséquent l'extension K/k n'est pas séparable.

Définition 2.2.3 *On dit qu'un corps k est parfait si la caractéristique de k est égale à 0 ou bien si le morphisme de Frobenius $F : k \to k$, $F(x) = x^p$ est un isomorphisme quand la caractéristique du corps k est égale à $p > 0$.*

Exemple.
Le corps fini $\mathbb{F}_p$ est parfait. Le corps $\mathbb{F}_p(T)$ n'est pas parfait si T est transcendant.

Proposition 2.2.1 *Un corps k est parfait si et seulement si toute extension algébrique K/k est séparable.*

Définition 2.2.4 *On dit qu'une extension algébrique K/k est normale si pour tout $x \in K$ le polynôme minimal $\mathrm{Min}_k(x)$ se scinde dans $K[X]$, c'est-à-dire si*

$$\mathrm{Min}_k(x) = \prod_{i=1}^{n} (X - a_i) \qquad \textit{avec} \qquad a_i \in K.$$

Exemple.
L'extension $\mathbb{Q}[\sqrt[5]{2}]$ n'est pas normale. En effet le polynôme minimal $P := \mathrm{Min}_{\mathbb{Q}}(\sqrt[5]{2}) = X^5 - 2$ n'a pas toutes ses racines dans $\mathbb{Q}[\sqrt[5]{2}]$. Posons $\omega = e^{\frac{2i\pi}{5}}$. Alors le corps de décomposition K_P est égal à $\mathbb{Q}[\sqrt[5]{2}, \omega]$. C'est une extension normale de $\mathbb{Q}$ — voir plus loin.

Définition 2.2.5 *On dit qu'une extension finie K/k est galoisienne si elle est normale et séparable.*

Exemple.
Soit $k = \mathbb{Q}$ et $K = \mathbb{Q}[\zeta]$ avec $\zeta^p = 1$ et p premier. Alors $\mathrm{Aut}(K/k) = (\mathbb{Z}/p\mathbb{Z})^*$. Si $i \in (\mathbb{Z}/p\mathbb{Z})^*$, l'automorphisme σ_i associé opère sur K en envoyant le générateur ζ sur ζ^i.

Définition 2.2.6 *Soit K/k une extension finie avec groupe d'automorphismes $G = \mathrm{Aut}(K/k)$. Soit H un sous-groupe de G. Le corps fixé par H est le corps*

$$K^H := \{x \in K \mid \sigma(x) = x \quad \forall \sigma \in H\}.$$

Bien entendu, on a les inclusions $k \subset K^H \subset K$.

Proposition 2.2.2 *Soit K/k une extension finie avec groupe d'automorphismes $G = \mathrm{Aut}(K/k)$. Alors les assertions suivantes sont équivalentes.*

1. *L'extension K/k est galoisienne.*
2. *On a $k = K^H$ pour un sous-groupe $H \subset G$.*
3. *Le corps K est égal au corps de décomposition K_P d'un polynôme séparable $P \in k[X]$.*

Définition 2.2.7 *Si l'extension finie K/k est galoisienne, on appelle G le groupe de Galois — c'est un groupe fini. Parfois on le note aussi* $\mathrm{Gal}(K/k)$.

Remarque.
Pour une extension K/k finie et galoisienne, on a

$$|G| = [K : k] \qquad \text{et} \qquad k = K^G.$$

Proposition 2.2.3 *Soit K/k une extension finie galoisienne et soit $k \subset L \subset K$ une extension intermédiaire. Alors l'extension K/L est aussi galoisienne.*

Démonstration. Soit $x \in K$. Considérons les deux polynômes minimaux $\mathrm{Min}_k(x)$ et $\mathrm{Min}_L(x)$ comme des polynômes à coefficients dans L. Par définition du polynôme minimal, $\mathrm{Min}_L(x)$ divise $\mathrm{Min}_k(x)$. Ainsi toutes les racines de $\mathrm{Min}_L(x)$ sont simples et contenues dans K. ∎

Proposition 2.2.4 *Soit L/k une extension finie et séparable. Alors il existe une extension K/L tel que K/k soit galoisienne, c'est-à-dire toute extension finie et séparable est contenue dans une extension galoisienne.*

Démonstration. On sait que L admet un nombre fini de générateurs $x_1, \ldots, x_n$, c'est-à-dire L est de la forme $L = k[x_1, \ldots, x_n]$. Posons $P_i = \mathrm{Min}_k(x_i)$ et $P = \prod_{i=1}^n P_i$. Alors P est un polynôme séparable (car L est séparable) et on pose $K = K_P$. C'est une extension galoisienne de k (Proposition 2.2.2) et elle contient L. ∎

Théorème 2.2.1 (Théorème fondamental de la théorie de Galois) *Soit K/k une extension galoisienne finie et G son groupe de Galois. Alors on a une bijection entre les ensembles suivants*

$$\begin{array}{rcl} \{k \subset L \subset K\} & \longleftrightarrow & \{H < G\} \\ L & \longrightarrow & \mathrm{Gal}(K/L) \\ K^H & \longleftarrow & H \end{array}$$

Ces bijections sont inverses l'une de l'autre. Etant donné un sous-groupe $H < G$ on a l'équivalence

$$K^H/k \quad \textit{galoisienne} \qquad \Longleftrightarrow \qquad H \triangleleft G,$$

et dans ce cas $\mathrm{Gal}(K^H/k) = G/H$.

2.3 Corps finis

Soit p un nombre premier et k un corps fini de caractéristique p. Comme k est un $\mathbb{F}_p$-espace vectoriel de dimension finie n on obtient que le cardinal de k est égal à p^n. Le groupe multiplicatif k^* a $p^n - 1$ éléments, donc pour tout $x \in k^*$ on a $x^{p^n-1} = 1$. En rajoutant l'élément 0 on voit que tout $x \in k$ est racine du polynôme

$$P_n := X^{p^n} - X \in \mathbb{F}_p[X].$$

Le polynôme P_n est séparable : en effet une racine double de P_n annulerait la dérivée $P_n' = -1$. Soit K_{P_n} le corps de décomposition du polynôme P_n dans une clôture algébrique fixé $\overline{\mathbb{F}}_p$. On choisit un plongement de k dans $\overline{\mathbb{F}}_p$.

Proposition 2.3.1 *On a les assertions suivantes.*

1. *Le corps fini k est isomorphe au corps de décomposition K_{P_n}. On le notera $\mathbb{F}_{p^n}$.*
2. *L'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne et on a un isomorphisme*

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \qquad \overline{1} \mapsto F$$

où F désigne le Frobenius de $\mathbb{F}_{p^n}$.

Démonstration. D'après ce qui précède il est clair que $k \subset K_{P_n}$. Pour montrer l'égalité il suffit montrer que K_{P_n} à p^n éléments. Par définition K_{P_n} est engendré comme $\mathbb{F}_p$-algèbre par les p^n racines du polynôme P_n. Il suffit donc de vérifier que si x et y sont racines de P_n, alors $x \cdot y$ et $x + y$ sont aussi racines de P_n. Ceci résulte directement de l'exercice 2.6.2.

D'après la proposition 2.2.2 l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne. Il est clair que le morphisme de Frobenius $F \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est un élément d'ordre n, ce qui prouve la deuxième assertion. ∎

Soit $q = p^n$ et m un entier. On note F_q le morphisme d'élévation à la puissance q, c'est-à-dire $F_q(x) = x^q$. On montre sans difficultés la proposition suivante.

Proposition 2.3.2 *L'extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ est une extension galoisienne et son groupe de Galois est isomorphe au groupe cyclique $\mathbb{Z}/m\mathbb{Z}$ et est engendré par F_q.*

On aura besoin du résultat suivant sur la factorisation des polynômes de $\mathbb{F}_q[T]$.

Proposition 2.3.3 *Soit $P \in \mathbb{F}_q[T]$ un polynôme irréductible de degré d. Soit n un entier et e le pgcd de n et d. Alors le polynôme P se factorise dans $\mathbb{F}_{q^n}[T]$ en e polynômes irréductibles de même degré $\frac{d}{e}$, c'est-à-dire on a $P = P_1 \cdot P_2 \cdots P_e$ avec $P_i \in \mathbb{F}_{q^n}[T]$.*

Démonstration. Considérons un facteur irréductible $P_1 \in \mathbb{F}_{q^n}[T]$ de la décomposition du polynôme P dans $\mathbb{F}_{q^n}[T]$. Le groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ opère sur les facteurs irréductibles et comme P est irréductible, on en déduit que la décomposition de P est de la forme $P = P_1 \cdot P_2 \cdots P_k$, où l'ensemble des polynômes $\{P_1, P_2, \ldots, P_k\}$ est l'orbite du polynôme P_1 sous le groupe $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

Déterminons le degré de P_1. Pour cela considérons le corps de rupture du polynôme P : c'est une extension de degré d, donc isomorphe à l'extension $\mathbb{F}_{q^d}/\mathbb{F}_q$, qui est galoisienne de groupe $\mathbb{Z}/d\mathbb{Z}$. Soit a une racine de P dans $\mathbb{F}_{q^d}$. Alors le polynôme P se scinde

$$P(T) = \prod_{\sigma \in \mathbb{Z}/d\mathbb{Z}} (T - \sigma(a)).$$

Comme $P_1 \in \mathbb{F}_{q^n}[T]$ est irréductible le morphisme de Frobenius de $\mathbb{F}_{q^n}$ opère transitivement sur les racines de P_1. Ainsi on voit que la partition des racines en k sous-ensembles (= racines de P_i pour $i = 1, \ldots, k$) correspond aux orbites de l'automorphisme $F_{q^n} = (F_q)^n$ sur les d racines de P. Or ces d racines de P sont en bijection avec le groupe $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \mathbb{Z}/d\mathbb{Z}$. Sous cette bijection les racines de P_1 correspondent au sous-groupe cyclique engendré par la classe de n dans $\mathbb{Z}/d\mathbb{Z}$, c'est-à-dire le groupe cyclique $\mathbb{Z}/m\mathbb{Z}$ avec $m = \frac{d}{e}$, où $e = \mathrm{pgcd}(n, d)$. Il en résulte que $\deg P_1 = \frac{d}{e}$ et qu'il y a $k = e$ facteurs irréductibles. ∎

2.4 Extensions transcendantes

Définition 2.4.1 *Soit K/k une extension et $x_1, \ldots, x_n \in K$. On dit que les éléments $x_1, \ldots, x_n$ sont algébriquement indépendants si l'homomorphisme d'algèbre*

$$k[X_1, \ldots, X_n] \to K \qquad P \mapsto P(x_1, \ldots, x_n)$$

est injectif, c'est-à-dire s'il n'existe pas de polynôme non nul P tel que $P(x_1, \ldots, x_n) = 0$.

Exemple. Les réels e et π sont algébriquement indépendants.

Définition 2.4.2 *Soit K/k une extension et $x_1, \ldots, x_n \in K$ des éléments algébriquement indépendants. Le corps de fraction de l'anneau $k[x_1, \ldots, x_n]$ est noté*

$$k(x_1, \ldots, x_n) = \mathrm{Frac}(k[x_1, \ldots, x_n]) \subset K.$$

On dit qu'une extension L/k est transcendante pure si elle est isomorphe à un corps $k(x_1, \ldots, x_n)$ avec $x_1, \ldots, x_n$ algébriquement indépendants sur k.

Définition 2.4.3 *On dit que K est une extension de type fini de k si K est de la forme $K = \mathrm{Frac}(k[x_1, \ldots, x_n])$, c'est-à-dire K admet un nombre fini de générateurs.*

Remarque. Attention ! Il y a deux notions de finitude pour une extension K/k : finie et de type finie. Bien entendu être fini entraîne être de type fini.

Théorème 2.4.1 *Soit K une extension de k de type fini. Alors il existe un sous-ensemble $A = \{x_1, \ldots, x_n\}$ d'éléments algébriquement indépendants tel que*

$$k \subset k(x_1, \ldots, x_n) \subset K$$

et l'extension $K/k(x_1, \ldots x_n)$ est finie (donc algébrique). De plus tous les sous-ensembles $A = \{x_1, \ldots, x_n\}$ d'éléments algébriquement indépendants tel que $K/k(x_1, \ldots x_n)$ est finie ont le même cardinal, appelé le degré de transcendance de K sur k et noté $\mathrm{degtr}_k(K)$.

Exemples.

On a $\mathrm{degtr}_k(k(x)) = 1$ si x est transcendant sur k et $\mathrm{degtr}_k(k(x)) = 0$ si x est algébrique sur k.

Définition 2.4.4 *On dit qu'une base de transcendance $\{x_1, \ldots, x_n\}$ de K sur k est séparable si l'extension $K/k(x_1, \ldots, x_n)$ est séparable.*

Théorème 2.4.2 *Si k est parfait alors toute extension K/k de type fini admet une base de transcendance séparable.*

Définition 2.4.5 *On dit que K/k est un corps de fonctions (à n variables) si K/k est de type fini et* $\mathrm{degtr}_k(K) = 1$.

Définition 2.4.6 *Soit K/k un corps de fonctions. Le corps des éléments de K qui sont algébriques sur k est appelé le corps des constantes de K.*

2.5 Application de la théorie de Galois

Théorème 2.5.1 (Indépendance linéaire des caractères de Dedekind) *Soit K un corps et G un groupe. Alors toute famille $\{\chi_1, \ldots, \chi_m\}$ d'homomorphismes $\chi_i : G \longrightarrow K^*$ est linéairement indépendante, c'est-à-dire si $\sum_{i=1}^m a_i\chi_i = 0$ avec $a_i \in K$, alors $a_i = 0$ pour tout i.*

Démonstration. On le démontre par récurrence sur m. Pour $m = 1$ c'est évident. Supposons que toute famille de $m-1$ caractères est linéairement indépendante. Considérons m caractères $\chi_1, \ldots, \chi_m$ tous distincts. En particulier $\chi_1 \neq \chi_2$. Il existe donc un $g \in G$ tel que $\chi_1(g) \neq \chi_2(g)$. Considérons une relation linéaire à coefficients dans K entre les m caractères, c'est-à-dire

$$\forall x \in G, \qquad a_1\chi_1(x) + a_2\chi_2(x) + \ldots + a_m\chi_m(x) = 0. \tag{2.1}$$

En remplaçant x par $g \cdot x$ on obtient la relation (notons que $\chi_i(g \cdot x) = \chi_i(g)\chi_i(x)$)

$$\forall x \in G, \qquad a_1\chi_1(g)\chi_1(x) + a_2\chi_2(g)\chi_2(x) + \ldots + a_m\chi_m(g)\chi_m(x) = 0. \tag{2.2}$$

On multiplie maintenant la relation (2.1) par $\chi_1(g)$ et on soustraie (2.2) :

$$\forall x \in G, \qquad a_2(\chi_1(g) - \chi_2(g))\chi_2(x) + \ldots + a_m(\chi_1(g) - \chi_m(g))\chi_m(x) = 0.$$

Ceci est une relation linéaire sur $m-1$ caractères, donc d'après l'hypothèse de récurrence on a $a_i(\chi_1(g) - \chi_i(g)) = 0$ pour tout $i = 2, \ldots, m$. Comme $\chi_1(g) - \chi_2(g) \neq 0$, on en déduit que $a_2 = 0$. Ainsi la relation (2.1) ne comporte que $m-1$ termes et on peut appliquer à nouveau l'hypothèse de récurrence. D'où $a_i = 0$ pour tout $i = 1, \ldots, m$. ∎

Dans la suite on utilisera le cas particulier $G = K^*$.

Proposition 2.5.1 *Toute famille $\{\sigma_1, \ldots, \sigma_m\}$ d'homomorphismes de corps $\sigma_i : K^* \longrightarrow K^*$ distincts est linéairement indépendante.*

Corollaire 2.5.1 *Soit K/k une extension galoisienne et $\{\alpha_1, \ldots, \alpha_m\}$ une k-base de K. On note les éléments du groupe de Galois $\mathrm{Gal}(K/k) = \{\sigma_1, \ldots, \sigma_m\}$. Alors la matrice carrée d'ordre m $M = (\sigma_i(\alpha_j))_{i,j}$ est inversible.*

Démonstration. Supposons par l'absurde qu'il existe un vecteur non nul $(c_1, \ldots, c_m) \in K^m$ dans $\ker M$, ce qui équivaut aux m équations

$$\sum_{i=1}^{m} c_i \sigma_i(\alpha_j) = 0 \qquad j = 1, \ldots, m.$$

Comme $\{\alpha_1, \ldots, \alpha_m\}$ est une base de K, on obtient une relation $\sum_{i=1}^m c_i\sigma_i = 0$, ce qui contredit l'indépendance linéaire des σ_i (Proposition 2.5.1). ∎

Définition 2.5.1 *Soit K/k une extension galoisienne de groupe $G = \mathrm{Gal}(K/k)$ et soit V un K-espace vectoriel de dimension finie. On dit que V est muni d'une action linéaire galoisienne de G s'il existe une représentation linéaire $\rho : G \longrightarrow \mathrm{GL}(V)$ tel que*

$$\sigma(\lambda v) = \sigma(\lambda)\sigma(v), \qquad \forall \lambda \in K, \quad \forall v \in V.$$

Pour simplifier la notation on écrit σ au lieu de $\rho(\sigma)$. En d'autres mots l'action linéaire ρ est galoisienne si l'action de G sur V est compatible avec l'action de G sur le corps des scalaires K.

Exemple.
L'espace vectoriel $V = K^n$ muni de l'action $\sigma(x_1, \ldots, x_n) = (\sigma(x_1), \ldots, \sigma(x_n))$.

Proposition 2.5.2 *Soit K/k une extension galoisienne de groupe $G = \mathrm{Gal}(K/k)$. Soit V un K-espace vectoriel de dimension finie muni d'une action galoisienne de G. Alors on a*

1. *L'ensemble des vecteurs G-invariants $V^G = \{v \in V \mid \sigma(v) = v\}$ est un k-espace vectoriel.*
2. *Il existe une K-base $\{v_1, v_2, \ldots, v_n\}$ de V tel que $v_i \in V^G$ pour tout i.*

Remarques.

1. Noter que V^G n'est pas un K-sous-espace vectoriel. En effet on a pour $v \in V^G$, $\sigma(\lambda v) = \sigma(\lambda)v \neq \lambda v$ si λ n'appartient pas à k.

2. On peut exprimer la deuxième assertion en termes de produit tensoriel :

$$V = V^G \otimes_k K.$$

Démonstration. La première partie resulte immédiatement du fait que $K^G = k$.

Montrons maintenant qu'il existe une K-base $\{v_1, v_2, \ldots, v_n\}$, où les vecteurs v_i sont dans l'espace G-invariant V^G. Choisissons une k-base $\{b_1, \ldots, b_n\}$ de V^G. Ceci est bien possible, car V est de dimension finie sur K et K est de dimension finie sur k, donc $V^G \subset V$ est aussi de dimension finie sur k. Introduisions le k-sous-espace vectoriel $\Pi \subset V$

$$\Pi := V^G \otimes_k K = \{v = \sum_{i=1}^{m} \lambda_i b_i \mid \lambda_i \in K\}.$$

Il va d'abord montrer que $\Pi = V$. Soit $\{\alpha_1, \ldots, \alpha_m\}$ une k-base de K. On notera les éléments du groupe de Galois $\mathrm{Gal}(K/k) = \{\sigma_1 = \mathrm{id}, \ldots, \sigma_m\}$. Choisissons un vecteur $v \in V$ et introduisons les m vecteurs pour $j = 1, \ldots, m$

$$w_j = \sum_{i=1}^{m} \sigma_i(\alpha_j v) = \sum_{i=1}^{m} \sigma_i(\alpha_j)\sigma_i(v)$$

On peut exprimer ces égalités sous forme matricielle

$$\begin{pmatrix} w_1 \\ \ldots \\ w_m \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_m(\alpha_1) \\ \ldots & & \ldots \\ \sigma_1(\alpha_m) & \ldots & \sigma_m(\alpha_m) \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(v) \\ \ldots \\ \sigma_m(v) \end{pmatrix}$$

D'après le corollaire 2.5.1 la matrice $M = (\sigma_i(\alpha_j))_{i,j}$ est inversible. Donc en particulier $\sigma_1(v) = v$ s'écrit comme combinaison linéaire des vecteurs w_j. Vérifions que $w_j \in V^G$. En effet pour tout k et j on a les égalités

$$\begin{aligned} \sigma_k(w_j) &= \sum_{i=1}^{m} \sigma_k[\sigma_i(\alpha_j v)] = \sum_{i=1}^{m} (\sigma_k\sigma_i)(\alpha_j v) \\ &= \sum_{i=1}^{m} \sigma_i(\alpha_j v) = w_j. \end{aligned}$$

Ce raisonnement montre que la k-base $\{b_1, \ldots, b_n\}$ de V^G est un famille génératrice du K-espace vectoriel V. Pour conclure il faut encore vérifier que la famille $\{b_1, \ldots, b_n\}$ est K-linéairement indépendante. Pour cela considérons l'application K-linéaire

$$\Phi : K^n \longrightarrow V, \qquad (\lambda_i)_i \mapsto \sum_{i=1}^{n} \lambda_i b_i.$$

On remarque que Φ est G-équivariant, donc le noyau $\ker \Phi$ est un sous-espace vectoriel de K^n qui est stable par l'action de G, donc muni d'une action galoisienne de G. On peut donc

appliquer ce qu'on a montré précédemment : le K-espace vectoriel $\ker \Phi$ est engendré sur K par les vecteurs G-invariants. Or $(\ker \Phi)^G = \ker \Phi \cap k^n$. Ainsi $\ker \Phi \cap k^n = \{0\}$ entraine $\ker \Phi = \{0\}$, ce qui prouve l'indépendance linéaire de la famille $\{b_1, \ldots, b_n\}$. ∎

Remarque.

De manière plus générale on peut montrer sans hypothèse sur l'extension K/k qu'une famille de vecteurs libre sur k reste libre sur K. En termes savants ceci s'exprime par l'exactitude du foncteur $T : k - \text{ev} \to K - \text{ev}$ défini par $T(V) = V \otimes_k K$.

2.6 Exercices

Exercice 2.6.1 Montrer qu'un morphisme de corps $\phi : k \to K$ est injectif.

Exercice 2.6.2 Soit k un corps de caractéristique $p > 0$ et soit F l'application d'élévation à la puissance p, c'est-à-dire $F(x) = x^p$ pour tout $x \in k$.

1. Montrer que le coefficient binomial $\binom{p}{n}$ est divisible par p pour $0 < n < p$.
2. En déduire que l'application F est un morphisme de corps qui est $\mathbb{F}_p$-linéaire, c'est-à-dire

$$F(xy) = F(x) \cdot F(y), \qquad F(x+y) = F(x) + F(y), \qquad F(\lambda x) = \lambda F(x)$$

pour $x, y \in k$ et $\lambda \in \mathbb{F}_p$.

On appelle F le *morphisme de Frobenius* de k.

Exercice 2.6.3 Soit A un anneau principal, c'est-à-dire tous ses idéaux sont engendrés par un élément — par exemple l'anneau de polynômes $A = k[X]$ est principal. On note $(a) \subset A$ l'idéal engendré par l'élément $a \in A$. Montrer que les trois assertions suivantes sont équivalentes.

1. L'élément a est irréductible.
2. L'idéal (a) est premier.
3. L'idéal (a) est maximal.

Exercice 2.6.4 Soit P un polynôme irréductible de $k[X]$ de degré n. Montrer qu'il existe une extension K de k tel que P soit scindé dans K, c'est-à-dire

$$P(X) = \prod_{i=1}^{n} (X - a_i)$$

avec $a_i \in K$ et tel que $[K : k] \leq n!$.

Indication : considérer le corps de rupture de P et faire une récurrence sur le degré de P.

Exercice 2.6.5 Soit K une extension de k et $x \in K$. Montrer que les assertions suivantes sont équivalentes.

1. L'élément x est algébrique sur k.
2. L'algèbre $k[x]$ est de dimension finie sur k.
3. L'algèbre $k[x]$ est un corps.

Exercice 2.6.6 Soit K une extension de k. Montrer que l'ensemble des éléments de K qui sont algébriques sur k est un corps. On appelle ce corps la clôture algébrique de k dans K.

Exercice 2.6.7 On considère les extensions $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt[3]{2})$ sur $\mathbb{Q}$.

1. Déterminer leurs degrés.
2. Est-ce que ces extensions sont galoisiennes ? Si oui, déterminer le groupe de Galois.

Exercice 2.6.8 Calculer le degré de $\mathbb{Q}(\sqrt{3},\sqrt{2})$ sur $\mathbb{Q}$. Comparer $\mathbb{Q}(\sqrt{3},\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Déterminer le polynôme minimal de $\sqrt{3}+\sqrt{2}$ sur $\mathbb{Q}$. Montrer que l'extension $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ de $\mathbb{Q}$ est galoisienne et en déterminer le groupe de Galois.

Exercice 2.6.9 Montrer que l'extension $K := \mathbb{Q}[\sqrt[3]{2}, e^{\frac{2i\pi}{3}}]$ de $\mathbb{Q}$ est galoisienne de groupe de Galois S_3, le groupe symétrique sur 3 lettres. Déterminer toutes les extensions intermédiaires $\mathbb{Q} \subset L \subset K$.

Exercice 2.6.10 Soit k un corps et $K = k(T)$ l'extension transcendante pure en une variable de k. Déterminer la clôture algébrique de k dans K.

Chapitre 3

Variétés algébriques

Le but de ce chapitre est de présenter les notions élémentaires de la théorie des variétés algébriques sur un corps quelconque. Pour une introduction plus détaillé on pourra lire les chapitres 1 et 2 de [P] ou bien [H].

Dans ce chapitre k désigne un corps parfait et $\overline{k}$ une clôture algébrique.

3.1 Espace affine et variétés affines

Définition 3.1.1 *Soit k un corps et $n \in \mathbb{N}^*$. L'ensemble des n-uplets dans k noté*

$$\mathbb{A}^n(k) = \{(a_1, \ldots, a_n) \mid a_i \in k\}$$

est appelé l'ensemble des points k-rationnels de l'espace affine de dimension n.

Remarques.

1. Pour toute extension de corps K/k on a une inclusion ensembliste $\mathbb{A}^n(k) \subset \mathbb{A}^n(K)$.
2. La définition précédente ne définit pas l'espace affine $\mathbb{A}^n$, mais seulement la notion de point k-rationnel de l'espace affine. La définition de $\mathbb{A}^n$ sera donnée plus tard.

Considérons un point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$. On peut associer à P un homomorphisme de k-algèbres appelé l'évaluation au point P

$$\mathrm{ev}_P : k[X_1, \ldots X_n] \to k, \qquad f \mapsto f(P) := f(a_1, \ldots, a_n).$$

Soit I un idéal de $k[X_1, \ldots X_n]$. On associe à I le sous-ensemble de $\mathbb{A}^n(\overline{k})$ défini par

$$V(I) = \{P \in \mathbb{A}^n(\overline{k}) \mid f(P) = 0,\ \forall f \in I\}.$$

Remarquons que l'anneau $k[X_1, \ldots X_n]$ est noethérien (théorème de Hilbert) et que par conséquent tout idéal I admet un nombre fini de générateurs $f_1, \ldots, f_m$. Ainsi on voit que l'ensemble $V(I)$ est défini par les m équations $f_i(P) = 0$.

Définition 3.1.2 *On dit qu'un sous-ensemble $V \subset \mathbb{A}^n(\overline{k})$ est algébrique, s'il existe un idéal $I \subset \overline{k}[X_1, \ldots X_n]$ tel que $V = V(I)$.*

On peut définir une topologie sur l'ensemble $\mathbb{A}^n(\overline{k})$, la topologie de Zariski : les fermés pour cette topologie sont par définition les sous-ensembles algébriques. On vérifie que cela donne effectivement un topologie sur $\mathbb{A}^n(\overline{k})$, c'est-à-dire l'intersection quelconque de fermés est un fermé et une réunion finie de fermés est un fermé.

Exemple.
La droite affine $\mathbb{A}^1(\overline{k})$. On sait que l'anneau $\overline{k}[X]$ est principal, donc tout idéal I est de la forme $I = (P)$, où P est un polynôme de degré d en X. Comme $\overline{k}$ est algébriquement clos, P se scinde et $V(I)$ est une réunion d'au plus d points $\overline{k}$-rationnels.

Remarque.
La topologie de Zariski n'est pas séparée : l'intersection de deux ouverts de $\mathbb{A}^n(\overline{k})$ est toujours non vide.

Définition 3.1.3 *Soit $Y \subset X$ un sous-ensemble d'un espace topologique X. On dit que Y est irréductible si Y n'est pas la réunion $Y_1 \cup Y_2$ de deux fermés Y_1 et Y_2 de X.*

Proposition 3.1.1 *Soit $I \subset \overline{k}[X_1, \ldots, X_n]$ un idéal. Alors on a une équivalence*

$$I \text{ premier} \qquad \Longleftrightarrow \qquad V(I) \text{ irréductible.}$$

Remarque.
Attention ! Il est important de considérer les idéaux dans $\overline{k}[X_1, \ldots, X_n]$, même s'il sont définis sur un corps plus petit. Considérons l'exemple suivant : $k = \mathbb{Q}$ et $I = (X_1^2 - 2X_2^2) \subset \mathbb{Q}[X_1, X_2] \subset \overline{\mathbb{Q}}[X_1, X_2]$. On constate que I est premier en tant qu'idéal dans $\mathbb{Q}[X_1, X_2]$, mais se factorise $I = (X_1 + \sqrt{2}X_2)(X_1 - \sqrt{2}X_2)$ dans $\overline{\mathbb{Q}}[X_1, X_2]$. Ainsi $V(I) \subset \mathbb{A}^2(\overline{\mathbb{Q}})$ n'est pas irréductible.

Définition 3.1.4 *Une variété affine V est un fermé irréductible de $\mathbb{A}^n(\overline{k})$. De manière équivalente une variété affine un sous-ensemble algébrique $V(I)$, où I est un idéal premier de $\overline{k}[X_1, \ldots, X_n]$*

Exemples.
On considère l'idéal $I = (X_1X_2) \subset \overline{k}[X_1, X_2]$. Alors $V(I)$ est la réunion de deux droites $D_1 = V(X_1)$ et $D_2 = V(X_2)$ dans $\mathbb{A}^2(\overline{k})$.

Soit S un sous-ensemble de $\mathbb{A}^n(\overline{k})$. On associe à S un idéal $\mathcal{I}(S) \subset \overline{k}[X_1, \ldots, X_n]$ défini par

$$\mathcal{I}(S) = \{f \in \overline{k}[X_1, \ldots, X_n] \mid f(P) = 0 \ \forall P \in S\}.$$

Le théorème suivant montre que l'application définie par $\mathcal{I}$ est en fait l'inverse de celle déteriné par Z si l'on se restreint aux variétés affines.

Théorème 3.1.1 (Théorème des zéros de Hilbert) *Pour tout idéal $I \subset \overline{k}[X_1, \ldots, X_n]$ on a l'égalité suivante dans $\overline{k}[X_1, \ldots, X_n]$*

$$\mathcal{I}(V(I)) = \mathrm{Rad}(I),$$

où l'idéal $\mathrm{Rad}(I) = \{f \in \overline{k}[X_1, \ldots, X_n] \mid f^n \in I\}$ est appelé le radical de I.
En particulier, si I est premier on a $\mathcal{I}(V(I)) = I$.

Corollaire 3.1.1 *On a une bijection entre l'ensemble des variétés affines $V \subset \mathbb{A}^n(\overline{k})$ et l'ensemble des idéaux premiers de $\overline{k}[X_1, \ldots, X_n]$.*

Remarque.
Le théorème des zéros de Hilbert n'est plus vrai sur un corps k qui n'est pas algébriquement clos. Par exemple si l'on prend $I = (X_1^2 + X_2^2 + 1) \subset \mathbb{R}[X_1, X_2]$, on a $V(I) = \emptyset$ et $\mathcal{I}(V(I)) = \mathbb{R}[X_1, X_2]$. Par contre $\mathrm{Rad}(I) = I$, car $X_1 + X_2 + 1$ est irréductible sur $\mathbb{R}$.

3.2 Actions galoisiennes

Définition 3.2.1 *Soit $V = V(I) \subset \mathbb{A}^n(\overline{k})$ une variété affine. On dit que V est défini sur le corps k si l'idéal $I = \mathcal{I}(V) \subset \overline{k}[X_1, \ldots X_n]$ peut être engendré par des éléments dans $k[X_1, \ldots X_2]$. Dans ce cas on note V/k au lieu de V.*

Remarques.

1. Comme $\overline{k}[X_1, \ldots X_n]$ est un anneau neothérien, tout idéal $I \subset \overline{k}[X_1, \ldots X_n]$ est engendré par un nombre fini de générateurs $I = (f_1, \ldots, f_m)$ avec $f_i \in \overline{k}[X_1, \ldots X_n]$· Les polnômes f_i n'ont qu'un nombre fini de coefficients $a_{ij} \in \overline{k}$. Tous les a_{ij} sont algébriques, donc $L = k[a_{ij}]$ est une extension finie de k. Toute variété affine V définie sur $\overline{k}$ est en fait définie sur une extension finie L de k.
2. Par le même raisonnement on montre que tout point $\overline{k}$-rationnel $P \in \mathbb{A}^n(\overline{k})$ est définie sur une extension finie L de k, c'est-à-dire $P \in \mathbb{A}^n(L)$.

Soit $V \subset \mathbb{A}^n(\overline{k})$ une variété affine. On définit pour tout corps K tel que $k \subset K \subset \overline{k}$ l'idéal de $K[X_1, \ldots X_n]$

$$\mathcal{I}_K(V) = \{f \in K[X_1, \ldots X_n] \mid \ f(P) = 0 \ \ \forall P \in V\}.$$

Remarquons que dans ce cas le morphisme d'évaluation en $P \in \mathbb{A}^n(\overline{k})$ détermine un homomorphisme de K-algèbres $\mathrm{ev}_P : K[X_1, \ldots X_n] \to \overline{k}$.

Proposition 3.2.1 *Soit $V \subset \mathbb{A}^n(\overline{k})$ une variété affine. Alors on a une équivalence entre les assertions suivantes.*

1. *La variété affine V est définie sur k.*
2. *On a une égalité $\mathcal{I}_{\overline{k}}(V) = \mathcal{I}_k(V) \cdot \overline{k}[X_1, \ldots X_n]$.*

Démonstration. ∎

3.3 Espace projectif et variétés projectives

3.4 Exercices

Exercice 3.4.1 Déterminer le lieu singulier des courbes affines suivantes

$$C_1 \ : \ Y^2 = X^3 \qquad C_2 \ : \ 4X^2Y^2 = (X^2 + Y^2)^3.$$

Exercice 3.4.2 On considère les deux courbes projectives suivantes

$$C_1 \ : \ X^2+Y^2=Z^2 \qquad C_2 \ : \ X^2+Y^2=3Z^2.$$

1. Montrer que $C_2(\mathbb{Q})=\emptyset$. *Indication :* Réduire modulo 3.
2. On considère les deux applications

   $$\psi : C_1 \longrightarrow \mathbb{P}^1,\ \psi([X,Y,Z])=[X+Z,Y], \qquad \phi : \mathbb{P}^1 \longrightarrow C_1,\ \phi([S,T])=[S^2-T^2,2ST,S^2+T^2].$$

   Montrer que l'application ψ est régulière en tout point de C_1.
3. Montrer que ψ et ϕ sont inverses l'une de l'autre.
4. En déduire que $C_1(\mathbb{Q})=\mathbb{P}^1(\mathbb{Q})$ et que C_1 n'est pas isomorphe à C_2 sur $\mathbb{Q}$.
5. Montrer qu'il existe un isomorphisme défini sur $\mathbb{Q}[\sqrt{3}]$ entre C_1 et C_2.
6. Pour quels corps finis k existe-t-il un isomorphisme entre C_1 et C_2 qui est défini sur k ? *Indication :* utiliser la loi de réciprocité quadratique.

Exercice 3.4.3 Soit $C/\mathbb{Q}$ la courbe projective plane définie par l'équation homogène

$$5X^2+6XY+2Y^2=2YZ+Z^2.$$

Montrer que $C(\mathbb{Q})=\emptyset$.
Indication : Ecrire l'équation comme somme de carrés et réduire modulo un nombre premier.

Exercice 3.4.4 Soit $C/\mathbb{Q}$ la courbe projective définie par l'équation affine

$$Y^2=X^3+17.$$

1. Soient $P_1=(x_1,y_1)$ et $P_2=(x_2,y_2)$ des points distincts de $C=C(\overline{\mathbb{Q}})$ et soit D la droite passant par P_1 et P_2. Montrer que

   $$C\cap D=\{P_1,P_2,P_3\}$$

   et exprimer $P_3=(x_3,y_3)$ en fonction de P_1 et P_2.
2. Calculer P_3 pour $P_1=(-1,4)$ et $P_2=(2,5)$.
3. Montrer que si $P_1,P_2\in C(\mathbb{Q})$, alors $P_3\in C(\mathbb{Q})$.

Exercice 3.4.5 Soit p un nombre premier ≥ 3 et soit $C_p/\mathbb{Q}$ la conique dans $\mathbb{P}^2$ définie par l'équation

$$X^2+Y^2=pZ^2.$$

1. Montrer que $C_p(\mathbb{Q})\neq\emptyset$ si et seulement si $p\equiv 1 \mod 4$.
   Indication : Si $p\equiv 1 \mod 4$, utiliser le fait que p s'écrit comme somme de deux carrés d'entiers. Si $p\equiv 3 \mod 4$, réduire modulo p.
2. Si $p\equiv 1 \mod 4$, montrer qu'il existe un isomorphisme ϕ défini sur $\mathbb{Q}$

   $$\phi : \mathbb{P}^1 \longrightarrow C_p.$$

   Donner les équations de ϕ.
   Indication : Projeter à partir d'un point $P\in C_p(\mathbb{Q})$.

Exercice 3.4.6 Déterminer pour tout entier $m \geq 1$ le nombre $|C(\mathbb{F}_{p^m})|$ de points $\mathbb{F}_{p^m}$-rationnels pour les courbes projectives C suivantes

1. la droite projective $\mathbb{P}^1$,
2. la conique définie par $X^2 + Y^2 = Z^2$,
3. la cubique plane définie par $ZY^2 = X^3$.

Exercice 3.4.7 Soit n un entier ≥ 2 et soit C_n la courbe projective plane donnée par l'équation homogène (dite courbe de Fermat)

$$x^n + y^n + z^n = 0.$$

1. Pour quels couples (n, p) la courbe C_n considérée comme courbe sur $\mathbb{F}_p$ est-elle lisse ?
2. Montrer que pour $n = p - 1$ on a $|C_n(\mathbb{F}_p)| = 0$.

Exercice 3.4.8 Soit $V \subset \mathbb{P}^n$ une variété projective définie sur le corps fini $\mathbb{F}_q$.

1. Montrer que l'application

$$\varphi : \mathbb{P}^n \to \mathbb{P}^n, \qquad [x_0, \ldots, x_n] \mapsto [x_0^q, \ldots x_n^q]$$

   définit un morphisme $\varphi : V \to V$, appelé le morphisme de Frobenius.
2. Montrer que φ induit une bijection $\varphi_K : V(K) \to V(K)$ pour toute extension $K/\mathbb{F}_q$.
3. Soit $\mathbb{F}_q(V)$ le corps de fonctions de la variété V. On note $i : \mathbb{F}_q(V) \to \mathbb{F}_q(V)$ l'application définie par $i(f) = f \circ \varphi$. Calculer le degré $[\mathbb{F}_q(V) : i(\mathbb{F}_q(V))]$. En déduire que φ n'est pas un isomorphisme.
4. Montrer que $V(\mathbb{F}_q) = \{P \in V \mid \varphi(P) = P\}$.

Chapitre 4

Courbes projectives

4.1 Anneau de valuation discrète

4.2 Diviseurs et groupe de Picard

définir $\mathrm{Div}(C)$ et $\mathrm{Div}_+(C)$.

définir le nombre $\delta \in \mathbb{N}^*$ comme étant l'entier δ tel que l'image de l'homomorphisme deg : $\mathrm{Pic}(C) \to \mathbb{Z}$ soit égal à $\delta\mathbb{Z}$.

Proposition 4.2.1 *Soit $D \in \mathrm{Div}(C)$. Alors on a les assertions suivantes*

1. *L'ensemble $\mathcal{L}_k(D)$ est un k-espace vecoriel.*
2. *Si $D_1 \sim D_2$, alors $\mathcal{L}_k(D_1) \cong \mathcal{L}_k(D_2)$.*
3. *Si $\deg D < 0$, alors $\mathcal{L}_k(D) = \{0\}$.*
4. *Si $\deg D \geq 0$, alors $\dim \mathcal{L}_k(D) \leq \deg D + 1$.*

En particulier $\mathcal{L}_k(D)$ est un k-espace vectoriel de dimension finie. On notera cette dimension $l(D)$.

Démonstration. Montrons d'abord que $\mathcal{L}_k(D)$ est un k-espace vectoriel. Prenons $\varphi, \varphi' \in \mathcal{L}_k(D) \subset k(C)$. On a donc les deux relations $\mathrm{div}(\varphi) + D \geq 0$ et $\mathrm{div}(\varphi') + D \geq 0$. Ecrivons $D = \sum_P n_P P$ avec $n_P \in \mathbb{Z}$. Pour tout point fermé $P \in C$ on sait que la fonction $\mathrm{ord}_P : k(C)^* \to \mathbb{Z}$ est une valuation, c'est-à-dire

$$\mathrm{ord}_P(\varphi + \varphi') \geq \min(\mathrm{ord}_P(\varphi), \mathrm{ord}_P(\varphi')).$$

Or comme $\mathrm{ord}_P(\varphi) \geq -n_P$ et $\mathrm{ord}_P(\varphi') \geq -n_P$, on obtient par conséquent que $\mathrm{ord}_P(\varphi + \varphi') \geq -n_P$ pour tout $P \in C$, c'est-à-dire $\varphi + \varphi' \in \mathcal{L}_k(D)$. De plus comme $\mathrm{div}(\lambda\varphi) = \mathrm{div}(\varphi)$ pour tout $\lambda \in k^*$, on en déduit (1).

Si $D_1 \sim D_2$, il existe $\varphi_0 \in k(C)^*$ tel que $D_2 = D_1 + \mathrm{div}\varphi_0$. Considérons l'application k-linéaire $\mu : k(C) \to k(C)$ définie par la multiplication par φ_0, c'est-à-dire $\mu(\varphi) = \varphi\varphi_0$. Alors μ induit un isomorphisme

$$\mu : \mathcal{L}_k(D_2) \to \mathcal{L}_k(D_1) \qquad \mu(\varphi) = \varphi\varphi_0.$$

En effet pour $\varphi \in \mathcal{L}_k(D_2)$ on a les égalités

$$\mathrm{div}(\mu(\varphi) + D_1) = \mathrm{div}\varphi + \mathrm{div}\varphi_0 + D_1 = \mathrm{div}\varphi + D_2 \geq 0,$$

c'est-à-dire $\mu(\varphi) \in \mathcal{L}_k(D_1)$. Il est clair que μ est un isomorphisme.

Supposons qu'il existe un élément non nul $\varphi \in \mathcal{L}_k(D)$. Alors $\mathrm{div}(\varphi) + D$ est un diviseur effectif, donc $\deg(\mathrm{div}(\varphi) + D) \geq 0$. Or d'après la proposition **??** on sait que $\deg\ \mathrm{div}(\varphi) = 0$. D'où $\deg D \geq 0$. Ceci prouve l'assertion (3).

Montrons l'implication (4). Si $\mathcal{L}_k(D) = \{0\}$ il n'y a rien à montrer. On peut donc supposer qu'il existe un diviseur effectif Δ avec $\Delta \sim D$. D'après (2) on a un isomorphisme $\mathcal{L}_k(D) \cong \mathcal{L}_k(\Delta)$. Ecrivons $\Delta = \sum_P n_P P$ et choisissons une uniformisante $t_P \in \mathcal{O}_P \subset k(C)$ pour tout point fermé P du support de Δ. Soit $\varphi \in \mathcal{L}_k(\Delta)$. Par définition de $\mathcal{L}_k(\Delta)$ on a donc $\mathrm{ord}_P(\varphi) \geq -n_P$ et de manière équivalent $\mathrm{ord}_P(\varphi t_P^{n_P}) \geq 0$, c'est-à-dire $\varphi t_P^{n_P} \in \mathcal{O}_P$. On peut donc considérer l'application k-linéaire

$$\mathrm{ev}_\Delta : \mathcal{L}_k(\Delta) \longrightarrow \bigoplus_P \mathcal{O}_P/\mathfrak{M}_P^{n_P} \qquad \varphi \mapsto (\varphi t_P^{n_P} \bmod \mathfrak{M}_P^{n_P})$$

D'après **??** on sait que $\mathcal{O}_P/\mathfrak{M}_P^{n_P}$ est un k_P-espace vectoriel de dimension n_P, donc un k-espace vectoriel de dimension $n_P \deg P$. Le noyau de ev_Δ est alors le sous-espace vectoriel des fonctions rationnelles φ qui vérifient $\mathrm{ord}_P\mathrm{div}(\varphi t_P^{n_P}) \geq n_P$, ou de manière équivalent $\mathrm{ord}_P\ \mathrm{div}\ \varphi \geq 0$ pour tout point fermé P. Ainsi on obtient que φ est une fonction rationnelle sans pôles et d'après la prop **??** $\mathrm{ev}_\Delta = \mathcal{L}_k(0) = k$. Le théorème du rang donne alors l'inégalité annoncée. ∎

4.3 Formes différentielles

4.4 Le théorème de Riemann-Roch

Théorème 4.4.1 (Riemann-Roch) *Soit C une courbe projective lisse et soit ω un diviseur canonique de C. On note g le genre de C. Alors pour tout diviseur $D \in \mathrm{Div}(C)$ on a la relation*

$$l(D) - l(\omega - D) = \deg D + 1 - g.$$

4.5 Exercices

Exercice 4.5.1 Déterminer tous les points fermés de degré 1, 2 et 3 de la droite projective $\mathbb{P}^1_{\mathbb{F}_2}$ définie sur le corps $\mathbb{F}_2$. Pour chaque point de $\mathbb{P}^1_{\mathbb{F}_2}$ donner l'orbite sous le groupe de Galois $\mathrm{Gal}(\mathbb{F}_2)$ dans la droite projective $\mathbb{P}^1_{\overline{\mathbb{F}}_2}$ définie sur la clôture algébrique $\overline{\mathbb{F}}_2$.

Réponse : D'après le cours les points fermés de degré d de $\mathbb{P}^1_{\mathbb{F}_2}$ correspondent aux polynômes irréductible de degré d de $\mathbb{F}_2[t]$. On rajoute le point ∞ qui est de degré 1. On obtient ainsi : degré $1 : T$ et $T{+}1$; degré $2 : T^2{+}T{+}1$, l'orbite associée dans $\mathbb{P}^1_{\overline{\mathbb{F}}_2}$ est égale à $\{(x, 1); (x{+}1, 1)\} \subset \mathbb{P}^1(\mathbb{F}_4)$ où l'on utilise $\mathbb{F}_4 = \mathbb{F}_2[x]$ avec x une racine de $T^2 + T + 1$; degré $3 : T^3 + T + 1$ et $T^3 + T^2 + 1$. Il y a trois points dans chaque orbite.

Exercice 4.5.2 (diviseurs sur la droite projective) On introduit des coordonnées homogènes $[x, y]$ sur la droite projective $\mathbb{P}^1$ définie sur un corps k. On note $0 = [0, 1]$, $1 = [1, 1]$ et $\infty = [1, 0]$.

1. Montrer que le corps de fonctions $k(\mathbb{P}^1)$ est isomorphe à l'extension transcendante pure $k(t)$, où t désigne la fonction rationnelle $t = \frac{x}{y}$.
2. Déterminer les anneaux locaux $\mathcal{O}_0$, $\mathcal{O}_1$, $\mathcal{O}_\infty$ ($\subset k(\mathbb{P}^1)$) aux points $0, 1$ et ∞ et donner des uniformisantes t_0, t_1 et t_∞ en fonction de t.
3. Calculer les diviseurs principaux $\mathrm{div}(t_0), \mathrm{div}(t_1), \mathrm{div}(t_\infty)$.
4. Montrer que tout diviseur de degré 0 sur $\mathbb{P}^1$ est principal.
5. En déduire que $\mathrm{Pic}(\mathbb{P}^1) = \mathbb{Z}$.

Exercice 4.5.3 Déterminer le diviseur principal $\mathrm{div}(\varphi) \in \mathrm{Div}(\mathbb{P}^1_k)$ avec

$$\varphi(T) = \frac{T^3 - 2}{T^2 - 3} \in k(T) = k(\mathbb{P}^1)$$

dans les cas suivants $k = \mathbb{Q}$, $k = \overline{\mathbb{Q}}$ et $k = \mathbb{F}_5$.

Exercice 4.5.4 Soit k un corps et $a_1, a_2, a_3 \in k$ trois éléments distincts. On introduit la courbe projective C/k d'équation affine

$$y^2 = (x - a_1)(x - a_2)(x - a_3).$$

1. Donner l'équation homogène de la courbe projective $C \subset \mathbb{P}^2$. On notera les coordonnées homogènes $[x, y, z]$.
2. Montrer qu'il existe un seul point de C sur la droite à l'infini, donnée par l'équation homogène $z = 0$. On notera ce point P_∞. Donner les coordonnées de P_∞ et son degré sur k.
3. Montrer que la courbe C est lisse.
4. On note $P_i = [a_i, 0, 1] \in \mathbb{P}^2(k)$ pour $i = 1, 2, 3$. Déterminer les anneaux locaux $\mathcal{O}_{P_i} \subset k(C)$ et donner des uniformisantes. Donner le degré du point P_i.
5. Déterminer l'anneau local $\mathcal{O}_{P_\infty}$ et donner une uniformisante.
6. Montrer les égalités suivantes

$$\mathrm{div}(y) = \mathrm{div}(dx) = P_1 + P_2 + P_3 - 3P_\infty.$$

7. En déduire le degré de la classe canonique et le genre de C.

Exercice 4.5.5 On considère le point fermé P de la droite projective $\mathbb{P}^1_{\mathbb{Q}}$ déterminé par le polynôme
$p(T) = 1 + T + T^2 + \ldots + T^{p-1}$.

1. Vérifier que le polynôme p est irréductible sur $\mathbb{Q}$.
2. Donner la dimension du $\mathbb{Q}$-espace vectoriel $\mathcal{L}_{\mathbb{Q}}(P)$. Donner une base de cet espacce vectoriel.

Exercice 4.5.6 Soit $P \in k[T]$ un polynôme irréductible de degré d et soit $\phi_P : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ l'application rationnelle définie par les équations $\phi_P(x, y) = (y^d P(\frac{x}{y}), y^d)$

1. Montrer que ϕ_P est un morphisme et déterminer son degré.
2. Soit $Q \in \mathbb{P}^1$. Déterminer l'ensemble $\phi_P^{-1}(Q) = \{R \in \mathbb{P}^1 \mid \phi_P(R) = Q\}$.

Chapitre 5

Fonction zêta

Dans ce chapitre k désigne un corps fini.

5.1 Courbes projectives sur un corps fini

Soit C une courbe projective lisse définie sur $k = \mathbb{F}_q$. Parfois on notera aussi C_k au lieu de C s'il faut préciser le corps des constantes de la courbe C.

Proposition 5.1.1 *Soit $d_0 \in \mathbb{N}$. Il n'existe qu'un nombre fini de points fermés $P \in C$ avec $\deg P \leq d_0$.*

Démonstration. Choisissons une fonction rationnelle $\varphi \in k(C)^*$ et considérons le morphisme (défini sur k) associé

$$\pi_\varphi : C \longrightarrow \mathbb{P}^1.$$

Soit $Q \in C$ un point ayant un degré $\leq d_0$. Notons $P = \pi_\varphi(Q) \in \mathbb{P}^1$. Alors d'après le lemme **??** $\deg P \leq \deg Q \leq d_0$. On a vu dans ? ? ? que les points fermés de degré d de la droite projective $\mathbb{P}^1$ correspondent aux polynômes irréductibles de $k[t]$ de degré d (si l'on omet le point à l'infini !). Or comme k est fini, il n'y a qu'un nombre fini de polynômes de degré $\leq d_0$, et par conséquent il n'y a qu'un nombre fin de points fermés de degré $\leq d_0$. De plus d'après la proposition **??** il y a au plus $[k(C) : k(\varphi)]$ points Q qui dominent P. Ainsi il n'y a qu'un nombre fini de points Q de C de degré $\leq d_0$. ∎

Remarque.
Fixons un entier $d \in \mathbb{N}$. Il est immédiat de voir que le nombre de points $\mathbb{F}_{q^d}$-rationnels de C est fini. En effet l'ensemble $C(\mathbb{F}_{q^d})$ est contenu dans $\mathbb{P}^n(\mathbb{F}_{q^d})$, qui est fini. Voir la proposition 5.1.1 pour le calcul de $|\mathbb{P}^n(\mathbb{F}_{q^d})|$.

On renvoie à la section 4.2 pour la définition du groupe de Picard de C.

Proposition 5.1.2 *On a les assertions suivantes*

1. *La composante de degré 0 du groupe de Picard $\mathrm{Pic}^0(C)$ est un groupe abélien fini.*
2. *Les ensembles $\mathrm{Pic}^d(C)$, pour $d \in \mathbb{Z}$, sont finis et de même cardinal, noté $h(C)$.*

Démonstration. On va d'abord montrer que les ensembles $\mathrm{Pic}^d(C)$ sont finis si $d > g-1$. Considérons $\mathcal{D} \in \mathrm{Pic}^d(C)$. D'après le théorème de Riemann-Roch (Théorème 4.4.1) on a

$$l(\mathcal{D}) = l(K - \mathcal{D}) + d + 1 - g > 0.$$

Donc il existe un diviseur effectif $D \in \mathrm{Div}_+^d(C)$ qui est dans la classe $\mathcal{D}$. En écrivant

$$D = \sum_P n_P P \qquad \text{et} \qquad \deg D = \sum n_P \deg P$$

on constate que pour tout point fermé P du support de D on a l'inégalité évidente $\deg P \leq \deg D = d$. Comme il n'y a qu'un nombre fini de points $P \in C$ de degré $\leq d$, il n'y a qu'un nombre fini de diviseurs effectifs de degré $\leq d$. On en déduit que $\mathrm{Pic}^d(C)$ est fini.

Montrons maintenant que le cardinal de $\mathrm{Pic}^d(C)$ ne dépend pas de d. Rappelons que l'image de l'homomorphisme $\deg : \mathrm{Pic}(C) \to \mathbb{Z}$ est un sous-groupe $\delta\mathbb{Z} \subset \mathbb{Z}$ avec $\delta \in \mathbb{N}^*$. Considérons deux entiers $d_1, d_2 \in \delta\mathbb{Z}$ et choisissons $\mathcal{D}_1 \in \mathrm{Pic}^{d_1}(C)$ et $\mathcal{D}_2 \in \mathrm{Pic}^{d_2}(C)$. On vérifie alors facilement que l'application

$$\mathrm{Pic}^{d_1}(C) \longrightarrow \mathrm{Pic}^{d_2}(C), \qquad \mathcal{D} \mapsto \mathcal{D} + \mathcal{D}_2 - \mathcal{D}_1$$

est une bijection entre $\mathrm{Pic}^{d_1}(C)$ et $\mathrm{Pic}^{d_2}(C)$. ∎

On vient de montrer aussi la

Proposition 5.1.3 *Pour tout $d \in \mathbb{N}$ l'ensemble $\mathrm{Div}_+^d(C)$ est fini.*

Remarque.
Les ensembles $\mathrm{Pic}^d(C)$ pour $d \neq 0$ ne sont pas des sous-groupes de $\mathrm{Pic}(C)$. Cependant il existe pour tout $d \in \mathbb{Z}$ des bijections (qui sont non-canoniques)

$$\phi : \mathrm{Pic}^d(C) \xrightarrow{\cong} \mathrm{Pic}^0(C)$$

qui induisent une structure de groupe sur $\mathrm{Pic}^d(C)$. La bijection est en fait déterminée par le choix d'un élément $\mathcal{D} \in \mathrm{Pic}^d(C)$, qui est envoyé par ϕ sur la classe du diviseur nul.

Lemme 5.1.1 *Soit $D \in \mathrm{Div}(C)$. Le nombre de diviseurs effectifs linéairement équivalents à D est égal à*

$$\frac{q^{l(D)} - 1}{q - 1} = |\mathbb{P}^{l(D)-1}(\mathbb{F}_q)|.$$

Démonstration. Soit Δ un diviseur effectif linéairement équivalent à D. Alors $\Delta - D = \mathrm{div}\varphi$ avec $\varphi \in \mathcal{L}_k(D)$. Inversément soient $\varphi, \psi \in \mathcal{L}_k(D)$ tel que

$$\Delta = D + \mathrm{div}\varphi = D + \mathrm{div}\psi.$$

Alors $\mathrm{div}\varphi - \mathrm{div}\psi = 0$, ce qui implique $\mathrm{div}\frac{\varphi}{\psi} = 0$. D'après la proposition **??** cette relation entraine $\frac{\varphi}{\psi} \in k(C) \cap \overline{k} = k$. Il existe donc $c \in k$ tel que $\varphi = c\psi$. Ainsi l'ensemble des diviseurs effectifs linéairement équivalents à D est égal à l'ensemble des points de l'espace projectif $\mathbb{P}\mathcal{L}_k(D)$. Comme cet espace est de dimension $l(D) - 1$ on calcule aisément le nombre de points $\mathbb{F}_q$-rationnels. Voir aussi exercice **??**. ∎

5.2 Définition de la fonction zêta

Définition 5.2.1 *Soit C une courbe projective lisse défini sur le corps $k = \mathbb{F}_q$. La fonction zêta associée à la courbe $C_{\mathbb{F}_q}$ est la série formelle*

$$Z(C,t) = \sum_{D \in \mathrm{Div}_+(C)} t^{\deg D} \in \mathbb{Z}[[t]],$$

où D parcourt l'ensemble infini $\mathrm{Div}_+(C)$ des diviseurs effectifs sur C

De manière plus explicite on peut écrire

$$Z(C,t) = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + a_n t^n + \ldots$$

où $a_d = |\mathrm{Div}_+^d(C)|$ est égal au nombre de diviseurs effectifs de degré d sur C. D'après la proposition 5.1.3 ce nombre est fini. Comme il existe des diviseurs effectifs de degré arbitrairement grand, il y a un nombre infini de termes dans le développement de $Z(C,t)$.

Regardons d'abord les termes de petit degré de $Z(C,t)$. On notera $N_d = |C(F_{q^d})|$ pour tout $d \geq 1$ et l'on va exprimer les coefficients de la fonction zêta en fonction des entiers N_d.

- On a $a_1 = |\mathrm{Div}_+^1(C)| = |C(\mathbb{F}_q)| = N_1$. En effet un diviseur effectif de degré 1 est un point fermé de degré 1, donc un point $\mathbb{F}_q$-rationnel de C.
- Nous constatons qu'un diviseur effectif D de degré 2 sur C est de deux types différents
  1. $D = P$, où P désigne un point fermé de degré 2. Il y en a $\frac{N_2 - N_1}{2}$.
  2. $D = P_1 + P_2$, où P_1 et P_2 désignent des points fermés de degré 1, donc des points $\mathbb{F}_q$-rationnels de C. Il y en a $\frac{N_1(N_1+1)}{2}$.

  D'où la formule $a_2 = \frac{N_2 - N_1}{2} + \frac{N_1(N_1+1)}{2} = \frac{N_1^2 + N_2}{2}$.

Lemme 5.2.1 (produit eulerien) *On a l'égalité dans $\mathbb{Z}[[t]]$*

$$Z(C,t) = \sum_{D \in \mathrm{Div}_+(C)} t^{\deg D} = \prod_{P \in C} \frac{1}{1 - t^{\deg P}},$$

où P parcourt l'ensemble des points fermés de C.

Démonstration. Tout d'abord il faut donner un sens au produit infini $\mathbb{S} = \prod_{P \in C} \frac{1}{1 - t^{\deg P}}$. Fixons un entier $N \in \mathbb{N}$ et montrons que $\mathbb{S}$ détermine un élément $\mathbb{S}_N$ dans le quotient $\mathbb{Z}[[t]]/t^{N+1}\mathbb{Z}[[t]]$. Nous observons que ce quotient est l'ensemble des polynômes de degré $\leq N$. D'après la proposition 5.1.1 il n'existe qu'un nombre fini de points P avec $\deg P \leq N$. Ainsi le produit infini $\mathbb{S}$ se décompose

$$\prod_{P \in C} \frac{1}{1 - t^{\deg P}} = \prod_{\deg P \leq N} \frac{1}{1 - t^{\deg P}} \cdot \prod_{\deg P > N} \frac{1}{1 - t^{\deg P}}.$$

On remarque que le deuxième facteur est égal à 1 modulo $t^{N+1}\mathbb{Z}[[t]]$, ce qui implique que $\mathbb{S}_N := \mathbb{S}$ modulo $t^{N+1}\mathbb{Z}[[t]]$ est en fait un produit fini. En utilisant le développement en série formelle

$$\frac{1}{1 - t^{\deg P}} = 1 + t^{\deg P} + t^{2\deg P} + t^{3\deg P} + \cdots$$

on observe que le coefficient de t^d du polynôme $\mathbb{S}_N$, avec $d \leq N$, est égal à

$$a_d = |\{D = \sum n_P P \mid \deg P = d\}|.$$

Ainsi on a prouvé que

$$Z(C,t) = \mathbb{S}_N \mod t^{N+1}\mathbb{Z}[[t]].$$

Comme cette relation est vraie quelque soit $N \in \mathbb{N}$, on a prouvé le lemme. ∎

Proposition 5.2.1 *La fonction zêta $Z(C,t)$, considérée comme une série entière d'une variable complexe t, est absolument convergente sur le disque ouvert de rayon $t = \frac{1}{q}$.*

Démonstration. On peut écrire la fonction zêta sous la forme

$$Z(C,t) = \sum_{\substack{D \in \mathrm{Div}_+(C) \\ \deg D \leq 2g-2}} t^{\deg D} + \sum_{\substack{D \in \mathrm{Div}_+(C) \\ \deg D > 2g-2}} t^{\deg D}.$$

Le premier terme est un polynôme en t de degré $2g-2$. Pour les questions de convergence il est donc suffisant d'étudier le deuxième terme $Z'(C,t)$, qu'on peut encore écrire sous la forme

$$Z'(C,t) = \sum_{\substack{d \in \delta\mathbb{N} \\ d > 2g-2}} \sum_{\mathcal{D} \in \mathrm{Pic}^d(C)} \sum_D t^{\deg D},$$

où la dernière somme est prise sur tous les diviseurs effectifs D dans la classe $\mathcal{D} \in \mathrm{Pic}^d(C)$. D'après le corollaire **??** on a $l(D) = d+1-g$ pour tout diviseur D de degré $d > 2g-2$. Compte tenu de la proposition 5.1.2 et du lemme 5.1.1 on peut écrire

$$Z'(C,t) = h(C) \sum_{\substack{d \in \delta\mathbb{N} \\ d > 2g-2}} \frac{q^{d+1-g}-1}{q-1} t^d \tag{5.1}$$

$$= \frac{h(C)}{q-1} \left[q^{1-g} \sum_{\substack{d \in \delta\mathbb{N} \\ d > 2g-2}} (qt)^d - \sum_{\substack{d \in \delta\mathbb{N} \\ d > 2g-2}} t^d \right]. \tag{5.2}$$

Cette dernière expression montre immédiatement que $Z'(C,t)$ converge absolument sur le disque ouvert de rayon $\frac{1}{q}$. ∎

5.3 Analogie avec la fonction zêta de Riemann

On pose $t = q^{-s}$ et on introduit la fonction en la variable s

$$\zeta(C,s) = Z(C, q^{-s}).$$

Ainsi la proposition précédente montre que $\zeta(C,s)$ converge sur la région ouverte du plan complexe définie par l'équation $\Re(s) > 1$. On peut reformuler le produit eulerien

$$\zeta(C,s) = \prod_{P \in C} \frac{1}{1 - \frac{1}{N(P)^s}},$$

où $N(P) := q^{\deg(P)}$ désigne la norme du point fermé P. En particulier $N(P)$ est égal au nombre d'éléments du corps fini k_P.

Rappelons la définition de la fonction zêta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

et quelques-unes de ses propriétés

1. La série entière $\zeta(s)$ converge absolument pour $\Re(s) > 1$.
2. La fonction zêta de Riemann admet un prolongement analytique en une fonction méromorphe sur tout le plan complexe avec un pôle simple en $s = 1$.
3. La célèbre "hypothèse de Riemann" prédit que tous les zéros de ζ se trouvent sur la droite d'équation $\Re(s) = \frac{1}{2}$.
4. On a un produit eulerien
$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$
5. On a une équation fonctionnelle. On pose
$$f(s) = \frac{1}{\pi^{\frac{s}{2}}} \Gamma(\frac{s}{2}) \zeta(s),$$
où Γ désigne la fonction Gamma d'Euler. Alors on a l'équation suivante
$$f(s) = f(1 - s).$$

Une tentative d'explication de l'analogie entre $\zeta(s)$ et $\zeta(C, s)$

5.4 Rationalité de la fonction zêta

5.5 Fonction zêta et points $\mathbb{F}_{q^m}$-rationnels

5.6 Exercices

Chapitre 6

Corrigés des exercices

Exercice 4.5.4

1. On prend comme coordonnées homogènes x, y, z dans $\mathbb{P}^2$. L'équation homogène est

$$F : \qquad y^2z - (x - a_1z)(x - a_2z)(x - a_3z) = 0.$$

2. $P_\infty = [0, 1, 0]$. $\deg P_\infty = 1$.
3. Il faut montrer que le système d'équation

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

n'admet pas de solution. Cela est un calcul sans difficultés.

4. Le corps de fonctions $k(C)$ a deux descriptions.
(i) Appelons $C_{aff} \subset \mathbb{A}^2$ la courbe affine d'équation

$$f : \qquad y^2 - (x - a_1)(x - a_2)(x - a_3) = 0.$$

Alors $k(C)$ est le corps de fraction de l'anneau de coordonnées $A(C_{aff}) = k[x, y]/(f)$. Ainsi une fonction rationnelle $\varphi \in k(C)$ peut être représentée comme quotient $\varphi = \frac{\overline{a}}{\overline{b}}$ avec $a, b \in k[x, y]$ et $\overline{a}, \overline{b}$ désigne les classes de a, b modulo l'idéal (f).
(ii) On peut homogénéiser les deux polynômes a, b par rapport à la variable z et l'on peut écrire $\varphi = \frac{\overline{c}}{\overline{d}}$ où $c, d \in k[x, y, z]$ sont des polynômes homogènes de même degré.

Soit $M_i \subset A(C_{aff})$ l'idéal des fonctions qui s'annulent au point P_i. Alors $\mathcal{O}_{P_i}$ est par définition l'anneau localisé de $A(C_{aff})$ en l'idéal M_i. On sait que M_i est engendré par les deux fonctions $x - a_i$ et y. Comme on a la relation

$$y^2 = (x - a_1)(x - a_2)(x - a_3),$$

et comme les deux éléments $x - a_2$, $x - a_3$ sont inversibles dans $\mathcal{O}_{P_1}$ on obtient que l'idéal $(x - a_1)$ est égal (y^2). Donc y est une uniformisante de $\mathcal{O}_{P_1}$ et $\mathrm{ord}_{P_1}(x - a_1) = 2$. On a $\deg P_i = 1$.

5. On considère l'ouvert affine $\mathbb{A}^2_y \subset \mathbb{P}^2$ donné comme complémentaire de la droite projective d'équation $y = 0$. On a donc un morphisme d'inclusion donné par les équations $(x, z) \mapsto [x, 1, z]$. L'équation de la restriction de C à l'ouvert affine $\mathbb{A}^2_y$ est obtenu en posant $y = 1$:

$$z - (x - a_1 z)(x - a_2 z)(x - a_3 z) = 0.$$

Le point P_∞ a comme coordonnées affines $(0, 0)$. L'équation précédente peut se mettre sous la forme

$$z - (x^3 + \alpha x^2 z + \beta x z^2 + \gamma z^3) = 0.$$

ou bien de manière équivalente

$$z(1 - \alpha x^2 - \beta x z + \gamma z^2) = x^3.$$

On remarque que l'expression entre parenthèses n'est pas dans l'idéal maximal, donc est inversible. On a donc la relation $z = ux^3$ dans l'anneau local $\mathcal{O}_{P_\infty}$, avec $u \in \mathcal{O}_{P_\infty}$ inversible. L'uniformisante de $\mathcal{O}_{P_\infty}$ est x et $\mathrm{ord}_{P_\infty}(z) = 3$.

6. Montrons d'abord que $\mathrm{div}(y) = P_1 + P_2 + P_3 - 3P_\infty$. Comme l'uniformisante de l'anneau local $\mathcal{O}_{P_i}$ est y on a la relation $\mathrm{ord}_{P_i}(y) = 1$. D'autre part la fonction y sur $\mathbb{A}^2 \subset \mathbb{P}^2$ correpond à la fonction rationnelle $\frac{y}{z}$ sur $\mathbb{P}^2$. Sa restriction à l'ouvert affine $\mathbb{A}^2_y$ est égal à $\frac{1}{z}$. On a par conséquent $\mathrm{ord}_{P_\infty}(y) = \mathrm{ord}_{P_\infty}(\frac{1}{z}) = -3$. Il reste à voir qu'il n'y a pas de pôles en dehors des P_i et P_∞.

Bibliographie

[C] A. Chambert-Loir : Algèbre corporelle, Springer

[H] R. Hartshorne : Algebraic geometry, GTM 52, Springer, 1977

[La] S. Lang : Algebra, Addison Wesley, 1984

[L] Y. Laszlo : Théorie de Galois, disponible sur http ://www.math.polytechnique.fr/~laszlo/

[Mal] M.-P. Malliavin : Algèbre commutative, Masson, 1985

[Ma] B. Mazur : Arithmetic on curves, AMS Colloquium Lectures, Bull. AMS 14, No.2 (1986), 206-59

[Mi] J. Milne : Fields and Galois theory, disponible sur http ://www.jmilne.org/math/

[Mo] C. Moreno : Algebraic curves over finite fields, Cambridge Tracts in Mathematics 97 (1991), Cambridge University Press

[P] D. Perrin : Géométrie Algébrique, CNRS Edition 2001

[Si] J. H. Silverman : The Arithmetic of Elliptic Curves, GTM 106, Springer, 1985

[St] I. Stewart : Galois Theory, Chapman and Hall, 1991

[We] A. Weil : Number of solutions of equations in finite fields, Bull. AMS 55 (1949), 497-508