

ACCQ 205 - Courbes algébriques

1 Corps et extensions de corps

Anneaux, algèbres, corps, idéaux premiers et maximaux et corps des fractions

On considère les anneaux commutatifs sauf précision contraire.

Def. Soit k un anneau. Une k -**algèbre** (commutative) est un anneau A muni d'un morphisme d'anneaux $\varphi_A: k \rightarrow A$, appelé **morphisme structural** de l'algèbre, dont l'image est contenue dans le centre de A .

Formellement une k -algèbre est le couple (A, φ_A) mais on le réduit souvent à la donnée de φ_A . De façon équivalente une k -algèbre est un k -module qui est muni d'une multiplication k -bilinéaire qui en fait un anneau.

Def. Un **morphisme de k -algèbres** est un morphisme d'anneaux $\psi: A \rightarrow B$ tel que $\varphi_B = \psi \circ \varphi_A$. Ce sont aussi les applications k linéaires qui préservent la multiplication.

Rem. Une \mathbf{Z} -algèbre est exactement la même chose qu'un anneau.

En pratique k est généralement un corps et A est donc un k -ev muni d'une multiplication k -bilinéaire qui en fait un anneau.

Def. Un élément a d'un anneau A est dit **régulier** si $x \mapsto ax$ est injectif, i.e. $ax = 0 \implies x = 0$ (il est inversible si bijectivité de l'application). A est dit **intègre** si tous les éléments sauf 0 sont réguliers, i.e. $0 \neq 1$ et $\forall a, b \in A \setminus \{0\}, ab = 0 \implies a = 0$ ou $b = 0$. Par convention l'anneau nul n'est pas intègre.

Def. Un idéal \mathfrak{p} d'un anneau A est dit **premier** lorsque l'anneau quotient A/\mathfrak{p} est intègre, i.e. $\mathfrak{p} \neq A$ et $\forall a, b \in A, ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

Prop. Dans un anneau A , l'ensemble A^\times des inversibles est un groupe, aussi appelé groupe des **unités de A** .

Def. Un **corps** est un anneau k dans lequel $k^\times = k \setminus \{0\}$. C'est équivalent à dire que k a deux idéaux qui sont $\{0\}$ et lui-même. C'est en particulier un anneau intègre. Par convention l'anneau nul n'est pas un corps.

Def. Un idéal \mathfrak{m} d'un anneau A est dit **maximal** si A/\mathfrak{m} est un corps. De façon équivalente $\mathfrak{m} \neq A$ et \mathfrak{m} est maximal pour l'inclusion parmi les idéaux différents de A .

Prop. Un idéal maximal est premier.

Ex. Dans un anneau factoriel A , un idéal de la forme (f) avec $f \in A$ est premier ssi f est nul ou irréductible.

Lem (Principe maximal de Hausdorff). Soit $\mathcal{F} \subset \mathcal{P}(A)$ non vide et tel que, pour tout partie $\mathcal{I} \subset \mathcal{F}$ non vide totalement ordonnée par l'inclusion, $\exists F \in \mathcal{F}, \bigcup_{I \in \mathcal{I}} I \subset F$. Alors il existe $M \in \mathcal{F}$ maximal pour l'inclusion.

Prop. Dans un anneau A , tout idéal strict (autre que A) est inclus dans un idéal maximal.

Def. Un élément x d'un anneau A est dit **nilpotent** lorsque $\exists n \in \mathbf{N}, x^n = 0$. Si 0 est le seul élément nilpotent, A est dit réduit.

Prop. Dans un anneau, l'ensemble des éléments nilpotents est un idéal appelé **nilradical** de l'anneau. C'est aussi l'intersection des idéaux premiers de l'anneaux. Le quotient de l'anneau par son nilradical est réduit.

Def. Soit A un anneau intègre. On définit le **corps des fractions** de A , $\text{Frac}(A) = \left\{ \frac{a}{q} \mid a \in A, q \in A \setminus \{0\} \right\}$ en convenant d'identifier $\frac{a}{q}$ avec $\frac{a'}{q'}$ lorsque $aq' = a'q$.

Prop. Soit A un anneau intègre, K un corps et $\varphi: A \rightarrow K$ un morphisme d'anneau injectif. Alors il existe un unique morphisme de corps $\hat{\varphi}: \text{Frac}(A) \rightarrow K$ qui prolonge φ et il est donné par $\hat{\varphi}\left(\frac{a}{q}\right) = \frac{\varphi(a)}{\varphi(q)}$.

Def. Le corps des fractions de l'anneau des polynômes $k[t_1, \dots, t_n]$ est appelé corps des **fractions rationnelles** et noté $k(t_1, \dots, t_n)$.

Prop. Soit k un corps et K une k -algèbre de dimension finie intègre. Alors K est un corps.

Lem (de Gauß). Soit A un anneau factoriel et K son corps des fractions. Alors :

- (i) $A[t]$ est factoriel,
- (ii) $f \in A[t]$ est irréductible ssi f est constant et irréductible dans A , ou bien f est primitif, i.e. irréductible dans $K[t]$ et le pgcd dans A de ses coefficients vaut 1.

Algèbres engendrée, extensions de corps

2 Le Nullstellensatz et les fermés de Zariski

Anneaux nothérien

Def. Un idéal I d'un anneau A est de **type fini** s'il est engendré par un nombre fini d'éléments (équivalent à être de type fini en tant que sous-module de A).

Def. Un anneau A est dit **noethérien** lorsque tout idéal I de A est de type fini.

Rem. Un quotient d'un anneau noethérien est noethérien.

Th (de la base de Hilbert). Si A est un anneau noethérien, alors l'anneau $A[t]$ des polynômes à une indéterminée sur A est noethérien.

Cor. Soit k un corps ou un anneau noethérien. Alors l'anneau $k[t_1, \dots, t_n]$ des polynômes en n indéterminées sur k est un anneau noethérien, et plus généralement toute k -algèbre de type fini (comme k -algèbre) $k[x_1, \dots, x_n]$ est un anneau noethérien.

Idéaux maximaux d'anneaux de polynômes

Lem. Soit k un corps algébriquement clos et K une extension. On suppose que $h_1, \dots, h_m \in k[t_1, \dots, t_n]$ ont un zéro commun dans K (i.e $\exists z_1, \dots, z_n \in K, \forall i, h_i(z_1, \dots, z_n) = 0$). Alors ils en ont un dans k .

Not. Soit k un corps et $(x_1, \dots, x_n) \in k^n$. On note

$$\mathfrak{m}_{(x_1, \dots, x_n)} := \{f \in k[t_1, \dots, t_n] \mid f(x_1, \dots, x_n) = 0\} = (t_1 - x_1, \dots, t_n - x_n).$$

Prop. Soit k un corps algébriquement clos. Les idéaux maximaux de $k[t_1, \dots, t_n]$ sont exactement les idéaux $\mathfrak{m}_{(x_1, \dots, x_n)}$.

Prop (lemme de Zariski). Soit k un corps et K une extension de type fini comme k -algèbre. Alors k est en fait une extension finie.

Le Nullstellensatz

Prop (Nullstellensatz faible). Soient $h_1, \dots, h_m \in k[t_1, \dots, t_n]$ avec k algébriquement clos. Si h_1, \dots, h_m n'engendrent pas l'idéal unité, alors ils ont un zéro commun dans k : $\exists x_1, \dots, x_n \in k, \forall i, h_i(x_1, \dots, x_n) = 0$.

Prop (Nullstellensatz fort). Soient $g, h_1, \dots, h_m \in k[t_1, \dots, t_n]$ avec k algébriquement clos. Si g s'annule sur tous les zéros communs de h_1, \dots, h_m alors $\exists l \in \mathbb{N}, g^l \in (h_1, \dots, h_m)$ (idéal engendré).

Fermés de Zariski

Def. Un idéal \mathfrak{r} d'un anneau A est dit **radical** lorsque A/\mathfrak{r} est réduit, i.e $\forall x \in A, \forall n \in \mathbb{N}, x^n \in \mathfrak{r} \implies x \in \mathfrak{r}$.

Un idéal premier, et a fortiori un idéal maximal, est en particulier un idéal radical.

Dans ce qui suit on note k un corps et k^{alg} une clôture algébrique.

Not. Soit $\mathcal{F} \subset k[t_1, \dots, t_n]$. On pose $Z(\mathcal{F}) := \{(x_1, \dots, x_d) \in (k^{\text{alg}})^d \mid \forall f \in \mathcal{F}, f(x_1, \dots, x_d) = 0\}$.

Def. On appelle **fermé de Zariski** tout ensemble de la forme $Z(\mathcal{F})$.

Rem. Z est décroissante pour l'inclusion et on peut toujours supposer que \mathcal{F} est un idéal radical.

Def. Un fermé de Zariski de la forme $Z(f) = Z(\{f\})$ est appelé une **hypersurface**.

Rem. Le vide, $(k^{\text{alg}})^d$ et les singletons sont des fermés de Zariski.

Not. Soit $E \subset (k^{\text{alg}})^d$. On pose $J(E) := \{f \in k[t_1, \dots, t_n] \mid \forall (x_1, \dots, x_d) \in E, f(x_1, \dots, x_d) = 0\}$.

Rem. $J(E)$ est un idéal radical, J est décroissant pour l'inclusion et $J(E) = \bigcap_{x \in E} \mathfrak{m}_x$ où $\mathfrak{m}_x = J(\{x\})$.

3 Corps de courbes algébriques

Définitions

Def. Soit k un corps. Un **corps de fonctions** K de dimension n sur k est une extension de corps de k de type fini et de degré de transcendance n sur k . Pour $n = 1$ on parle de **corps de fonctions de courbe** sur k .

Par abus de langage on dit que K est une courbe (algébrique) sur k .

Def. **Droite projective** sur k , notée \mathbb{P}_k^1 ou \mathbb{P}^1 : courbe simple donnée par $k(t)$ le corps des fractions rationnelles.

...

Anneaux de valuation

Def. Soit K un corps. Un **anneau de valuation** de K est un sous-anneau R de K vérifiant $\forall x \in K, x \in R$ ou $x^{-1} \in R$. Il est dit non-trivial si $R \neq K$. Lorsque $k \subset R$ est un sous-corps de K , on dit que R est un anneau de valuation au-dessus de k .

Rem. R est intègre et $K = \text{Frac}(R) \rightarrow$ on parle d'anneau de valuation dans l'absolu pour un anneau de valuation de son corps des fractions.

Def. Soit $x, y \in K$. On dit que :

- x est *plus valué* que y si $\exists z \in R, x = yz$,
- x et y ont la *même valuation* si $\exists z \in R^\times, x = yz$.

Ceci définit une relation d'équivalence dont les classes sont appelées **valuations** et notées $v_R(x)$ ou $v(x)$. On note $v(0) = \infty$ mais cette classe est mise à part et on ne considère généralement pas qu'il s'agisse d'une valuation.

Rem. On a défini une relation d'ordre total sur les valuations (plus ∞ qui est le plus grand élément).

Not. On définit $v(x) + v(y) = v(xy)$ et $\forall c \in R^\times, v(c) = v(1) = 0$.

Def. Soit $\Gamma := K^\times / R^\times$ l'ensemble des valuations. Le groupe abélien $(\Gamma, +)$ est appelé **groupe des valuations** (ou des **valeurs**) de R .

Def. Si $\Gamma = \mathbb{Z}$, i.e. est engendré par un unique élément, on dira que R est un anneau de valuation **discrète**.

Prop. Soit R un anneau de valuation de K . On a :

- (i) $v(x) = \infty \iff x = 0$
- (ii) $v(xy) = v(x) + v(y)$
- (iii) $v(x + y) \geq \min\{v(x), v(y)\}$
- (iv) $v(x + y) = \min\{v(x), v(y)\}$ si $v(x) = v(y)$

De plus $v(K^\times) = \Gamma$ et $R = \{x \in K \mid v(x) \geq 0\}$.

Ex. Soit $K = k(t)$ et h un polynôme unitaire irréductible sur k . On pose, pour $f \in k[t]$, $v_h(f)$ est l'exposant de la plus grande puissance de h qui divise f . Si $g \in k[t] \setminus \{0\}$, $v_h\left(\frac{f}{g}\right) = v_h(f) - v_h(g)$. Alors v_h vérifie les conditions ci-dessus et atteint 1 en h . De plus R est l'ensemble des fractions rationnelles sans h facteur du dénominateur.

Ex. Soit p premier et $K = \mathbb{Q}$. Pour $m \in \mathbb{Z}$, on pose $v_p(m)$ la valuation p -adique de m , i.e. l'exposant de la plus grande puissance de p qui divise m . Si $\frac{n}{m} \in \mathbb{Q}$, $v_p\left(\frac{n}{m}\right) = v_p(n) - v_p(m)$. Alors v_p vérifie les conditions ci-dessus et atteint 1 en p . De plus R est l'ensemble des rationnels dont le dénominateur réduit n'est pas multiple de p .

Rem. Si A est un anneau intègre et $v: A \rightarrow \mathbb{Z} \cup \{\infty\}$ vérifie (i), (ii) et (iii) alors il existe une unique fonction $v: \text{Frac}(A) \rightarrow \mathbb{Z} \cup \{\infty\}$ qui prolonge le v donné sous les mêmes conditions, à savoir $v: \frac{x}{y} \mapsto v(x) - v(y)$ où $y \neq 0$. Si, de plus, v est positive sur A alors $A \subset R$ ou R est l'anneau de la valuation.

Def. Un anneau R est dit **local** s'il vérifie l'une des propriétés équivalentes suivantes :

- (i) R a un unique idéal maximal,
- (ii) le complémentaire de R^\times dans R est un idéal (forcément maximal),
- (iii) pour tout $x \in R$, soit x est inversible, soit $1 - cx$ est inversible pour tout $c \in R$.

Prop. Un anneau de valuation est un anneau local. Son idéal maximal est $\mathfrak{m}_v = \{x \in R \mid v(x) > 0\}$.

Def. On note parfois \mathcal{O}_v l'anneau de valuation associé à la valuation v . Le corps $\kappa_v = \mathcal{O}_v / \mathfrak{m}_v$ s'appelle **corps résiduel** de la valuation v .

Prop. Si v est une valuation au-dessus de k (corps de base) alors κ_v est une extension de k . Son degré (s'il est fini) s'appellera degré sur k de la valuation v .

Def. Soit K un corps de fonction de courbe sur k . Une valuation non triviale au-dessus de k sur un corps K de fonctions de k s'appelle une **place** de K (ou de la courbe C telle que $K = k(C)$). On note $\mathcal{V}_{K/k}$ ou \mathcal{V}_C l'ensemble de ces places.

Prop. Soit K un corps, $A \subset K$ un sous-anneau et \mathfrak{p} un idéal premier de A . Alors il existe un anneau de valuation R de K tel que $A \subset R \subset K$ et $\mathfrak{m} \cap A = \mathfrak{p}$ où \mathfrak{m} est l'idéal maximal de R .

Cette proposition sert à construire des valuations "centrées" sur un idéal premier \mathfrak{p} qu'on s'est donné.

Prop. Soit K un corps et $A \subset K$ un sous-anneau. Alors $B := \bigcap_{A \subset R \subset K} R$ (avec R anneau de valuation de K) est exactement l'ensemble des $x \in K$ entiers (algébriques) sur A au sens où il existe $f \in A[t]$ unitaire, non constant, à coefficients dans A tels que $f(x) = 0$. B est donc un sous-anneau de K et s'appelle **fermeture intégrale** de A dans K , ou **clôture intégrale** lorsque $K = \text{Frac}(A)$. En particulier, si k est un sous-corps de K alors B est la fermeture algébrique de k dans K .

Prop. Soit \mathcal{O}_v un anneau de valuation discrète de valuation v . Un élément $t \in \mathcal{O}_v$ engendre \mathfrak{m} en tant qu'idéal si et seulement si $v(t) = 1$. Il est appelé **uniformisante** de \mathcal{O}_v et pour un tel t fixé (il en existe) :

- tout $x \neq 0$ de K a une représentation unique sous la forme $x = ut^r$ avec $u \in \mathcal{O}_v^\times$ et $r \in \mathbb{Z}$, avec $r = v(x)$,
- tout idéal $I \neq \{0\}$ de \mathcal{O}_v est l'idéal $\mathfrak{m}^r = \{x \in \mathcal{O}_v \mid v(x) \geq r\}$ engendré par t^r pour un certain $r \in \mathbb{N}$.

Places des courbes

Lem. Soit K un corps de fonctions de courbes sur k et v une valuation de K au-dessus de k . Alors :

- (i) Si x vérifie $v(x) \neq 0$ et $v(x) < \infty$ alors x est transcendant sur k et le corps K est fini sur $k(x)$.
- (ii) Si x_1, \dots, x_n vérifient $0 < v(x_1) < v(x_2) < \dots < v(x_n) < \infty$, alors x_1, \dots, x_n sont linéairement indépendants sur $k(x_n)$, et en particulier le degré $[K : k(x_n)]$ (fini) est supérieur ou égal à n .
- (iii) Si x vérifie $0 < v(x) < \infty$ alors $[\kappa_v : k] \leq [K : k(x)]$.

Prop. Soit K un corps de fonctions de courbe sur k . Alors toutes les places de K sont discrètes.

Dans ce cas κ_v est une extension finie, donc algébrique, de k . Le degré $[\kappa_v : k]$ s'appelle aussi degré de la place v . S'il vaut 1, i.e. $\kappa_v = k$, v est dite rationnelle. C'est notamment le cas si v est algébriquement clos.

Def. Soit K un corps de fonctions de courbe sur k . Si $f \in K$ et $v \in \mathcal{V}_K$ on peut définir l'évaluation de f en v

$$f(v) \in \kappa_v, \quad f(v) = \begin{cases} \text{la classe de } f \in \mathcal{O}_v \text{ modulo } \mathfrak{m}_v \text{ lorsque } v(f) \geq 0 \\ \text{le symbole spécial } \infty \text{ (pas celui de } v(0)) \text{ lorsque } v(f) < 0 \end{cases}$$

Dans le cas $f(v) = \infty$ on dit que f a un **pôle** en v . On a trois possibilités exclusives :

$$\begin{aligned} v(f) > 0 &\iff f(v) = 0 \iff f \in \mathfrak{m}_v && f \text{ a un zéro en } v \\ v(f) < 0 &\iff f(v) = \infty \iff f \notin \mathcal{O}_v && f \text{ a un pôle en } v \\ v(f) = 0 &\iff f(v) \in \kappa_v^\times \iff f \in \mathcal{O}_v^\times \end{aligned}$$

$v(f)$ est appelé multiplicité du zéro de f en v , et $-v(f)$ multiplicité du pôle. Si $v(f) = 1$, f est appelé **paramètre local** pour K en v (comme uniformisante).

Prop. La fermeture algébrique \tilde{k} de k dans K peut s'appeler **corps des constantes** et coïncide avec $\{f \in K \mid \forall v \in \mathcal{V}_K, v(f) = 0\}$, ces fonctions f étant dites **constantes**. On a alors l'équivalence suivante :

$$\begin{aligned} f \text{ n'est pas constante} &\iff f \text{ est transcendante} &\iff \exists v \in \mathcal{V}_K \text{ où } f \text{ ait un pôle} \\ &\iff f \text{ n'est pas nulle et } \exists v \in \mathcal{V}_K \text{ où } f \text{ ait un zéro} \end{aligned}$$

Rem. Tous les corps résiduels κ_v sont des extensions de \tilde{k} . Notamment $[\tilde{k} : k]$ divise tous les $\deg(v) = [\kappa_v : k]$ et, en particulier, s'il existe une place **rationnelle**, i.e. telle que $\deg(v) = 1$, ou simplement deux places de degrés premiers entre eux, on a $\tilde{k} = k$.

Les places de la droite projective

Soit $h \in k[t]$ unitaire et irréductible, $v_h(f)$ pour $f \in k[t]$ l'exposant de h dans la décomposition de f en polynômes irréductibles et $\forall f, g \in k[t], v_h\left(\frac{f}{g}\right) = v_h(f) - v_h(g)$.

Prop. Le corps résiduel κ_h de la place v_h est le corps de rupture $k[t]/(h)$ de h sur k .

Rem. La valeur de f en la place v_ξ , définie comme v_h où $h = t - \xi, \xi \in k^{\text{alg}}$, peut s'identifier à la valeur $f(\xi)$ dans le corps $k(\xi) = k[t]/(h)$.

Rem. Une autre valuation non-triviale de $k(t)$ au-dessus de k est $v_\infty : \frac{f}{g} \mapsto \deg(g) - \deg(f)$.

Prop. Soit k un corps. Alors les places du corps $k(t)$ sont exactement les places v_h , et v_∞ .

L'indépendance des valuations

L'identité du degré

Diviseurs sur les courbes

Espaces de Riemann-Roch

Différentielles de Kähler

Théorème de Riemann-Roch

Points et places

Revêtements de courbes