

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

Def. Soit A une k -algèbre et $(x_i)_{i \in I}$ famille de A . La k -**algèbre engendrée** $k[x_i]_{i \in I}$ dans A par les x_i est l'intersection de toutes les sous- k -algèbres de A contenant les x_i . C'est la plus petite sous- k -algèbre contenant les x_i . Elle est dite **de type fini** si I est fini.

On peut aussi décrire $k[x_i]_{i \in I}$ comme l'ensemble de tous les éléments de A qui peuvent être obtenus à partir de 1 et des x_i par les opérations \times, \cdot et $+$.

Def. Une **extension de corps** est un morphisme d'anneaux $k \rightarrow K$ entre corps (K est une k -algèbre qui est un corps). On note $k \subseteq K$ ou K/k et l'on dit que k est un **sous-corps** de K .

Def. Soit $k \subseteq K$ une extension de corps et $(x_i)_{i \in I}$ une famille de K . La **sous-extension engendrée** (dans K) par les x_i , notée $k(x_i)_{i \in I}$, est l'intersection de tous les sous-corps de K contenant k et les x_i . C'est le plus petit corps intermédiaire contenant les x_i . Elle est dite **de type fini** si I est fini.

Ce sont les valeurs des fractions rationnelles à coefficients dans k évaluées en des x_i .

Prop. Une sous-extension d'une extension de corps de type fini est de type fini. Mais une sous-algèbre d'une algèbre de type fini n'est pas, en général, de type fini !

Extension algébrique et degré

Def. Soit $k \subseteq K$ est une extension et $x \in K$. L'extension $k \subseteq k(x)$ est dite **monogène**.

Avec ce x , on définit $\varphi: \begin{matrix} k[t] & \rightarrow & K \\ P & \mapsto & P(x) \end{matrix}$ le morphisme d'évaluation, le seul à envoyer l'indéterminée t sur x .

Alors $\text{Ker}(\varphi)$ est un idéal de $k[t]$ et l'on est dans l'un des deux cas suivants :

- φ est injectif, x est **transcendant** sur k , φ se prolonge de manière unique en une extension de corps $k(t) \rightarrow K$, et l'image de $k(t)$ (corps des fractions rationnelles) est $k(x)$ (extension).
- ou $\text{Ker}(\varphi)$ est engendré par $\mu_x \in k[t]$ unitaire, appelé **polynôme minimal** de x et x est dit **algébrique**. Alors $\varphi(k[t])$ s'identifie à la k -algèbre $k[t]/(\mu_x)$ de dimension $\deg(\mu_x)$, appelé **degré** de x .

Rem. Les algébriques de degré 1 sur k sont exactement les éléments de k .

Rem. Si $k \subseteq k' \subseteq K$, le polynôme minimal d'un $x \in K$ sur k' divise celui sur k .

Def. Soit $\mu \in k[t]$ unitaire irréductible. Le **corps de rupture** de μ sur k est $k[t]/(\mu)$.

Def. Une extension de corps $k \subseteq K$ est dite **algébrique** (« au-dessus » de k , ou « sur » k) lorsque chaque élément de K est algébrique sur k .

Def. Un corps k est **algébriquement clos** si sa seule extension algébrique est lui-même. Cela revient à dire que les seuls polynômes unitaires irréductibles dans $k[t]$ sont les $t - a$.

Def. Soit $k \subseteq K$ une extension de corps. Considérant K comme un k -ev, sa dimension (finie ou infinie) est notée $[K : k]$ et appelée **degré** de l'extension. Une extension de degré fini est dite **finie**.

Prop. L'extension monogène $k \subseteq k(x)$ est finie si et seulement si x est algébrique sur k , et dans ce cas $k(x) \simeq k[t]/(\mu_x)$ et $[k(x) : k] = \deg(\mu_x) = \deg(x)$.

Prop. Soit $k \subseteq K \subseteq L$ deux extensions imbriquées. Alors $[L : k] = [K : k][L : K]$.

Cor.

- Une extension $k \subseteq k(x_1, \dots, x_n)$, $n \in \mathbb{N}$ avec x_1, \dots, x_n algébriques est finie et a une base comme k -ev formée de monômes en les x_1, \dots, x_n (i.e. de la forme $x_1^{r_1} \cdots x_n^{r_n}$).
- Une extension est finie si et seulement si elle est à la fois algébrique et de type fini.
- Une extension de corps engendrée par une famille quelconque d'éléments algébriques est algébrique. Donc les sommes, différences, produits et inverses de quantités algébriques sur k le sont aussi.
- Si $k \subseteq K$ et $K \subseteq L$ sont algébriques alors $k \subseteq L$ l'est.

Def. Soit $k \subseteq K$ une extension de corps. Le corps des éléments de K algébriques sur k est appelé **fermeture algébrique** de k dans K . Si c'est précisément k , on dit que k est **algébriquement fermé** dans K .

Prop. Un corps algébriquement clos est algébriquement fermé dans toute extension (mais pas l'inverse en général).

Rem. Soit K algébrique au-dessus de k et t_1, \dots, t_n des indéterminées. Alors $K(t_1, \dots, t_n)$ est algébrique sur $k(t_1, \dots, t_n)$.

Extensions linéairement disjointes

Def. Soit $k \subseteq K$ et $k \subseteq L$ deux extensions contenues dans une même troisième M . On dit qu'elles sont **linéairement disjointes** lorsque toute famille d'éléments de K linéairement indépendante sur K est encore linéairement indépendante sur L en tant que famille d'éléments de M .

Rem. Cette condition est symétrique et l'on a $K \cap L = k$. On appelle **composé** de K et L le sous-corps de M engendré par K et L : $K.L = k(K \cup L) = K(L) = L(K)$.

Prop. Soit $k \subseteq K$ et $k \subseteq L$ deux extensions contenues dans une troisième M et (v_j) une base de K comme k -ev. Alors K et L sont linéairement disjointes si et seulement si (v_i) est encore linéairement indépendante sur L quand on la voit comme une famille d'éléments de M .

Prop. Soit $k \subseteq K$ et $k \subseteq L$ deux extensions, l'une algébrique, contenues dans M . Alors $K.L$ est le sous- k -ev $\text{Vect}(\{xy, x \in K, y \in L\})$ de M et toute base de K sur k est encore une base de $K.L$ sur L .

Cor. On a $[K.L : L] = [K : k]$ et $[K.L : k] = [K : k] \cdot [L : k]$.

Prop. Soit $k \subseteq K$ une extension de corps et t_1, \dots, t_n des indéterminées. Alors les extensions $k \subseteq K$ et $k \subseteq k(t_1, \dots, t_n)$ sont linéairement disjointes dans $K(t_1, \dots, t_n)$. Si de plus K est algébrique sur k , alors toute base de K comme k -ev est une base de $K(t_1, \dots, t_n)$ comme $k(t_1, \dots, t_n)$ -ev.

Bases et degré de transcendance

Def. Soit $k \subseteq K$ une extension de corps. Une famille finie $x_1, \dots, x_n \in K$ est dite **algébriquement indépendante** sur k lorsque le seul polynôme $P \in k[t_1, \dots, t_n]$ tel que $P(x_1, \dots, x_n) = 0$ est le polynôme nul. En particulier, chacun des x_i est transcendant sur k , et un unique $x \in K$ est algébriquement indépendant sur k si et seulement s'il est transcendant sur k . Une famille infinie est algébriquement indépendante si toute sous-famille finie l'est.

Def. Base de transcendance : famille $(x_i)_{i \in I}$ de K algébriquement indépendante sur k telle que K est algébrique au-dessus de l'extension $k(x_i)_{i \in I}$.

Rem. Des indéterminées t_1, \dots, t_n sont algébriquement indépendantes et si x_1, \dots, x_n sont algébriquement indépendants alors $k(x_1, \dots, x_n)$ s'identifie à $k(t_1, \dots, t_n)$ et l'extension $k \subseteq k(x_1, \dots, x_n)$ est dite **transcendante pure**.

Prop. Soit $k \subseteq K$ une extension de corps. On a :

- Toute famille de K algébriquement indépendante sur k se complète en une base de transcendance de K sur k .
- De toute famille qui engendre K en tant qu'extension de corps de k , ou même qui engendre un corps intermédiaire E au-dessus duquel K est algébrique, on peut extraire une base de transcendance.
- (lemme d'échange) Soit z_1, \dots, z_n une base de transcendance finie de K sur k et $t \in K$ tel que z_1, \dots, z_l, t soit algébriquement indépendants sur k pour un certain $l \geq 0$. Alors $\exists j \in [l+1; n]$ tel qu'en remplaçant z_j par t dans z_1, \dots, z_n on obtienne encore une base de transcendance.
- Deux bases de transcendance de K sur k ont toujours le même cardinal.

Def. Soit $k \subseteq K$ une extension. Le cardinal d'une base de transcendance de K sur k est le **degré de transcendance** de K sur k , noté $\deg. \text{tr}_k(K)$ (nul ssi l'extension est algébrique).

Prop. Soit $k \subseteq K \subseteq L$ une tour d'extensions. Alors $\deg. \text{tr}_k(L) = \deg. \text{tr}_k(K) + \deg. \text{tr}_K(L)$.

Prop. Soit $k \subseteq k' \subseteq K$ une tour d'extensions avec k' algébrique sur k . Alors si $(x_i)_{i \in I}$ est une famille de K algébriquement indépendants sur k , ils le sont encore sur k' . De plus, toute base de k' comme k -ev est encore une base de $k'(x_i)_{i \in I}$ sur $k(x_i)_{i \in I}$, et $[k'(x_i)_{i \in I} : k(x_i)_{i \in I}] = [k' : k]$.

Corps de rupture, corps de décomposition et clôture algébrique

Def. Soit K un corps et $\mu \in K[t]$ irréductible. On appelle **corps de rupture** de μ sur K une extension $K \subseteq L$ telle que μ admette une racine $x \in K$ pour laquelle $L = K(x)$.

Prop. Soit K un corps et $\mu \in K[t]$ irréductible. Alors :

- Il existe un corps de rupture de μ sur K , à savoir $K[t]/(\mu)$.
- Soit $K \subseteq L$ un corps de rupture de μ sur K avec $L = K(x)$ et $K \subseteq L'$ une extension dans laquelle μ a une racine x' . Alors il existe un unique morphisme de corps $\varphi : L \rightarrow L'$ tel que $\varphi|_K = \text{Id}_K$ et $\varphi(x) = x'$.
- Si, en plus de (ii), $K \subseteq L'$ est aussi un corps de rupture de μ sur K , φ est un isomorphisme.

Def. Soit K un corps et $f \in K[t]$. On appelle **corps de décomposition** de f sur K une extension $K \subseteq L$ telle que f soit scindé sur L . Pour une famille (f_i) de polynômes, il s'agit d'une extension de K dans laquelle tous les f_i sont scindés, et qui est engendrée en tant que corps par l'ensemble de toutes les racines de tous les f_i .

Prop. Soit K un corps et (f_i) une famille quelconque de $K[t]$. Alors :

- Il existe un corps de décomposition des f_i sur K .
- Soit $K \subseteq L$ un corps de décomposition des f_i sur K et $K \subseteq L'$ une extension dans laquelle tous les f_i sont scindés. Alors il existe un unique morphisme de corps $\psi : L \rightarrow L'$ tel que $\psi|_K = \text{Id}_K$.
- Si f_j dans la famille est irréductible et x, x' sont racines de f_j dans L et L' respectivement, on peut choisir ψ tel que $\psi(x) = x'$.
- Si $K \subseteq L'$ est aussi un corps de décomposition des f_i sur K , tout ψ comme en (ii) est un isomorphisme.

Def. Soit K un corps. On appelle **clôture algébrique** de K , notée K^{alg} , une extension $K \subseteq L$ algébrique telle que tout polynôme de $K[t]$ soit scindé sur L .

Rem. Un corps est algébriquement clos si et seulement si il est égal à sa propre clôture algébrique.

Rem. Une clôture algébrique de K est égal au corps de décomposition de tous les polynômes de $K[t]$.

Th (de Steinitz). Soit K un corps quelconque. Alors il existe une clôture algébrique de K et, si L et L' sont deux clôtures algébriques de K , il existe un isomorphisme entre elles qui soit l'identité sur K . Enfin, une clôture algébrique est algébriquement close.

Éléments et extensions algébriques séparables

Def. Caractéristique d'un corps k : plus petit entier p égal à 0 dans k , ou 0 s'il n'en existe pas.

Def. Si k est de caractéristique $p > 0$ on définit le **Frobenius** d'exposant p : application $\text{Frob}_p : \begin{matrix} k & \rightarrow & k \\ x & \mapsto & x^p \end{matrix}$.

C'est un morphisme de corps, i.e. $(x+y)^p = x^p + y^p$ et $(xy)^p = x^p y^p$. On note k^p son image (sous-corps de k).

Def. Soit k un corps et $f \in k[t]$. On dit que f est **séparable** s'il est premier avec sa dérivée f' . C'est équivalent à avoir des racines simples dans une extension où f est scindé. Si f est irréductible cela revient à $f' \neq 0$.

Prop. Si k est de caractéristique $p = 0$, tout polynôme irréductible est séparable. Si $p > 0$ tout $f \in k[t]$ s'écrit de façon unique sous la forme $f(t) = f_0(t^{p^e})$ avec $e \in \mathbb{N}$ et $f_0' \neq 0$. Dans ce cas, si f est séparable $e = 0$, et si f est irréductible alors f_0 l'est aussi.

Lem. Soit k de caractéristique $p > 0$ et $h \in k[t]$ tel que $\exists i \in \llbracket 1; p \rrbracket, h^i \in k^p[t]$. Alors $h \in k^p[t]$.

Prop. Soit k de caractéristique $p > 0$, $f_0 \in k[t]$ unitaire irréductible et $f(t) := f_0(t^{p^e})$ où $e > 0$. Alors f est réductible (i.e. non irréductible) si et seulement si $f_0 \in k^p[t]$. Dans ce cas, on a aussi $f \in k^p[t]$.

Def. Soit $k \subseteq K$ une extension de corps. Un élément $x \in K$ algébrique sur k est dit **séparable** (sur k) si son polynôme minimal l'est.

Rem. En caractéristique 0, tout algébrique est séparable. En caractéristique p , $\forall x$ algébrique, $\exists ! e$ tel que x^{p^e} soit séparable, de degré $\deg(x)/p^e$. En particulier, si $p \nmid \deg(x)$, x est séparable.

Prop. Soit $k \subseteq K$ une extension de caractéristique $p > 0$ et $x \in K$ algébrique sur k . Exactement l'un des deux cas suivants se produit :

- x est séparable, le polynôme minimal de x^p sur k est dans $k^p[t]$, $\deg(x^p) = \deg(x)$ et $k(x) = k(x^p)$,
- x n'est pas séparable, le polynôme minimal de x^p sur k n'est pas dans $k^p[t]$ et $\deg(k^p) = \deg(x)/p$.

Def. Une extension $k \subseteq K$ algébrique est dite **séparable** lorsque tout élément de K est séparable sur k .

Prop. Soit $k \subseteq K$ une extension de corps finie de caractéristique p telle que K^p engendre K comme k -ev. Alors K est séparable sur k .

Prop. Soit $k \subseteq K$ une extension et $x_1, \dots, x_n \in K$ tel que $\forall i \in \llbracket 1; n \rrbracket, x_i$ est algébriques séparable sur $k(x_1, \dots, x_{i-1})$. Alors $k(x_1, \dots, x_n)$ est séparable sur k .

Cor. Soit $K = k(x_i)_{i \in I}$ avec les x_i algébriques séparables sur k . Alors tout K est algébrique séparable sur k .

Cor. Soit $k \subseteq K \subseteq L$ une tour d'extensions algébriques. Si K est séparable sur k et L est séparable sur K , alors L est séparable sur k .

Rem. Soit $k \subseteq K$ une extension. L'extension de k engendrée par les éléments de K algébriques séparables sur k est exactement l'ensemble de ces mêmes éléments, appelé **fermeture séparable** de k dans K . La fermeture séparable de k dans une clôture algébrique de k s'appelle **clôture séparable** de k . Si k est égal à sa clôture séparable on qu'il est **séparablement clos**.

Rem. Une extension $k \subseteq K$ telle que k soit égal à sa propre fermeture séparable dans K est dite **purement inséparable**. C'est la cas si et seulement si, en notant $p > 0$ la caractéristique, le polynôme minimal sur k d'un élément quelconque de K est de la forme $t^{p^e} - c$ où $c \in k$.

Corps parfaits, théorème de l'élément primitif

Def. Un corps k de caractéristique p est dit **parfait** lorsque, soit $p = 0$, soit $p > 0$ et $k^p = k$.

Prop. Un corps k est parfait si et seulement si toute extension algébrique de k est séparable.

Prop. Soit $k \subseteq K$ une extension algébrique avec k parfait. Alors K est aussi parfait.

Th (de l'élément primitif). Soit $K = k(x_1, \dots, x_n)$ avec x_1, \dots, x_n algébriques sur k et x_2, \dots, x_n séparables sur k . Alors l'extension $k \subseteq K$ est monogène, i.e. $\exists y \in K, K = k(y)$.

Cor. Toute extension finie séparable est monogène, en particulier toute extension finie d'un corps parfait.

Prop. Soit k un corps parfait et $k \subseteq K$ une extension de type fini. Alors $\exists x_1, \dots, x_{d+1} \in K, K = k(x_1, \dots, x_{d+1})$ avec x_1, \dots, x_d algébriquement indépendants sur k et x_{d+1} algébrique séparable sur $k(x_1, \dots, x_d)$.

Théorie de Galois

Def. Soit $K \subseteq L$ une extension algébrique. Deux éléments $x, x' \in L$ sont dits **conjugués** s'ils ont le même polynôme minimal sur K . C'est une relation d'équivalence qui définit des **classes de conjugaisons**.

Prop. Deux éléments $x, x' \in L$ sont conjugués lorsque tout polynôme de $K[t]$ qui s'annule sur l'un s'annule sur l'autre.

Rem. Si x est séparable, son polynôme minimal sur K est à racines simples dans K^{alg} , donc il admet $\deg(x)$ conjugués.

Def. Une extension $K \subseteq L$ est dite **normale** si elle vérifie une des propriétés équivalentes suivantes :

- tout conjugué sur K dans L^{alg} d'un élément de L est encore dans L ,
- tout polynôme irréductible sur K qui a une racine dans L est scindé sur L ,
- L est corps de décomposition d'une famille de polynômes sur K ,
- l'image de tout morphisme de corps $L \rightarrow L^{\text{alg}}$ qui soit l'identité sur K est égale à L .

Def. Une extension algébrique est **galoisienne** si elle est à la fois normale et séparable.

Def. Soit $K \subseteq L$ une extension galoisienne. On appelle **groupe de Galois** de l'extension, noté $\text{Gal}(K \subseteq L)$, l'ensemble des automorphismes de L au-dessus de K , i.e. les automorphismes de L qui soient l'identité sur K . Lorsque $L = K^{\text{sep}}$ (clôture séparable), on dit que $\text{Gal}(K \subseteq L) = \text{Gal}(K) = \Gamma_K$ est le groupe de Galois **absolu** de K .

Ex. $\text{Gal}(\mathbf{R} \subseteq \mathbf{C}) = \{\text{Id}_{\mathbf{C}}; x \mapsto \bar{x}\}$ et $\text{Gal}(\mathbf{F}_p \subseteq \mathbf{F}_{p^d}) = \{\text{Frob}_p^i, 0 \leq i \leq d-1\}$.

Th. Soit $K \subseteq L$ une extension galoisienne et $G := \text{Gal}(K \subseteq L)$. Alors :

- si $K \subseteq L$ est finie, alors G est fini et $\text{Card}(G) = [L : K]$,
- si $x \in L$ est fixé par tous les éléments de G alors $x \in K$.

De plus, si on appelle $\Phi: E \mapsto \text{Gal}(E \subseteq L)$ qui à un corps intermédiaire $K \subseteq E \subseteq L$ associe le groupe de Galois de l'extension $E \subseteq L$ (galoisienne) vu comme sous-groupe de G , on a :

- Φ est une injection (décroissante pour l'inclusion), si $K \subseteq L$ est finie c'est une bijection,
- un inverse à gauche est $H \mapsto \text{Fix}(H) = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$,
- $\Phi(E)$ est distingué dans G ssi $K \subseteq E$ est galoisienne, auquel cas $\text{Gal}(K \subseteq E) = G/\Phi(E)$,
- $\Phi(E_1.E_2) = \Phi(E_1) \cap \Phi(E_2)$, et si $K \subseteq L$ est finie, $\Phi(E_1 \cap E_2)$ est le ss-gr de G engendré par $\Phi(E_1)$ et $\Phi(E_2)$.

Def. Le **groupe de Galois d'un polynôme séparable** f sur un corps K est le groupe des permutations des racines de f qui définissent un automorphisme du corps de décomposition.

Rem. Pour L galoisienne sur K , les orbites $\{\sigma(x), \sigma \in \text{Gal}(K \subseteq L)\}$ sont exactement les classes d'équivalence pour la relation "être conjugué sur K ".

Th. Soit L un corps, G un groupe fini d'automorphismes de L et $K = \text{Fix}_L(G) = \{x \in L \mid \forall \sigma \in G, \sigma(x) = x\}$. Alors $K \subseteq L$ est une extension galoisienne de groupe de Galois G et $[L : K] = \text{Card}(G)$.

Th. Soit G un groupe, L un corps et χ_1, \dots, χ_n des caractères de G dans L (i.e. des morphismes $G \rightarrow L^\times$) deux à deux distincts. Alors les χ_1, \dots, χ_n sont linéairement indépendants en tant qu'applications $G \rightarrow L$.

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 $\exists l \in \mathbf{N}, g^l \in (h_1, \dots, h_m)$ (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. $\forall x \in A, \forall n \in \mathbf{N}, x^n \in \mathfrak{r} \implies x \in \mathfrak{r}$.

Def. Soit I un idéal de A . Le **radical de I** est $\sqrt{I} = \{x \in A \mid \exists n \in \mathbf{N}, x^n \in I\}$. C'est un idéal radical.

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 $J(E) := \{f \in k[t_1, \dots, t_d] \mid \forall (x_1, \dots, x_d) \in E, f(x_1, \dots, x_d) = 0\}$.

Rem. $J(E)$ est un idéal radical, J est décroissante pour l'inclusion, $J(E) = \bigcap_{x \in E} \mathfrak{M}_x$ où $\mathfrak{M}_x = J(\{x\})$ et en particulier $J(E) \neq k[t_1, \dots, t_d] \iff E = \emptyset$. De plus $J((k^{\text{alg}})^d) = \{0\}$.

Prop. Soit $E \subset (k^{\text{alg}})^d$ et $\mathcal{F} \subset k[t_1, \dots, t_d]$. On a $E \subset Z(\mathcal{F}) \iff \mathcal{F} \subset J(E)$.

Prop. Une partie $E \subset (k^{\text{alg}})^d$ vérifie $E = Z(J(E))$ si et seulement si c'est un fermé de Zariski.

Prop. Soit I un idéal de $k[t_1, \dots, t_d]$ et $E \subset (k^{\text{alg}})^d$. Alors $J(Z(I)) = \sqrt{I}$ et $Z(J(E))$ est le plus petit fermé de Zariski défini sur k qui contient E . De plus, Z et J définissent des bijections réciproques décroissantes entre idéaux radicaux de $k[t_1, \dots, t_d]$ et fermés de Zariski de $(k^{\text{alg}})^d$ définis sur k .

Def. Les éléments de $Z(I) \cap k^d$ sont appelés **points rationnels** de $Z(I)$. Ceux dans $Z(I) \cap ((k^{\text{alg}})^d \setminus k^d)$ sont appelés **points géométriques**. Enfin on appelle **point fermé** les $Z(\mathfrak{m})$ avec \mathfrak{m} un idéal maximal de $k[t_1, \dots, t_d]$ et $I \subset \mathfrak{m}$.

Def. Le corps $\kappa_{\mathfrak{m}} = k[t_1, \dots, t_d]/\mathfrak{m}$ s'appelle **corps résiduel** de $Z(\mathfrak{m})$. La classe modulo \mathfrak{m} d'un polynôme s'appelle **évaluation** du polynôme en $Z(\mathfrak{m})$ et $[\kappa_{\mathfrak{m}} : k]$ est appelé **degré** de $Z(\mathfrak{m})$.

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 \mathbf{P}_k^1 ou \mathbf{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 $\Gamma = \mathbf{Z}$, 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 :

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

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 $K = \mathbf{Q}$. Pour $m \in \mathbf{Z}$, 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 $\frac{n}{m} \in \mathbf{Q}$, $v_p\left(\frac{n}{m}\right) = v_p(n) - v_p(m)$. 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 $v: A \rightarrow \mathbf{Z} \cup \{\infty\}$ vérifie (i), (ii) et (iii) alors il existe une unique fonction $v: \text{Frac}(A) \rightarrow \mathbf{Z} \cup \{\infty\}$ 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 $r \in \mathbf{Z}$, 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 $r \in \mathbf{N}$.

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 :

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

$v(f)$ 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 v_∞ et les places v_h .

Rem. Lorsque k est algébriquement clos, les places de \mathbf{P}_k^1 s'identifient donc aux éléments de k ($x \in k$ est identifié à $f \in k(t) \mapsto v_x(f)$) plus l'élément ∞ (correspondant à la valuation v_∞).

L'indépendance des valuations

L'identité du degré

Diviseurs sur les courbes

Espaces de Riemann-Roch

Différentielles de Kähler

Def. Soit k un anneau et A une k -algèbre. On appelle espace des **différentielles de Kähler** de A sur k , noté $\Omega_{A/k}^1$, le A -module engendré par les symboles dx pour $x \in A$, soumis aux relations suivantes :

- (i) $d : A \rightarrow \Omega_{A/k}^1$ est linéaire, i.e. $\forall x, x' \in A, d(x + x') = dx + dx'$ et $\forall c \in k, \forall x \in A, d(cx) = c dx$,
- (ii) $\forall x, y \in A, d(xy) = x dy + y dx$.

Donc $\Omega_{A/k}^1$ est le quotient du A -module libre de base $\{dx, x \in A\}$ par le sous-module engendré par les relations ci-dessus.

Prop. Soit K une extension de corps de k de type fini. Les propriétés suivantes sont équivalentes :

- si la caractéristique est $p > 0$ alors, dans K , les corps K^p et k sont linéairement disjoints sur k^p ,
- il existe une base de transcendance (t_1, \dots, t_n) pour laquelle K est (algébrique) séparable sur $k(t_1, \dots, t_n)$.

Lorsque ces conditions sont vérifiées on dit que K est **séparable**. On dit aussi que (t_1, \dots, t_n) est une base de transcendance **séparante**.

Rem. Toute extension de corps en caractéristique 0 est séparable.

Prop. Si $K = k(C)$ est le corps des fractions d'une courbe sur un corps k et qu'au moins une des hypothèses suivantes est satisfaite :

- le corps de base k est parfait,
- la courbe C est irréductible.

alors l'extension K est séparable.

Prop. Soit K une extension de corps de k de type fini et séparable. Soit (t_1, \dots, t_n) une base de transcendance séparable. Alors $\Omega_{K/k}^1$ est un K -espace vectoriel de base dt_1, \dots, dt_n . Réciproquement, si $t_1, \dots, t_n \in K$ sont tels que dt_1, \dots, dt_n sont linéairement indépendants sur K , alors ils sont une base de transcendance séparable.

...

Théorème de Riemann-Roch

Points et places

Revêtements de courbes