INTRODUCTION À L'ARITHMÉTIQUE DES COURBES ELLIPTIQUES
MASTER 2 – SORBONNE UNIVERSITÉ (2024)
FEUILLE DE TD 2

Soit k un corps. On rappelle qu'un corps de fonctions (d'une variable) sur k est une extension de corps $k \subset \mathrm{K}$ pour laquelle il existe $x \in \mathrm{K}$ transcendante sur k, telle que $k(x) \subset \mathrm{K}$ soit une extension (algébrique) finie.

Soit K un corps de fonctions sur k.

Exercice 1 (Propriétés des corps de fonctions)**.** On note κ la clôture algébrique de k dans K.

(1) Montrer que κ est une extension finie de k.

(2) Soit $y \in \mathrm{K} \setminus \kappa$. Montrer que l'extension $k(y) \subset \mathrm{K}$ est finie.

(3) Si l'on supppose de plus $p = \mathrm{car}(k) > 0$, montrer que $\mathrm{K}/k(y)$ est séparable si, et seulement si, y n'est pas une puissance $p$ième.

On appelle *point* P *de* K une valuation $v_{\mathrm{P}} : \mathrm{K} \to \mathbb{Z}$ qui est surjective. Pour P un point de K, on désignera par $\mathcal{O}_{\mathrm{P}} := \{x \in \mathrm{K} \mid v_{\mathrm{P}}(x) \geq 0\}$ l'anneau *des fonctions régulières en* P. C'est un anneau de valuation discrète d'idéal maximal $\mathfrak{m}_{\mathrm{P}} = \{x \in \mathrm{K} \mid v_{\mathrm{P}}(x) > 0\}$. On notera par $\deg \mathrm{P}$ l'entier $\dim_k(\mathcal{O}_{\mathrm{P}}/\mathfrak{m}_{\mathrm{P}})$.

(4) Montrer que $\deg \mathrm{P}$ est fini.

Solution: (1) Soit $k \subset \ell$ une extension finie, $l_1, \ldots, l_d$ une base. Alors le morphisme de $k[x]$-modules $\bigoplus_{i=1}^d k[x] \to \ell[x]$ qui envoie un d-uplet $(f_1(x), \ldots, f_d(x))$ vers $f_1(x)l_1 + \ldots + f_d(x)l_d$ est injective (on regarde les coefficients des polynômes !). On en déduit que l'application $\bigoplus_{i=1}^d k(x) \to \ell(x)$ de $k(x)$-espaces vectoriels est elle aussi injective (en virant les dénominateurs) et donc que $d \leq [\mathrm{K} : k(x)]$; autrement dit $[\ell : k] \leq [\mathrm{K} : k(x)]$. Soit ℓ une extension telle que le degré $[\ell : k]$ soit maximal : alors $\ell = \kappa$, car si $x \in \kappa$ on a $[\ell(x) : k] = [\ell(x) : \ell][\ell : k] \leq [\ell : k]$ soit $[\ell(x) : \ell] = 1$ puis $x \in \ell$. Ainsi $[\kappa : \ell] \leq [\mathrm{K} : k(x)]$.
(2) Par définition des corps de fonctions, y est algébrique sur $k(x)$: il existe un polynôme $g(\mathrm{X}, \mathrm{Y}) \in k[\mathrm{X}, \mathrm{Y}]$ tel que $g(x, y) = 0$. Comme y est transcendant sur k, $g(\mathrm{X}, \mathrm{Y}) \notin k[\mathrm{Y}]$. Ainsi, $k(y) \subset k(x, y)$ est finie. On a la tour d'extensions

$$k(y) \subset k(x, y) \subset \mathrm{K}$$

La seconde extension est aussi finie car $k(x) \subset k(x, y) \subset \mathrm{K}$ l'est.
(3) Si l'extension $\mathrm{K}/k(y)$ est inséparable, alors il y a une sous-extension $k(y) \subset \mathrm{L} \subset \mathrm{K}$ telle que $\mathrm{L} \subset \mathrm{K}$ est purement inséparable [1] de hauteur $k \geq 1$, et $k(y) \subset \mathrm{L}$ séparable. Puisque $\mathrm{K}^{p^k} \subset \mathrm{L}$, c'est en fait une égalité (comparer les degrés). Ainsi $k(y) \subset \mathrm{K}^p$. Réciproquement, si $y = x^p$, alors $k(y) \subset k(x) \subset \mathrm{K}$; la première extension étant purement inséparable, $\mathrm{K}/k(y)$ est inséparable.
(4) Soit $y \in \mathfrak{m}$ uniformisante. Comme y n'est pas algébrique sur k (voir *e.g.* Exercice 3.(1)), $[\mathrm{K} : k(y)]$ est fini. On prétend alors que $[\mathcal{O}/\mathfrak{m} : k] \leq [\mathrm{K} : k(y)]$. Pour le voir, soit $u_1, \ldots, u_m \in \mathcal{O}$ tels que $(\bar{u}_1, \ldots, \bar{u}_m)$ forme une base de $\mathcal{O}/\mathfrak{m}$ sur k. Alors $(u_1, \ldots, u_m)$ est linéairement indépendante sur $k(y)$; en effet, étant donnée une relation non triviale $f_1(y)u_1 + \ldots + f_m(y)u_m = 0$, on peut supposer $f_i(y)$ polynomial et non tous divisibles par y. En réduisant modulo $\mathfrak{m}$, on trouve une relation non triviale ce qui est une contradiction. Ainsi $m = [\mathcal{O}/\mathfrak{m} : k] \leq [\mathrm{K} : k(y)]$.

Exercice 2 (Le corps de fonctions $k(x)$)**.** Montrer qu'à un polynôme irréductible unitaire de $k[x]$ est associé un unique point de $k(x)$, et que presque tous les point de ce dernier sauf un peuvent se décrire ainsi.

Solution: Soit $\pi(x) \in k[x]$ un polynôme irréductible unitaire. On lui associe une valuation $v_\pi : k(x) \to \mathbb{Z}$ qui a chaque élément sous la forme $p(x)/q(x)$ lui associe $v_\pi(p(x)) - v_\pi(q(x))$. Comme $v_\pi(\pi) = 1$, cette valuation est surjective. Si, pour $\pi(x)$ et $\pi'(x)$ deux irréductibles distincts on a $v_\pi = v_{\pi'}$, alors il existe une relation de Bezout $a\pi + b\pi' = 1$ dans $k[x]$, et si v désigne la valuation correspondante à P, on aurait

$$0 = v(1) = v(a\pi + b\pi') \geq \min\{v(\pi), v(\pi')\} > 0$$

ce qui est absurde. On notera que la valuation $v_\infty = -\deg$ n'est pas atteinte de cette manière.

1. Une extension de corps L/K est dite *puremenent inséparable de hauteur* h si $x^{p^h} \in \mathrm{L}$ pour tout x dans L, et que h est minimal pour cette propriété.

Réciproquement, soit P un point de $k(x)$ et soit $v : k(x) \to \mathbb{Z}$ la valuation discrète sous-jacente. Il y a deux options : soit $v(k[x]) \geq 0$, soit il existe $f(x) \in k[x]$ avec $v(f(x)) < 0$.
Dans la première situation, il existe $p(x) \in k[x]$ tel que $v(p(x)) > 0$ (autrement, v serait constante égale à zéro sur $k(x)$ et donc pas discrète). Comme on le voit en décomposant $p(x)$ en produit d'irréductibles, il existe un polynôme irréductible $\pi(x)$ (divisant $p(x)$) tel que $v(\pi(x)) > 0$.
Dans la seconde situation, en écrivant $f(x) = a_d x^d + \ldots + a_0$ avec $a_i \in k$, on trouve $0 > v(f(x)) \geq \min\{v(x^d) | d \geq 0\}$ soit $v(x) < 0$ puis $v(x^{-1}) > 0$. De manière similaire, on trouve $v = v_\infty$.

- Le groupe des diviseurs de K est le groupe libre engendré par les points de K. On le note $\mathrm{Div_K}$. Un élément type de $\mathrm{Div_K}$ a la forme
$$\mathrm{D} = \sum_{\mathrm{P}} a(\mathrm{P})\mathrm{P}$$
où la somme porte sur les points P de K avec $a(\mathrm{P}) = 0$ sauf pour un ensemble fini de points.
- Le *degré de* D est l'entier $\deg \mathrm{P} := \sum_{\mathrm{P}} a(\mathrm{P}) \deg(\mathrm{P})$.
- On dit que D est *effectif* si $a(\mathrm{P}) \geq 0$ pour tout point P de K.

Exercice 3. Soit $a \in \mathrm{K}^\times$. On considère l'expression $(a) := \sum_{\mathrm{P}} \mathrm{ord_P}(a)\mathrm{P}$ où $\mathrm{ord_P}(a) = v_{\mathrm{P}}(a)$ avec v_{P} la valuation associée au point P.

(1) Montrer que $a \in \kappa^\times$ si, et seulement si, $\mathrm{ord_P}(a) = 0$ pour tout point de K. En déduire que si $a \in k^\times$, alors (a) est un diviseur.

(2) On suppose que $a \notin k^\times$. Montrer que la clôture intégrale de $k[a]$ dans K est un anneau de Dedekind. En déduire qu'il n'y a qu'un nombre fini de P tels que $\mathrm{ord_P}(a) > 0$ et que le diviseur effectif
$$(a)_+ := \sum_{\mathrm{P:\ ord_P}(a) \geq 0} \mathrm{ord_P}(a)\mathrm{P}$$
a pour degré $[\mathrm{K} : k(a)]$.

(3) En déduire que (a) est un diviseur de degré zéro.

Solution: (1) Soit $a \in \kappa^\times$ et P est un point de K de valuation v pour lequel $v(a) \neq 0$. Comme a est algébrique sur k, on trouve une relation du type $a^d = c_{d-1}a^{d-1} + \ldots + c_0$ à coefficients dans k où l'on peut supposer $c_0 \neq 0$. La somme de droite à des termes de valuations disctinctes, donc en prenant les valuations on trouve $dv(a) = \min\{0, (d-1)v(a)\}$; comme $v(a) \neq 0$, aucune de ces deux options n'est possible. Ainsi $v(a) = 0$. La réciproque découle de ce qui suit.
(2) Si $a \in \mathrm{K}^\times \setminus \kappa^\times$, alors l'extension $k(a) \subset \mathrm{K}$ est finie. Soit R la clôture intégrale de $k[a]$ dans K ; on sait que R est Dedekind, et en particulier on a une décomposition
$$\mathrm{R}a = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g}, \quad e_i > 0$$
en idéaux maximaux distincts de R. Si l'on note P_i le point correspondant à $v_{\mathfrak{P}_i}$ la valuation associée à $\mathfrak{P}_i$, alors on prétend que l'ensemble $\{\mathrm{P}_1, \ldots, \mathrm{P}_g\}$ est exactement l'ensemble des points de K tels que $\mathrm{ord_P}(a) > 0$. En effet, la localisation de l'égalité ci-dessus donne $\mathrm{ord_{P_i}}(a) = e_i$; réciproquement, si P est un point de K tel que $\mathrm{ord_P}(a) > 0$, alors $\{x \in \mathrm{K} | v_{\mathrm{P}}(x) > 0\} \cap \mathrm{R}$ définit un idéal maximal de R contenant a. Comme $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$ correspond à l'ensemble des idéaux maximaux de R contenant a, cela conclut.
Le théorème des reste Chinois donne
$$\mathrm{A}/a\mathrm{A} \cong \bigoplus_{i=1}^{g} \mathcal{O}_i/\mathfrak{P}_i^{e_i}$$
puis, en prenant les dimensions (et en appliquant les mêmes arguments qu'en théorie algébrique des nombres), on trouve $[\mathrm{K} : k(a)] = \sum_{i=1}^{g} \mathrm{ord_{P_i}}(a) \deg(\mathrm{P}_i)$. Ainsi, $(a)_+$ est un diviseur de degré $[\mathrm{K} : k(a)]$.
(3) On pose $(a)_- := \sum_{\mathrm{P:\ ord_P}(a) < 0} \mathrm{ord_P}(a)\mathrm{P}$ de sorte que $(a) = (a)_+ - (a)_-$. En appliquant le même raisonnement, cette fois-ci avec a^{-1}, on obtient que $(a)_-$ est un diviseur de degré $[\mathrm{K} : k(a^{-1})] = [\mathrm{K} : k(a)]$ et donc que (a) est un diviseur de degré zéro.

- On appelle un diviseur *principal* s'il est de la forme (a) pour un certain $a \in \mathrm{K}^\times$. Le sous-groupe de $\mathrm{Div_K}$ qu'ils forment est noté $\mathrm{Prin_K}$.
- On appelle groupe de classe et l'on note [2] $\mathrm{Cl_K}$ le groupe quotient $\mathrm{Div_K}/\mathrm{Prin_K}$.
- En particulier, $\deg : \mathrm{Div_K} \to \mathbb{Z}$ se factorise par $\mathrm{Cl_K}$, et on note $\mathrm{Cl_K^0}$ son noyau.

Exercice 4. Démontrer que $\mathrm{Cl}_{k(x)}$ est isomorphe à $\mathbb{Z}$.

2. Si $\mathrm{K} = k(\mathrm{C})$ pour C une courbe lisse sur k, on note également ce groupe $\mathrm{Pic(C)}$.

Solution: On cherche à montrer que l'application deg est un isomorphisme. Pour la surjectivité, il suffit de montrer qu'il existe un diviseur de degré 1 : n'importe quel diviseur de la forme P où $\mathrm{P} = \mathrm{P}_\pi$ avec $\pi(x)$ un polynôme de degré fait l'affaire. Pour l'injectivité, il reste à montrer qu'un diviseur de degré zéro est principal : soit donc $\mathrm{D} = \sum_{\mathrm{P}} a(\mathrm{P})\mathrm{P}$ un diviseur de degré zéro. On considère l'élément

$$f(x) := \prod_{\pi \text{ unit. irr.}} \pi(x)^{a(\mathrm{P}_\pi)}$$

où le produit est pris sur les polynômes irréductibles unitaires de $k[x]$. Comme on a l'égalité $(\pi) = \mathrm{P}_\pi - (\deg \pi)\mathrm{P}_\infty$ dans Div_K (les notations suivent la bijection de l'Exercice (2)), on trouve

$$(f) = \sum_{\pi \text{ unit. irr.}} a(\mathrm{P}_\pi)\mathrm{P}_\pi - \left(\sum_{\pi \text{ unit. irr.}} a(\mathrm{P}_\pi) \deg \pi \right) \cdot \mathrm{P}_\infty.$$

Comme $\deg \mathrm{D} = 0$, on trouve $a(\mathrm{P}_\infty) = -\sum_{\pi \text{ unit. irr.}} a(\mathrm{P}_\pi) \deg \pi$, ce qui montre que $\mathrm{D} = (f)$.

Soit L/K une extension finie de corps de fonctions sur k. Si $\mathfrak{P}$ est un point de L, alors $v_\mathfrak{P}|_\mathrm{K}$ définit une valuation sur K qui, cependant, peut ne pas être surjective. Á la place, son image est un idéal de $\mathbb{Z}$ et donc de la forme $e\mathbb{Z}$ pour un unique entier positif e. Soit P le point de K donné par $e^{-1} \cdot v_\mathfrak{P}|_\mathrm{K}$: on dit que P est le point de K *au-dessous de* $\mathfrak{P}$ (resp. $\mathfrak{P}$ est *au-dessus de* P) et on pose $e = e(\mathfrak{P}|\mathrm{P})$ qu'on appelle *indice de ramification*. Le *degré d'inertie*, noté $f(\mathfrak{P}|\mathrm{P})$, est l'entier $[\mathcal{O}_\mathfrak{P}/\mathfrak{m}_\mathfrak{P} : \mathcal{O}_\mathrm{P}/\mathfrak{m}_\mathrm{P}]$ ($\mathcal{O}_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}$ est bien un espace vectoriel sur $\mathcal{O}_\mathrm{P}/\mathfrak{m}_\mathrm{P}$). En suivant la méthode de l'Exercice (3), on montrerait qu'il n'y a qu'un nombre fini de points de L au-dessus de P, et

$$[\mathrm{L} : \mathrm{K}] = \sum_{\mathfrak{P}|\mathrm{P}} f(\mathfrak{P}|\mathrm{P}) e(\mathfrak{P}|\mathrm{P}).$$

En particulier, on peut définir deux morphismes de groupes :

$$\phi_* : \mathrm{Div}_\mathrm{L} \longrightarrow \mathrm{Div}_\mathrm{K}, \quad \mathfrak{P} \longmapsto \mathrm{P}, \quad \phi^* : \mathrm{Div}_\mathrm{K} \longrightarrow \mathrm{Div}_\mathrm{L}, \quad \mathrm{P} \longmapsto \sum_{\mathfrak{P}|\mathrm{P}} e(\mathfrak{P}|\mathrm{P})\mathfrak{P}$$

Exercice 5. Montrer les propriétés suivantes :

(1) Pour $\mathrm{D} \in \mathrm{Div}_\mathrm{K}$, $\deg(\phi^*\mathrm{D}) = [\mathrm{L} : \mathrm{K}](\deg \mathrm{D})$.

(2) Pour $\mathrm{D} \in \mathrm{Div}_\mathrm{L}$, $\deg(\phi_*\mathrm{D}) = \deg \mathrm{D}$.

(3) Pour $f \in \mathrm{K}^\times$, $\phi^*((f)) = (f)$; en déduire que ϕ^* induit un morphisme $\mathrm{Cl}_\mathrm{K} \to \mathrm{Cl}_\mathrm{L}$.

(4) Pour $f \in \mathrm{K}^\times$, $\phi_*((f)) = (f)$; en déduire que ϕ_* induit un morphisme $\mathrm{Cl}_\mathrm{L} \to \mathrm{Cl}_\mathrm{K}$.

(5) La composition $\phi_* \circ \phi^* : \mathrm{Div}_\mathrm{K} \to \mathrm{Div}_\mathrm{L}$ coincide à la multiplication par $[\mathrm{L} : \mathrm{K}]$.