Courbes algébriques
(notes de cours)

David A. Madore

17 avril 2017

ACCQ205

Git : `9e5a15a Mon Apr 17 19:45:30 2017 +0200`

Table des matières

1 Corps et extensions de corps

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

1.1.1. Sauf précision expresse du contraire, tous les anneaux considérés sont commutatifs et ont un élément unité (noté 1). Il existe un unique anneau dans lequel $0 = 1$, c'est l'anneau réduit à un seul élément, appelé l'**anneau nul**. (Pour tout anneau A, il existe un unique morphisme de A vers l'anneau nul ; en revanche, il n'existe un morphisme de l'anneau nul vers A que si A est lui-même l'anneau nul.)

1.1.2. Si k est un anneau, une **k-algèbre** (là aussi : implicitement commutative) est la donnée d'un morphisme d'anneaux $k \overset{\varphi_A}{\to} A$ appelé **morphisme structural** de l'algèbre. On peut multiplier un élément de A par un élément de k avec : $c \cdot x = \varphi_A(c)\, x \in A$ (pour $c \in k$ et $x \in A$). Un morphisme de k-algèbres est un morphisme d'anneaux $A \overset{\psi}{\to} B$ tel que le morphisme structural $k \overset{\varphi_B}{\to} B$ de B soit la composée $k \overset{\varphi_A}{\to} A \overset{\psi}{\to} B$ de celui de A avec le morphisme considéré.

De façon équivalente, une k-algèbre est un k-module qui est muni d'une multiplication k-bilinéaire qui en fait un anneau, et les morphismes de k-algèbres sont les applications k-linéaires qui préservent la multiplication ; le morphisme structural peut alors se retrouver par $c \mapsto c \cdot 1$. Notons qu'une $\mathbb{Z}$-algèbre est exactement la même chose qu'un anneau (raison pour laquelle il est souvent préférable d'énoncer les résultats en parlant de k-algèbres pour plus de généralité).

Dans la pratique, cependant k sera généralement un corps : une k-algèbre est donc un k-espace vectoriel muni d'une multiplication k-bilinéaire qui en fait un anneau, et le morphisme structural est automatiquement injectif si l'algèbre n'est pas l'algèbre nulle.

1.1.3. Un élément a d'un anneau A (sous-entendu : commutatif) est dit **régulier**, resp. **inversible**, lorsque $x \mapsto ax$ est injectif, resp. bijectif, autrement dit lorsque $ax = 0$ implique $x = 0$ (la réciproque est toujours vraie), resp. lorsqu'il existe x (appelé inverse de a) tel que $ax = 1$.

Un anneau dans A dans lequel l'ensemble des éléments régulier est égal à l'ensemble $A \setminus \{0\}$ des éléments non-nuls est appelé anneau **intègre** : autrement dit, un anneau intègre est un anneau dans lequel ($0 \neq 1$ et) $ab = 0$ implique $a = 0$ ou $b = 0$ (la réciproque est toujours vraie). Par convention, l'anneau nul n'est pas intègre.

Un idéal $\mathfrak{p}$ d'un anneau A est dit **premier** lorsque l'anneau quotient $A/\mathfrak{p}$ est un anneau intègre, autrement dit lorsque $\mathfrak{p} \neq A$ et que $ab \in \mathfrak{p}$ implique $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ (la réciproque est toujours vraie).

1.1.4. Dans un anneau (toujours sous-entendu commutatif...), l'ensemble noté $A^\times$ des éléments inversibles est un groupe, aussi appelé groupe des **unités** de A.

Un **corps** est un anneau k dans lequel l'ensemble $k^\times$ des éléments inversibles est égal à l'ensemble $k \setminus \{0\}$ des éléments non-nuls : autrement dit, un corps est un anneau dans lequel ($0 \neq 1$ et) tout élément non-nul est inversible. De façon équivalente, un corps est un anneau ayant exactement deux idéaux (qui sont alors 0 et lui-même). Par convention, l'anneau nul n'est pas un corps.

Un corps est, en particulier, un anneau intègre.

Un idéal $\mathfrak{m}$ d'un anneau A est dit **maximal** lorsque l'anneau quotient $A/\mathfrak{m}$ est un corps : de façon équivalente, lorsque $\mathfrak{m} \neq A$ et que $\mathfrak{m}$ est maximal pour l'inclusion parmi les idéaux $\neq A$. Un idéal maximal est, en particulier, premier.

1.1.5. À titre d'exemple, l'idéal $n\mathbb{Z}$ de $\mathbb{Z}$ (on rappelle que tous les idéaux de $\mathbb{Z}$ sont de cette forme, pour un $n \in \mathbb{N}$ défini de façon unique) est premier si et seulement si $n = 0$ (le quotient étant $\mathbb{Z}$ lui-même) ou bien n est un nombre premier ; il est intègre exactement si n est un nombre premier (le quotient étant alors le corps $\mathbb{Z}/n\mathbb{Z}$).

Pour donner un exemple moins évident, dans l'anneau $k[x, y]$ des polynômes à deux indéterminées x, y sur un corps k, l'idéal (y) (des polynômes s'annulant identiquement sur l'axe des abscisses) est premier mais non maximal puisque $k[x, y]/(y) \cong k[x]$, tandis que l'idéal (x, y) (des polynômes s'annulant à l'origine) est maximal puisque $k[x, y]/(x, y) \cong k$.

Plus généralement, dans un anneau factoriel A, un idéal de la forme (f) avec $f \in A$, est premier si et seulement si f est nul ou irréductible (mais ce ne sont, en général, pas les seuls idéaux premiers de A) ; comparer avec 1.1.14 plus bas.

Le résultat ensembliste suivant sera admis :

Lemme 1.1.6 (principe maximal de Hausdorff)**.** Soit $\mathscr{F}$ un ensemble de parties d'un ensemble A. On suppose que $\mathscr{F}$ est non vide et que pour toute partie non vide $\mathscr{T}$ de $\mathscr{F}$ totalement ordonnée par l'inclusion (c'est-à-dire telle que pour $I, I' \in \mathscr{T}$ on a soit $I \subseteq I'$ soit $I \supseteq I'$) la réunion $\bigcup_{I \in \mathscr{T}} I$ soit contenue dans un élément de $\mathscr{F}$. Alors il existe dans $\mathscr{F}$ un élément M maximal pour l'inclusion (c'est-à-dire que si $I \supseteq M$ avec $I \in \mathscr{F}$ alors $I = M$).

Proposition 1.1.7. Dans un anneau A, tout idéal strict (=autre que A) est inclus dans un idéal maximal.

Démonstration. Si I est un idéal strict de A, on applique le principe maximal de Hausdorff à $\mathscr{F}$ l'ensemble des idéaux stricts de A contenant I. Si $\mathscr{T}$ est une chaîne (=partie totalement ordonnée pour l'inclusion) de tels idéaux, la réunion $\bigcup_{I\in\mathscr{T}} I$ en est encore un [1] (pour voir que la réunion est encore un idéal strict, remarquer que 1 n'y appartient pas). Le principe maximal de Hausdorff permet de conclure. ☺

1.1.8. Un élément x d'un anneau A est dit **nilpotent** lorsqu'il existe $n \geq 0$ tel que $x^n = 0$ (un anneau dans lequel le seul élément nilpotent est 0 est dit **réduit**).

Proposition 1.1.9. Dans un anneau, l'ensemble des éléments nilpotents est un idéal : cet idéal est aussi l'intersection des idéaux premiers de l'anneau. (On l'appelle le **nilradical** de l'anneau.)

Le quotient de l'anneau par son nilradical est réduit.

Démonstration. L'ensemble des nilpotents est un idéal car si $x^n = 0$ et $y^n = 0$ alors $(x+y)^{2n} = 0$ en développant. Il est inclus dans tout idéal premier $\mathfrak{p}$, car $x^n \in \mathfrak{p}$ (et à plus forte raison $x^n = 0$) implique $x \in \mathfrak{p}$ par récurrence sur n. Montrons que si z est inclus dans tout idéal premier, alors z est nilpotent.

Supposons que z n'est pas nilpotent. Considérons $\mathfrak{p}$ un idéal maximal pour l'inclusion parmi les idéaux ne contenant aucun z^n : un tel idéal existe d'après le principe maximal de Hausdorff (il existe un idéal ne contenant aucun z^n, à savoir $\{0\}$). Montrons qu'il est premier : si $x, y \notin \mathfrak{p}$, on veut voir que $xy \notin \mathfrak{p}$. Par maximalité de $\mathfrak{p}$, chacun des idéaux [2] $\mathfrak{p} + (x)$ et $\mathfrak{p} + (y)$ doit rencontrer $\{z^n\}$, c'est-à-dire qu'on doit pouvoir trouver deux éléments de la forme $f + ax$ et $g + by$ avec $f, g \in \mathfrak{p}$ et $a, b \in A$, qui soient des puissances de z ; leur produit est alors aussi une puissance de z, donc n'est pas dans $\mathfrak{p}$, donc $abxy \notin \mathfrak{p}$ (car les trois autres termes sont dans $\mathfrak{p}$), et a plus forte raison $xy \notin \mathfrak{p}$.

Enfin, dire que le quotient de A par son nilradical est réduit signifie exactement que si une puissance d'un élément est nilpotente alors cet élément lui-même est nilpotent, ce qui est évident. ☺

1. La réunion de deux idéaux n'est généralement pas un idéal, car si $x \in I$ et $x' \in I'$, la somme $x + x'$ n'a pas de raison d'appartenir à $I \cup I'$. En revanche, si $\mathscr{T}$ est une famille d'idéaux totalement ordonnée par l'inclusion, alors $\bigcup_{I\in\mathscr{T}} I$ est un idéal : si $x \in I$ et $x' \in I'$, où $I, I' \in \mathscr{T}$, on peut écrire soit $I \subseteq I'$ soit $I' \subseteq I$, et dans un cas comme dans l'autre on a $x + x' \in \bigcup_{I\in\mathscr{T}} I$.

2. On rappelle que si I, J sont deux idéaux d'un anneau, l'ensemble $I + J = \{u + v : u \in I, v \in J\}$ est un idéal, c'est l'idéal engendré par $I \cup J$, c'est-à-dire, le plus petit idéal contenant I et J ; on l'appelle idéal somme de I et J. Dans le cas particulier où $J = (x)$ est engendré par un élément, c'est donc l'idéal engendré par $I \cup \{x\}$.

1.1.10. Si A est un anneau intègre, on définit un corps $\mathrm{Frac}(A)$, dit **corps des fractions** de A, dont les éléments sont les symboles formels $\frac{a}{q}$ avec $a \in A$ et $q \in A \setminus \{0\}$, en convenant d'identifier $\frac{a}{q}$ avec $\frac{a'}{q'}$ lorsque $aq' = a'q$ (i.e., formellement, $\mathrm{Frac}(A)$ est le quotient de $A \times (A \setminus \{0\})$ par la relation d'équivalence qu'on vient de dire) ; la structure d'anneau est définie par $\frac{a}{q} + \frac{a'}{q'} = \frac{aq'+a'q}{qq'}$ et $\frac{a}{q} \cdot \frac{a'}{q'} = \frac{aa'}{qq'}$. On a aussi un morphisme injectif $A \to \mathrm{Frac}(A)$ envoyant a sur $\frac{a}{1}$, et on identifiera A à son image par ce morphisme.

À titre d'exemple, $\mathrm{Frac}(\mathbb{Z})$ est $\mathbb{Q}$ (c'est même la définition de ce dernier).

1.1.11. Le corps des fractions d'un anneau intègre A vérifie la propriété « universelle » suivante : si K est un corps quelconque, et $\varphi\colon A \to K$ un morphisme d'anneaux injectif, il existe un unique morphisme de corps $\hat{\varphi}\colon \mathrm{Frac}(A) \to K$ (i.e., extension de corps, cf. ci-dessous) qui prolonge φ (i.e., $\hat{\varphi}(a) = \varphi(a)$ si $a \in A$). En effet, il suffit de définir $\hat{\varphi}(\frac{a}{q})$ par $\varphi(a)/\varphi(q)$.

Ainsi, $\mathrm{Frac}(A)$ est *engendré en tant que corps* par les éléments de A (comparer 1.2.4).

1.1.12. Le corps des fractions de l'anneau $k[t_1, \ldots, t_n]$ des polynômes en n indéterminées $t_1, \ldots, t_n$ sur un corps k est appelé corps des **fractions rationnelles** (ou parfois « fonctions rationnelles ») en n indéterminées $t_1, \ldots, t_n$ sur k, et noté $k(t_1, \ldots, t_n)$.

1.1.13. Le fait suivant sera important : si k est un corps et K une k-algèbre *de dimension finie* intègre, alors K est, en fait, un corps. En effet, une application k-linéaire $K \to K$ injective est automatiquement bijective, et en appliquant ce fait à la multiplication par un $a \in K$, on voit que tout élément régulier est inversible.

1.1.14. Rappelons par ailleurs le **lemme de Gauß** concernant les polynômes irréductibles : si A est un anneau factoriel et K son corps des fractions, alors l'anneau $A[t]$ des polynômes en une indéterminée sur A est factoriel ; et par ailleurs $f \in A[t]$ est irréductible (dans $A[t]$) si et seulement si f est constant et irréductible dans A, *ou bien* f est irréductible dans $K[t]$ et le pgcd (dans A) des coefficients de f vaut 1 (on dit que f est **primitif** lorsque cette dernière condition est vérifiée). Le point-clé dans la démonstration est de montrer que le pgcd $c(f)$ des coefficients d'un polynôme dans $A[t]$, aussi appelé **contenu** de f, est multiplicatif (i.e., $c(fg) = c(f)\,c(g)$) ; la décomposition en facteurs irréductibles dans $A[t]$ d'un élément de $A[t]$ s'obtient alors à partir de celle de $K[t]$ et de celle dans A du contenu.

Notamment, le corps $k[z_1, \ldots, z_n]$ des fractions rationnelles en n indéterminées sur un corps k est un anneau factoriel, un polynôme $f \in k[z_1, \ldots, z_n, t]$ (en $n+1$ indéterminées) irréductible et faisant effectivement intervenir t est encore irréductible dans $k(z_1, \ldots, z_n)[t]$, et réciproquement, un polynôme irréductible dans $k(z_1, \ldots, z_n)[t]$ donne un polynôme irréductible dans

$k[z_1, \ldots, z_n, t]$ quitte à multiplier par le pgcd des dénominateurs.

1.2 Algèbre engendrée, extensions de corps

1.2.1. Si A est une k-algèbre (où k est un anneau), et $(x_i)_{i\in I}$ est une famille d'éléments de A, l'intersection de toutes les sous-k-algèbres de A contenant les x_i est encore une sous-k-algèbre de A contenant les x_i, c'est-à-dire que c'est la plus petite sous-k-algèbre de A contenant les x_i. On l'appelle k-algèbre **engendrée** (dans A) par les x_i et on la note $k[x_i]_{i\in I}$. Lorsque les x_i sont en nombre fini (le cas qui nous intéressera le plus), disons indicés par $1, \ldots, n$, on note $k[x_1, \ldots, x_n]$, et on dit que $k[x_1, \ldots, x_n]$ est une k-algèbre **de type fini** (en tant que k-*algèbre*).


On prendra garde au fait que la même notation $k[x_1, \ldots, x_n]$ peut désigner soit la k-algèbre engendrée par $x_1, \ldots, x_n$ dans une k-algèbre A plus grande, soit l'anneau des polynômes à n indéterminées $x_1, \ldots, x_n$ sur k. Ces conventions sont cependant cohérentes en ce sens que l'anneau des polynômes à n indéterminées sur k est bien la k-algèbre engendrée par les indéterminées (cf. le point suivant). Il faut donc prendre garde à ce que sont $x_1, \ldots, x_n$ quand cette notation apparaît : si aucune remarque n'est faite et que les x_i n'ont pas été introduits auparavant, il est généralement sous-entendu que ce sont des indéterminées.

1.2.2. La k-algèbre engendrée par les x_i dans A peut encore se décrire concrètement comme l'ensemble de tous les éléments de A qui peuvent être obtenus à partir de 1 et des x_i par sommes, produits par éléments de k et produits binaires. Autrement dit, ce sont les valeurs des polynômes à coefficients dans k évalués en des x_i. Pour dire les choses de façon plus sophistiquée, en supposant les x_i en nombre fini pour simplifier (et indicés par $1, \ldots, n$), il existe un unique morphisme $k[t_1, \ldots, t_n] \to A$ envoyant t_i sur x_i, à savoir le morphisme « d'évaluation » qui à un $P \in k[t_1, \ldots, t_n]$ associe $P(x_1, \ldots, x_n)$, et $k[x_1, \ldots, x_n]$ est l'*image* de ce morphisme. On peut donc dire qu'une k-algèbre de type fini $k[x_1, \ldots, x_n]$ est la même chose qu'un *quotient* de l'algèbre de polynômes $k[t_1, \ldots, t_n]$ (par le noyau du morphisme d'évaluation).

Pour ce qui est du cas infini : la k-algèbre $k[x_i]_{i\in I}$ engendrée par une famille quelconque $(x_i)_{i\in I}$ d'éléments de A est la *réunion* des algèbres $k[x_i]_{i\in J}$ engendrées par toutes les sous-familles finies (i.e., $J \subseteq I$ fini) de la famille donnée. (Autrement dit, $y \in A$ appartient à $k[x_i]_{i\in I}$ si et seulement si il existe $J \subseteq I$ fini tel que y appartienne à $k[x_i]_{i\in J}$.)


Attention : une sous-algèbre d'une algèbre de type fini n'est pas, en général, de type fini. Un contre-exemple est fourni par l'anneau des polynômes $f \in k[x, y]$ à deux indéterminées sur un corps k qui prennent une valeur constante sur l'axe des ordonnées : cette k-algèbre est engendrée par $1, x, xy, xy^2, xy^3, \ldots$ et on peut montrer qu'aucun nombre fini de ses éléments ne suffit à l'engendrer.

1.2.3. Une **extension de corps** est un morphisme d'anneaux $k \to K$ entre corps (c'est-à-dire que K est une k-algèbre qui est un corps). Un tel morphisme est automatiquement injectif (car son noyau est un idéal d'un corps qui ne contient pas 1), et qui peut donc être considéré comme une inclusion : on notera soit $k \subseteq K$ soit K/k une telle extension ; lorsque l'inclusion a été fixée, on dit aussi que k est un **sous-corps** de K. Un **corps intermédiaire** à une extension $k \subseteq K$, ou encore **sous-extension**, est, naturellement, une extension de corps $k \subseteq E$ contenue dans K ; on dit aussi que $k \subseteq E \subseteq K$ est une **tour** d'extensions (et de même pour n'importe quel nombre de corps intermédiaires).

1.2.4. Si $k \subseteq K$ est une extension de corps, et $(x_i)_{i\in I}$ est une famille d'éléments de K, l'intersection de tous les sous-corps de K contenant k et les x_i est encore un sous-corps de K contenant k et les x_i, c'est-à-dire que c'est le plus petit corps intermédiaire contenant les x_i. On l'appelle sous-extension **engendrée** (dans K) par les x_i et on la note $k(x_i)_{i\in I}$. Lorsque les x_i sont en nombre fini (le cas qui nous intéressera le plus), disons indicés par $1, \dots, n$, on note $k(x_1, \dots, x_n)$, et on dit que $k(x_1, \dots, x_n)$ est une extension de k **de type fini** (en tant qu'extension de *corps*).


On prendra garde au fait que la même notation $k(x_1, \dots, x_n)$ peut désigner soit la sous-extension engendrée par $x_1, \dots, x_n$ dans une extension K plus grande, soit le corps des fractions rationnelles à n indéterminées $x_1, \dots, x_n$ sur k. Ces conventions sont cependant cohérentes en ce sens que le corps des fractions rationnelles à n indéterminées sur k est bien la sous-extension engendrée par les indéterminées (cf. le point suivant). Comme dans le cas de la k-algèbre engendrée, il faut donc prendre garde à ce que sont $x_1, \dots, x_n$ quand cette notation apparaît : si aucune remarque n'est faite et que les x_i n'ont pas été introduits auparavant, il est généralement sous-entendu que ce sont des indéterminées.

1.2.5. La sous-extension engendrée (au-dessus de k) par les x_i dans K peut encore se décrire concrètement comme l'ensemble de tous les éléments de A qui peuvent être obtenus à partir des éléments de k et des x_i par sommes, produits et inverses (d'éléments non nuls). Autrement dit, ce sont les valeurs des fractions rationnelles à coefficients dans k évalués en des x_i (à condition d'être bien définies).

Pour ce qui est du cas infini : la sous-extension $k(x_i)_{i\in I}$ engendrée par une famille quelconque $(x_i)_{i\in I}$ d'éléments de K est la *réunion* des sous-extensions $k(x_i)_{i\in J}$ engendrées par toutes les sous-familles finies (i.e., $J \subseteq I$ fini) de la famille donnée. (Autrement dit, $y \in K$ appartient à $k(x_i)_{i\in I}$ si et seulement si il existe $J \subseteq I$ fini tel que y appartienne à $k(x_i)_{i\in J}$.)

Contrairement au cas des algèbres (cf. 1.2.2), il *est* bien vrai qu'une sous-extension d'une extension de corps de type fini est de type fini. Mais ce n'est pas évident ! (Cela sera démontré en 1.5.8 ci-dessous.)

1.3 Extensions algébriques et degré

1.3.1. Si $k \subseteq K$ est une extension de corps et $x \in K$, on a noté (cf. 1.2.4) $k(x)$ l'extension de k engendrée par x. On dira aussi que $k \subseteq k(x)$ est une extension **monogène** (certains auteurs utilisent « simple », notamment en anglais).

On se pose la question de mieux comprendre cette extension. Pour cela, on introduit l'unique morphisme $\varphi\colon k[t] \to K$, où $k[t]$ est l'anneau des polynômes en une indéterminée t sur k, qui envoie t sur x, c'est-à-dire, le morphisme « d'évaluation » envoyant P sur $P(x)$ pour chaque $P \in k[t]$. Le noyau de φ est un idéal de $k[t]$. Exactement l'un des deux cas suivants se produit :

— Soit φ est injectif (=son noyau est nul), auquel cas on dit que x est **transcendant** sur k. Dans ce cas, d'après la propriété universelle du corps des fractions (cf. 1.1.11), φ se prolonge de manière unique en une extension de corps $k(t) \to K$ (où $k(t)$ est le corps des fractions rationnelles en l'indéterminée t sur k), envoyant $P/Q \in k(t)$ sur $P(x)/Q(x) \in K$, et l'image de $k(t)$ dans K est précisément $k(x)$ (cf. 1.2.5). Ceci permet d'identifier $k(x)$ avec le corps des fractions rationnelles en une indéterminée (i.e., de considérer x comme une indéterminée).

— Soit le noyau de φ est engendré par un unique polynôme unitaire $\mu_x \in k[t]$, qu'on appelle le **polynôme minimal** de x, et alors x est dit **algébrique** (ou **entier [algébrique]**)[3] sur k. Alors l'image $k[x]$ de φ (cf. 1.2.2) s'identifie à $k[t]/(\mu_x)$, une k-algèbre de dimension $\deg \mu_x$ finie sur k, qu'on appelle le **degré** de x ; mais comme $k[x]$ est intègre (puisque c'est une sous-algèbre d'un corps), et de dimension finie, c'est un corps (cf. 1.1.13) : on a donc $k(x) = k[x] = k[t]/(\mu_x)$ dans cette situation. De plus, le polynôme μ_x est irréductible dans $k[t]$ (sans quoi on aurait deux éléments dont le produit est nul dans K).

On remarquera que les éléments de k eux-mêmes sont exactement les algébriques de degré 1 sur k. On remarquera aussi que si $k \subseteq k' \subseteq K$, alors le polynôme minimal d'un $x \in K$ sur k' divise celui sur k (car ce dernier annule x et est à coefficients dans k donc dans k').

1.3.2. La dichotomie décrite ci-dessus admet une sorte de réciproque : d'une part, si t est une indéterminée, alors dans $k(t)$ (le corps des fractions rationnelles) l'élément t est bien transcendant sur k (en fait, toute fraction rationnelle non constante est transcendante sur k) ; d'autre part, si μ est un polynôme unitaire irréductible sur k, alors $k[t]/(\mu)$ est une k-algèbre de dimension finie intègre donc (cf. 1.1.13) une extension de corps de k dans laquelle la classe $x := \bar{t}$ de

3. Les termes « algébrique » et « entier [algébrique] » sont synonymes au-dessus d'un corps puisque tout polynôme peut être rendu unitaire en divisant par le coefficient dominant ; sur un anneau, la notion d'élément entier [algébrique] se comporte généralement mieux.

l'indéterminée t est algébrique de polynôme minimal μ : ce corps $k(x) = k[t]/(\mu)$ est appelé **corps de rupture** du polynôme irréductible μ sur k (lorsque μ n'est pas unitaire, on peut encore parler de corps de rupture quitte à diviser par le coefficient dominant ; en revanche, l'irréductibilité est essentielle), et il va de soi que le corps de rupture coïncide avec k si et seulement si μ est de degré 1 (précisément, si $\mu = t - a$ alors l'élément $x := \bar{t}$ de $k(x) = k[t]/(\mu)$ s'identifie avec $a \in k$).

1.3.3. Une extension de corps $k \subseteq K$ est dite **algébrique** lorsque chaque élément de K est algébrique sur k. On dit aussi que K est algébrique « au-dessus de » k ou « sur » k.

Un corps k est dit **algébriquement clos** lorsque la seule extension algébrique de k est k lui-même : d'après les remarques précédentes, cela revient à dire que les seuls polynômes unitaires irréductibles dans $k[t]$ sont les $t - a$.

À titre d'exemple, le corps $\mathbb{C}$ des nombres complexes est algébriquement clos (« théorème de D'Alembert-Gauß »).

1.3.4. Si $k \subseteq K$ est une extension de corps, on peut considérer K comme un k-espace vectoriel, et sa dimension (finie ou infinie) est notée $[K : k]$ et appelée **degré** de l'extension. Une extension de degré fini est aussi dite **finie** (ainsi, on pourra dire simplement que K est « fini sur k » pour dire que son degré est fini). Il va de soi qu'une sous-extension d'une extension finie est encore finie.

Il résulte de l'identification de $k(x)$ à $k[t]/(\mu_x)$ que, si x est un élément algébrique sur k, alors $[k(x) : k]$ est fini et égal au degré $\deg \mu_x =: \deg(x)$ de x. *A contrario*, si x est transcendant, alors $[k(x) : k]$ est infini. En particulier, on a montré que : *l'extension monogène $k \subseteq k(x)$ est finie si et seulement si x est algébrique sur k.*

1.3.5. On aura également besoin du fait que si $k \subseteq K \subseteq L$ sont deux extensions imbriquées alors $[L : k] = [K : k]\,[L : K]$ (au sens où le membre de gauche est fini si et seulement si les deux facteurs du membre de droite le sont, et dans ce cas leur produit lui est égal). Cela résulte du fait plus précis que si $(x_i)_{i\in I}$ est une k-base de K et $(y_j)_{j\in J}$ une K-base de L, alors $(x_i y_j)_{(i,j)\in I\times J}$ est une k-base de L (vérification aisée).

1.3.6. Les faits suivants sont à noter :

(1) Une extension de corps engendrée par un nombre fini d'éléments algébriques est finie (en effet, si $x_1, \ldots, x_n$ sont algébriques sur k, alors chaque extension $k(x_1, \ldots, x_{i-1}) \subseteq k(x_1, \ldots, x_i)$ est monogène algébrique, donc finie, donc leur composée est finie).

(1bis) En fait, sous ces conditions, on peut être un peu plus précis : $k(x_1, \ldots, x_n)$ a une base comme k-espace vectoriel formée de monômes en les $x_1, \ldots, x_n$ (c'est-à-dire d'expressions de la forme $x_1^{r_1} \cdots x_n^{r_n}$). Ceci découle de la description de la base donnée en 1.3.5 appliquée au fait que chaque $k(x_1, \ldots, x_i)$ a une base sur $k(x_1, \ldots, x_{i-1})$ formée des puissances de x_i (jusqu'au degré de

celui-ci exclu).

(2) Une extension $k \subseteq K$ est finie si et seulement si elle est à la fois algébrique et de type fini. (Le sens « si » résulte de l'affirmation (1) ; pour le sens « seulement si », remarquer que pour tout $x \in K$, l'extension $k \subseteq k(x)$ est finie donc algébrique, et qu'une base de K comme k-espace vectoriel engendre certainement K comme extension de corps de k.)

(3) Une extension de corps engendrée par une famille quelconque d'éléments algébriques est algébrique (en effet, si $K = k(x_i)_{i\in I}$ et $y \in K$, alors, cf. 1.2.5, y appartient à $k(x_i)_{i\in J}$ pour une sous-famille finie des x_i, et d'après le (1), cette extension est finie sur k donc $k(y)$ l'est, c'est-à-dire que y est algébrique sur k). Concrètement, donc, les sommes, différences, produits et inverses de quantités algébriques sur k sont algébriques sur k.

(4) Si $k \subseteq K$ et $K \subseteq L$ sont algébriques alors $k \subseteq L$ l'est (en effet, si $y \in L$, et si $x_1, \ldots, x_n \in K$ sont les coefficients du polynôme minimal de y sur K, alors y est algébrique sur $k(x_1, \ldots, x_n)$, qui est une extension finie de k d'après (1), donc $k(x_1, \ldots, x_n, y)$ est une extension finie de $k(x_1, \ldots, x_n)$ donc de k, donc $k(y)$ est une extension finie de k, donc y est algébrique sur k).

1.3.7. L'observation (3) ci-dessus entraîne que si $k \subseteq K$ est une extension de corps, l'extension de k engendrée par tous les éléments de K algébriques sur k est tout simplement l'*ensemble* de tous les éléments de K algébriques sur k, c'est-à-dire que cet ensemble est un corps, qui est manifestement la plus grande extension intermédiaire algébrique sur k : on l'appelle la **fermeture algébrique** de k dans K (la précision « dans K » est importante).

Si c'est précisément k, on dit que k est **algébriquement fermé** dans K : autrement dit, cela signifie que tout élément de K est soit transcendant sur k soit élément de k (=algébrique de degré 1). Un corps algébriquement clos est algébriquement fermé dans toute extension, mais un corps peut être algébriquement fermé dans une extension sans pour autant être algébriquement clos (par exemple $\mathbb{Q}$ dans le corps $\mathbb{Q}(t)$ des fractions rationnelles).

D'après (4) ci-dessus, la fermeture algébrique de k dans K est algébriquement fermée dans K.

1.3.8. On peut aussi remarquer le fait suivant : si K est algébrique au-dessus de k, alors $K(t_1, \ldots, t_n)$ où les t_i sont des indéterminées (ou, de façon équivalente, des éléments algébriquement indépendants sur K d'un corps plus gros, cf. 1.5.2) est algébrique sur $k(t_1, \ldots, t_n)$. (En effet, $K(t_1, \ldots, t_n)$ est engendré sur $k(t_1, \ldots, t_n)$ par tous les éléments de K, qui sont algébriques sur k, donc certainement aussi sur $k(t_1, \ldots, t_n)$, et on applique 1.3.6(3).)

1.4 Extensions linéairement disjointes

(On pourra se référer à 2.5.8 plus bas pour une réinterprétation des résultats de cette section.)

Définition 1.4.1. Si $k \subseteq K$ et $k \subseteq L$ sont 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 quand on la voit comme une famille d'éléments de M. (Il suffit, bien sûr, de le tester pour des familles *finies*.)

1.4.2. Remarquons que $K \cup L = k$ dans ces conditions (car si $c \in K$ n'est pas dans k, il est linéairement indépendant avec 1 sur k, donc il le reste sur L, et ne peut pas appartenir à L).

La condition d'être linéairement disjointes est cependant plus forte : par exemple, $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(\zeta\sqrt[3]{2})$, où ζ est une racine primitive cubique de l'unité (disons $\exp(2i\pi/3)$ dans les complexes) ont pour intersection $\mathbb{Q}$ dans $\mathbb{Q}(\zeta, \sqrt[3]{2})$ (ou dans les complexes), et pourtant elles ne sont pas linéairement disjointes (vérifier que $1, \sqrt[3]{2}, \sqrt[3]{4}$ sont linéairement indépendants sur $\mathbb{Q}$ mais que $(\zeta\sqrt[3]{2})^2 \times 1 + (\zeta\sqrt[3]{2}) \times \sqrt[3]{2} + 1 \times \sqrt[3]{4} = 0$).

La définition de la relation d'être linéairement disjointes n'est pas symétrique. Elle l'est cependant :

Proposition 1.4.3. La propriété pour deux extensions contenues dans une même troisième d'être linéairement disjointes est symétrique.

Démonstration. Supposons $k \subseteq K$ et $k \subseteq L$ linéairement disjointes comme on vient de le définir : on veut inverser le rôle de L et K. Soient $y_1, \ldots, y_n$ des éléments de L linéairement indépendants sur k. Supposons que pour certains $x_1, \ldots, x_n$ de K non tous nuls, on ait $x_1y_1 + \cdots + x_ny_n = 0$ dans M. Quitte à réordonner les x_i, on peut supposer que $x_1, \ldots, x_r$ sont linéairement indépendants sur k (avec $r \geq 1$) et que $x_{r+1}, \ldots, x_n$ en sont des combinaisons k-linéaires, disons $x_i = \sum_{j=1}^{r} c_{i,j}x_j$ pour $i > r$ avec $c_{i,j} \in k$. La relation $\sum_{i=1}^{n} x_iy_i = 0$ devient donc $\sum_{i=1}^{r} x_iy_i + \sum_{i=r+1}^{n}\sum_{j=1}^{r} c_{i,j}x_jy_i = 0$, soit, en regroupant : $\sum_{j=1}^{r}\left(y_j + \sum_{i=r+1}^{n} c_{i,j}y_i\right)x_j = 0$. Par indépendance linéaire des x_i sur k donc sur L, on a $y_j + \sum_{i=r+1}^{n} c_{i,j}y_i = 0$ pour chaque $j \leq r$, ce qui contredit l'indépendance linéaire des y_i sur L. ☺

Proposition 1.4.4. Soient $k \subseteq K$ et $k \subseteq L$ deux extensions contenues dans une même troisième M, et soit (v_j) une base de K comme k-espace vectoriel. 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.

Démonstration. La nécessité (« seulement si ») fait partie de la définition des extensions linéairement disjointes appliquée à la base (v_i). Montrons la suffisance. Pour cela, soit $x_1, \ldots, x_n$ des éléments de K linéairement indépendants sur k, et soient $v_1, \ldots, v_m$ les éléments de la base qui interviennent dans l'écriture des x_j. On peut écrire $x_j = \sum_{i=1}^{m} c_{i,j} v_j$ avec $c_{i,j} \in k$. Le fait que les x_j soient linéairement indépendants signifie exactement que la matrice des $c_{i,j}$ a rang n. Mais *le rang d'une matrice ne dépend pas du corps sur lequel on la considère*, si bien qu'elle a aussi rang n quand on la voit comme une matrice à coefficients dans L : comme par hypothèse les $v_1, \ldots, v_m$ vus comme des éléments de M sont linéairement indépendants sur L, ceci implique que les $x_j = \sum_{i=1}^{m} c_{i,j} v_j$ vus comme des éléments de M sont eux aussi linéairement indépendants sur L. On a donc bien prouvé que K et L sont linéairement disjointes. ☺

1.4.5. Lorsque $k \subseteq K$ et $k \subseteq L$ sont deux extensions contenues dans une même troisième M, on appelle **composé** des corps K et L le sous-corps de M engendré par K et L, autrement dit $k(K \cup L) = K(L) = L(K)$, et on le note $K.L$.


Il faut prendre garde au fait que l'extension composée n'a de sens que si les deux extensions sont contenues dans une même troisième (en changeant les plongements de K et L dans M on peut changer $K.L$ en un corps non isomorphe).

Proposition 1.4.6. Si $k \subseteq K$ est une extension algébrique et $k \subseteq L$ une extension quelconque, toutes les deux contenues dans une même extension M, alors l'extension composée $K.L$ est le sous-k-espace vectoriel de M engendré par les produits xy avec $x \in K$ et $y \in L$.

Démonstration. Soit V le sous-k-espace vectoriel de M engendré par les produits xy avec $x \in K$ et $y \in L$, autrement dit l'ensemble des $\sum_i x_i y_i$ (sommes finies) avec $x_i \in K$ et $y_i \in L$ (les coefficients dans k peuvent s'absorber dans les x_i ou les y_i). Il est trivial que $V \subseteq K.L$, et pour prouver l'inclusion contraire il suffit de montrer que V est bien un corps. En développant les produits $(\sum_i x_i y_i)(\sum x'_j y'_j) = \sum_{i,j} (x_i x'_j)(y_i y'_j)$ on voit que V est stable par produit : c'est donc une algèbre sur k ou K ou L comme on préfère. Comme V est un sous-anneau de M, qui est un corps, il s'agit d'un anneau intègre.

Dans le cas où $[K : k] < \infty$, le L-espace vectoriel V est également de dimension finie, car une famille génératrice (v_j) de K comme k-espace vectoriel est encore génératrice de V comme L-espace vectoriel (en effet, si tout élément de K peut s'écrire $\sum_j c_j v_j$ pour certains $c_i \in k$, alors tout élément de V peut s'écrire $\sum_i (\sum_j c_{i,j} v_j) y_i = \sum_j (\sum_i c_{i,j} y_i) v_j$), et d'après 1.1.13 on en déduit que V est un corps. On a donc obtenu le résultat annoncé pour le cas où $[K : k] < \infty$.

En général, si $z \in V$ n'est pas nul, on peut écrire $z = \sum_i x_i y_i$ pour certains $x_i \in K$ et $y_i \in L$. Soit K_0 l'extension de k engendrée par les x_i : l'hypothèse selon laquelle K est algébrique entraîne que $[K_0 : k] < \infty$ (cf. 1.3.6(1)), et on

a $z \in K_0.L$. D'après le cas précédemment traité, tout élément de $K_0.L$, et en particulier z^{-1}, appartient au sous-k-espace vectoriel V_0 de M engendré par les produits xy avec $x \in K_0$ et $y \in L$, et on a bien sûr $V_0 \subseteq V$. Donc $z^{-1} \in V$ et V est bien un corps. ☺

Proposition 1.4.7. Si $k \subseteq K$ et $k \subseteq L$ sont deux extensions linéairement disjointes contenues dans une même troisième, et si l'une des deux est algébrique, alors toute base de K sur k est encore une base de $K.L$ sur L.

Démonstration. Soit (v_j) une base de K comme k-espace vectoriel. D'après la définition de la relation d'être linéairement disjointes, les (v_j) vus dans $K.L$ sont linéairement indépendants sur L. Mais d'après la proposition 1.4.6, tout élément de $K.L$ peut s'écrire sous la forme d'une somme finie $\sum_i x_i y_i$ pour des $x_i \in K$ et $y_i \in L$, et on peut réécrire $x_i = \sum c_{i,j} v_j$ donc $\sum_i x_i y_i = \sum_i (\sum_j c_{i,j} v_j) y_i = \sum_j (\sum_i c_{i,j} y_i) v_j$ appartient au L-espace vectoriel engendré dans $K.L$ par les (v_j), c'est-à-dire que ceux-ci sont générateurs, et finalement sont une base de $K.L$. ☺

1.4.8. En particulier, dans les conditions de la proposition ci-dessus, on a $[K.L : L] = [K : k]$, et d'après 1.3.5 on a aussi $[K.L : k] = [K : k] \cdot [L : k]$.

Réciproquement, si pour deux extensions $k \subseteq K$ et $k \subseteq L$ contenues dans une même troisième on a l'égalité $[K.L : L] = [K : k]$ ***finie*** (notons que si à la fois $k \subseteq K$ et $k \subseteq L$ sont finies, il revient au même de supposer $[K.L : k] = [K : k] \cdot [L : k]$), on peut considérer une base (finie !) de K comme k-espace vectoriel, qui, d'après 1.4.6, engendre $K.L$ comme L-espace vectoriel, donc en est une base puisqu'elle a la bonne taille : d'après 1.4.4, ceci assure que K et L sont linéairement disjointes.

Proposition 1.4.9. Soit $k \subseteq K$ une extension de corps, et $t_1, \ldots, t_n$ des indéterminées. Alors les extensions $k \subseteq K$ et $k \subseteq k(t_1, \ldots, t_n)$ sont linéairement disjointes dans $K(t_1, \ldots, t_n)$, i.e., toute famille k-linéairement indépendante de K est encore linéairement indépendante sur $k(t_1, \ldots, t_n)$ (dans $K(t_1, \ldots, t_n)$). Si de plus K est algébrique sur k, alors toute base de K comme k-espace vectoriel est une base de $K(t_1, \ldots, t_n)$ comme $k(t_1, \ldots, t_n)$-espace vectoriel.

Démonstration. Soit $(u_j)_{j \in J}$ une famille k-linéairement indépendante de K : montrons qu'ils sont linéairement indépendants sur $k(t_1, \ldots, t_n)$. Si on a une relation de dépendance linéaire non triviale $\sum_{j \in J} c_j u_j = 0$ dans $K(t_1, \ldots, t_n)$ avec les c_j dans $k(t_1, \ldots, t_n)$ tous nuls sauf un nombre fini, les c_j sont des fractions rationnelles ; cette même relation est valable si on multiplie les c_j par un dénominateur commun, si bien qu'on peut supposer que les c_j sont des polynômes en $t_1, \ldots, t_n$; quitte à diviser autant de fois que nécessaire par chaque t_i qui divise tous les c_j, on peut supposer que le c_j ne s'annulent pas tous à l'origine (i.e., quand on remplace tous les t_i par 0) : mais alors, en les évaluant à l'origine (i.e., en

remplaçant tous les t_i par 0), on obtient une relation de dépendance linéaire non-triviale sur k, qui est censée ne pas exister. Ceci montre la première affirmation. La seconde découle de 1.4.7. ☺

1.5 Bases et degré de transcendance

Définition 1.5.1. Si $k \subseteq K$ est une extension de corps, une famille finie $x_1, \ldots, x_n$ d'éléments de K est dite **algébriquement indépendante** (il serait plus logique de dire « collectivement transcendante ») sur k lorsque le seul polynôme $P \in k[t_1, \ldots, t_n]$ à coefficients dans k et tel que $P(x_1, \ldots, x_n) = 0$ (relation de « dépendance algébrique » sur k entre les x_i) est le polynôme nul ; autrement dit, lorsque le morphisme « d'évaluation » $k[t_1, \ldots, t_n] \to K$ (avec $k[t_1, \ldots, t_n]$ l'anneau des polynômes en n indéterminées) envoyant P sur $P(x_1, \ldots, x_n)$ est injectif. En particulier, chacun des x_i est transcendant sur k ; et un unique élément x de K est algébriquement indépendant sur k si et seulement si il est transcendant sur k.

On dit d'une famille infinie $(x_i)_{i\in I}$ d'éléments de K qu'elle est algébriquement indépendante sur k lorsque toute sous-famille finie d'entre eux l'est (i.e., il n'existe pas de relation de dépendance algébrique entre les x_i, c'est-à-dire entre un nombre fini d'entre eux).

Une famille $(x_i)_{i\in I}$ d'éléments de K est appelée **base de transcendance** de K sur k lorsqu'elle est algébriquement indépendante sur k et que K est algébrique au-dessus de l'extension $k(x_i)_{i\in I}$ de k engendrée par les x_i.

1.5.2. Il est trivialement le cas que $t_1, \ldots, t_n$ sont algébriquement indépendants si $t_1, \ldots, t_n$ sont des indéterminées, c'est-à-dire, si $k(t_1, \ldots, t_n)$ est le corps des fractions rationnelles en n indéterminées. Réciproquement, si $x_1, \ldots, x_n$ sont algébriquement indépendants, alors $k(x_1, \ldots, x_n)$ s'identifie au corps des fractions rationnelles en n indéterminées comme dans le cas $n = 1$ déjà vu en 1.3.1 ci-dessus (en envoyant P/Q, avec $P, Q \in k[t_1, \ldots, t_n]$ et $Q \neq 0$, sur $P(x_1, \ldots, x_n)/Q(x_1, \ldots, x_n)$).

(On peut encore dire la même chose pour un nombre infini de x_i, à condition de définir le corps des fractions rationnelles en un nombre infini d'indéterminées, comme « réunion », techniquement la limite inductive, des corps de fractions rationnelles sur une sous-famille finie quelconque d'entre elles.)

1.5.3. Lorsque les $(x_i)_{i\in I}$ sont algébriquement indépendants, on dit aussi que l'extension $k \subseteq k(x_i)_{i\in I}$ est **transcendante pure** : autrement dit, une extension transcendante pure est un corps de fractions rationnelles en un nombre quelconque (peut-être infini, cf. ci-dessus) de variables.

La question de déterminer si une extension de corps est transcendante pure peut être extrêmement difficile ; à titre d'exemple, le corps $\mathbb{R}(x, y : x^2 + y^2 - 1)$

des fractions de $\mathbb{R}[x,y]/(x^2+y^2-1)$ est une extension transcendante pure de $\mathbb{R}$, car il est en fait isomorphe à $\mathbb{R}(t)$ où $t = \frac{y}{x+1}$ (de réciproque $x = \frac{1-t^2}{1+t^2}$ et $y = \frac{2t}{1+t^2}$) : on reviendra sur cet exemple en 3.1.4.

Certains auteurs disent parfois par abus de langage (ces notes tâcheront de l'éviter) que $k \subseteq k(x_1,\dots,x_n)$ est transcendante pure pour dire en fait que les $x_1,\dots,x_n$ sont algébriquement indépendants. L'exemple ci-dessus montre que c'est abusif ; cependant, on verra que ce ne l'est plus si on sait que le degré de transcendance est bien n.

Si $(x_i)_{i\in I}$ est une base de transcendance de K sur k, celle-ci « décompose » l'extension $k \subseteq K$ en deux : l'extension $k \subseteq k(x_i)_{i\in I}$ est transcendante pure, et l'extension $k(x_i)_{i\in I} \subseteq K$ est algébrique.

Proposition 1.5.4. Soit $k \subseteq K$ une extension de corps.

(1a) Toute famille algébriquement indépendante sur k d'éléments de K se complète en une base de transcendance de K sur k. (Ceci s'applique notamment à la famille vide, donc il existe toujours une base de transcendance de K sur k.)
(1b) 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.

(2) *Lemme d'échange :* Si $z_1,\dots,z_n$ est une base de transcendance finie de K sur k et t un élément de K tel que $z_1,\dots,z_\ell,t$ soient algébriquement indépendants sur k (pour un certain ℓ, qui peut être 0), alors il existe j entre $\ell+1$ et n tel qu'en remplaçant z_j par t dans la base de transcendance $z_1,\dots,z_n$ on obtienne encore une base de transcendance.

(3) Deux bases de transcendance de K sur k ont toujours le même cardinal.

Démonstration. (1a) Le principe de maximalité de Hausdorff (1.1.6, appliqué à l'ensemble $\mathscr{F}$ des familles algébriquement indépendantes sur k) montre que toute famille algébriquement indépendante est contenue dans une famille algébriquement indépendante maximale. Montrons qu'une telle famille est une base de transcendance : si $(x_i)_{i\in I}$ est une famille algébriquement indépendante maximale, on veut donc prouver que K est algébrique sur $k(x_i)_{i\in I}$; pour cela, soit $t \in K$, on veut montrer qu'il n'est pas transcendant sur $k(x_i)_{i\in I}$. Mais s'il l'est, on observe que la famille obtenue en rajoutant t à la famille $(x_i)_{i\in I}$ est encore algébriquement indépendante : en effet, si on avait un polynôme $P(t,x_{i_1},\dots,x_{i_n})$ qui l'annulât, en considérant P comme polynôme de la seule variable t (dont il dépend effectivement, sinon il donnerait une relation de dépendance algébrique sur k entre les x_i, chose qui n'existe pas) on contredirait la transcendance de t sur $k(x_i)_{i\in I}$. Par maximalité de $(x_i)_{i\in I}$, ceci ne peut pas se produire : donc K est bien algébrique sur $k(x_i)_{i\in I}$ et $(x_i)_{i\in I}$ est une base de transcendance.

(1b) Soit maintenant $(x_i)_{i\in J}$ une famille génératrice (i.e., $K = k(x_i)_{i\in J}$) ou telle que K soit algébrique sur $E = k(x_i)_{i\in J}$: soit I une partie maximale de J telle

que $(x_i)_{i\in I}$ soit algébriquement indépendante (de nouveau on utilise le principe de maximalité), et on va montrer qu'il s'agit d'une base de transcendance. Si ce n'est pas le cas, l'extension K de $k(x_i)_{i\in I}$ n'est pas algébrique, donc (cf. 1.3.6(3)) elle ne peut pas être engendrée uniquement par des éléments algébriques, autrement dit il existe $j \in J$ (et évidemment $j \notin I$) tel que x_j soit transcendant sur $k(x_i)_{i\in I}$, et par ce qu'on vient d'expliquer la famille obtenue en rajoutant j à I contredit la maximalité de I.

(2) Soit $z_1, \ldots, z_n$ une base de transcendance (finie) et $t \in K$ tel que $z_1, \ldots, z_\ell, t$ soient algébriquement indépendants. Puisque $t \in K$ est algébrique sur $k(z_1, \ldots, z_n)$, on peut trouver une relation de dépendance algébrique $P(t, z_1, \ldots, z_n) = 0$; comme $z_1, \ldots, z_\ell, t$ sont algébriquement indépendants par hypothèse, le polynôme P ne peut pas dépendre que de ces variables, donc il doit faire intervenir z_j pour un certain j entre $\ell + 1$ et n. Soit z'_i défini par $z'_i = z_i$ si $i \neq j$ et $z'_j = t$. La relation $P(t, z_1, \ldots, z_n) = 0$, ou, quitte à échanger deux variables, $\hat{P}(z_j, z'_1, \ldots, z'_n) = 0$, se lit aussi comme affirmant que z_j est algébrique sur $k(z'_1, \ldots, z'_n)$: il s'ensuit que K est algébrique sur $k(z'_1, \ldots, z'_n)$ (puisqu'il est algébrique sur $k(z_1, \ldots, z_n)$ et qu'on vient de voir que ce dernier est algébrique sur $k(z'_1, \ldots, z'_n)$, cf. 1.3.6 (3) et (4)). D'autre part, les z'_i sont algébriquement indépendants : car s'ils ne l'étaient pas, comme les $z_1, \ldots, z_n$ le sont, une relation $Q(z'_1, \ldots, z'_n) = 0$ ferait intervenir $z'_j = t$, c'est-à-dire que t serait algébrique sur les autres z'_i, donc z_j serait algébrique sur les $z'_i = z_i$ pour $i \neq j$ (vu qu'on sait déjà qu'il est algébrique sur tous les z'_i), or par hypothèse ce n'est pas le cas. On a bien prouvé que les z'_i forment une base de transcendance de K sur k.

(3) Tout d'abord, s'il existe une base de transcendance finie $z_1, \ldots, z_n$, alors toute famille algébriquement indépendante $x_1, \ldots, x_{n'}$ vérifie $n' \leq n$. En effet, si $n' > n$, le lemme d'échange permet de remplacer un des z_i, mettons z_1, par x_1, puis un des z_i autre que z_1, mettons z_2, par x_2, et ainsi de suite, toujours en obtenant des bases de transcendance. Finalement, on voit que $x_1, \ldots, x_n$ est une base de transcendance, contredisant le fait supposé que les x_i pour $n < i \leq n'$ sont encore transcendants dessus. (Ici, on a supposé la famille $x_1, \ldots, x_{n'}$ finie, mais de façon générale on voit que toute sous-famille finie d'une famille algébriquement indépendante doit avoir au plus n éléments donc toute famille algébriquement indépendante est finie.)

Enfin, si on a une base de transcendance infinie $(x_i)_{i\in I}$, d'après ce qu'on vient de voir, toute autre base de transcendance $(y_j)_{j\in J}$ est également infinie ; par ailleurs, tout élément y_j de K est algébrique sur le sous-corps engendré par une sous-famille *finie* des x_i, donc on a une application de J vers les parties finies de I telle que l'image réciproque d'une partie finie donnée de I soit finie, et ceci prouve bien que I et J ont même cardinal (en utilisant le fait que, pour I infini, I est équipotent à l'ensemble de ses parties finies). ☺

Définition 1.5.5. Si $k \subseteq K$ est une extension de corps, le cardinal d'une base de transcendance de K sur k (dont on vient de montrer qu'il ne dépend pas du choix de celle-ci) s'appelle **degré de transcendance** de K sur k et se note $\deg.\,\mathrm{tr}_k(K)$.

On remarquera que le degré de transcendance vaut 0 si et seulement si l'extension est algébrique.

Proposition 1.5.6. Si $k \subseteq K \subseteq L$ est une tour d'extensions, alors $\deg.\,\mathrm{tr}_k(L) = \deg.\,\mathrm{tr}_k(K) + \deg.\,\mathrm{tr}_K(L)$.

Démonstration. Si $(x_i)_{i\in I}$ est une base de transcendance de K sur k et $(y_j)_{j\in J}$ de L sur K, alors leur réunion (évidemment disjointe !) est une base de transcendance de L sur k : en effet, d'une part, une relation de dépendance algébrique sur k entre les x_i et les y_j est *a fortiori* une relation de dépendance algébrique sur K entre les y_j, qui n'existe pas, c'est-à-dire plus exactement qui ne peut pas faire intervenir les y_j, donc est une relation de dépendance algébrique sur k entre les x_i, qui n'existe pas non plus, c'est-à-dire plus exactement qu'elle est nulle, et ceci montre que la réunion considérée est algébriquement indépendante ; d'autre part, L est algébrique sur $K(y_j)$, qui est lui-même algébrique sur $k(x_i)_{i\in I}(y_j)_{j\in J}$ car K l'est sur $k(x_i)_{i\in I}$ (cf. 1.3.8), donc L est algébrique sur $k(x_i, y_j)$ (cf. 1.3.6(4)). ☺

Proposition 1.5.7. Soit $k \subseteq k' \subseteq K$ est une tour d'extensions avec k' algébrique sur k : alors si $(x_i)_{i\in I}$ est une famille d'éléments de K algébriquement indépendants sur k, ils le sont encore sur k'. De plus, dans ces conditions, toute base de k' comme k-espace vectoriel est encore une base de $k'(x_i)_{i\in I}$ sur $k(x_i)_{i\in I}$, et notamment, $[k'(x_i)_{i\in I} : k(x_i)_{i\in I}] = [k' : k]$.

Démonstration. Montrons la première affirmation. D'après la définition de l'indépendance algébrique d'une famille infinie, il suffit de la prouver pour un nombre fini $x_1, \ldots, x_n$ d'éléments.

D'après 1.5.4(1b), on peut extraire de $x_1, \ldots, x_n$ une base de transcendance de $k'(x_1, \ldots, x_n)$ sur k', disons $x_1, \ldots, x_r$. Ainsi, $k'(x_1, \ldots, x_n)$ est algébrique sur $k'(x_1, \ldots, x_r)$; or $k'(x_1, \ldots, x_r)$ est algébrique sur $k(x_1, \ldots, x_r)$ (cf. 1.3.8) ; donc $k'(x_1, \ldots, x_n)$, et en particulier $k(x_1, \ldots, x_n)$, est algébrique sur $k(x_1, \ldots, x_r)$, ce qui n'est possible que pour $n = r$ d'après 1.5.4(3). Donc $x_1, \ldots, x_n$ sont algébriquement indépendants sur k'.

(Variante en utilisant 1.5.6 : On a $\deg.\,\mathrm{tr}_k\, k'(x_1, \ldots, x_n) = \deg.\,\mathrm{tr}_k\, k(x_1, \ldots, x_n) + \deg.\,\mathrm{tr}_{k(x_1,\ldots,x_n)}\, k'(x_1, \ldots, x_n)$, où le premier terme vaut n par hypothèse et le second vaut 0 de nouveau parce que $k'(x_1, \ldots, x_n)$ est algébrique sur $k(x_1, \ldots, x_n)$ (cf. 1.3.8) : ceci montre $\deg.\,\mathrm{tr}_k\, k'(x_1, \ldots, x_n) = n$. Mais on a aussi $\deg.\,\mathrm{tr}_k\, k'(x_1, \ldots, x_n) = \deg.\,\mathrm{tr}_k\, k' + \deg.\,\mathrm{tr}_{k'}\, k'(x_1, \ldots, x_n)$, et de nouveau $\deg.\,\mathrm{tr}_k\, k' = 0$: ceci montre $\deg.\,\mathrm{tr}_{k'}\, k'(x_1, \ldots, x_n) = n$. C'est donc que $x_1, \ldots, x_n$ est une base de transcendance de $k'(x_1, \ldots, x_n)$ (d'après

1.5.4 (1b) et (3)). En particulier, $x_1, \ldots, x_n$ sont algébriquement indépendants sur k'.)

Pour ce qui est de la dernière affirmation, elle découle de 1.4.9 (au moins dans le cas d'un nombre fini de x_i ; mais comme tout élément de $k(x_i)_{i\in I}$ ou $k(x_i)_{i\in I}$ ne fait intervenir qu'un nombre fini des x_i, le cas général se ramène au cas fini). ☺

Proposition 1.5.8. Si $k \subseteq E \subseteq L$ et si L est de type fini sur k (i.e., $L = k(x_1, \ldots, x_n)$ pour un nombre fini d'éléments $x_1, \ldots, x_n$ de L), alors E l'est aussi.

Démonstration. On a vu $\deg.\,\mathrm{tr}_k(L) = \deg.\,\mathrm{tr}_k(E) + \deg.\,\mathrm{tr}_E(L)$: cette quantité étant finie, les deux termes de droite sont finis. Si $t_1, \ldots, t_r$ est une base de transcendance de E sur k, quitte à remplacer k par $k(t_1, \ldots, t_r)$, on peut supposer E algébrique sur k, et on veut montrer que E est finie sur k.

Supposons maintenant $L = k(x_1, \ldots, x_n)$ avec $x_1, \ldots, x_r$ une base de transcendance de L sur k (possible, quitte à renuméroter, d'après 1.5.4(1b)). On a $[L : k(x_1, \ldots, x_r)] < \infty$ d'après 1.3.6(1), et en particulier $[E(x_1, \ldots, x_r) : k(x_1, \ldots, x_r)] < \infty$. Or d'après 1.5.7, $[E(x_1, \ldots, x_r) : k(x_1, \ldots, x_r)] = [E : k]$: on a bien $[E : k] < \infty$ comme annoncé. ☺

1.6 Corps de rupture, corps de décomposition, clôture algébrique

Définition 1.6.1. Soit K un corps et $\mu \in K[t]$ un polynôme irréductible. On appelle **corps de rupture** de μ sur K une extension $K \subseteq L$ telle que μ admette une racine x dans K pour laquelle $L = K(x)$. (Bien sûr, μ est alors le polynôme minimal de x sur K.)

On a déjà introduit le terme « corps de rupture » en 1.3.2, mais il s'agit bien de la même notion, plus précisément :

Proposition 1.6.2. Soit K un corps et $\mu \in K[t]$ un polynôme irréductible. Alors : (1) il existe un corps de rupture de μ sur K, à savoir $K[t]/(\mu)$. (2) Si $K \subseteq L$ est un corps de rupture de μ sur K avec $L = K(x)$, et si $K \subseteq L'$ est une extension dans laquelle μ a une racine x', alors il existe un unique morphisme de corps [4] $L \to L'$ qui soit l'identité sur K et envoie x sur x'. (3) Si en outre $K \subseteq L'$ est aussi un corps de rupture de μ sur K, le morphisme en question est un isomorphisme ; autrement dit : si $K \subseteq L$ et $K \subseteq L'$ sont deux corps de rupture de μ sur K avec $L = K(x)$ et $L' = K(x')$, il existe un unique morphisme $L \to L'$ qui soit l'identité sur K et envoie x sur x', et c'est un isomorphisme ; notamment, deux corps de rupture de μ sur K sont isomorphes.

4. On rappelle qu'un morphisme de corps est automatiquement injectif.

Démonstration. L'affirmation (1) a déjà été démontrée en 1.3.2, en appelant x la classe de t dans $K[t]/(\mu)$. Pour ce qui est de (2), il suffit de le prouver pour $L = K[t]/(\mu)$, or le morphisme $L \to L'$ recherché doit provenir d'un morphisme $K[t] \to L'$ envoyant t sur x', ce morphisme existe bien et est unique (il s'agit de l'évaluation en x'), et il passe au quotient de façon unique (puisque x' a pour polynôme minimal μ sur K). Enfin, pour ce qui est de (3), le morphisme est un isomorphisme (i.e., est surjectif) puisque son image est un corps contenant K et x' et qu'on a $L' = K(x')$. ☺

Définition 1.6.3. Soit K un corps et $f \in K[t]$ un polynôme quelconque. On appelle **corps de décomposition** de f sur K une extension $K \subseteq L$ telle que f soit scindé (=complètement décomposé) sur L, i.e., $f = c\prod_{i=1}^{n}(t - x_i)$ (avec c le coefficient dominant de f, et $x_1, \ldots, x_n$ ses racines avec multiplicité) et que $L = K(x_1, \ldots, x_n)$.

On définit de même la notion de corps de décomposition sur K d'une famille (f_i) quelconque 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, cf. 1.2.4) par l'ensemble de toutes les racines de tous les f_i.

Proposition 1.6.4. Soit K un corps et $f \in K[t]$ un polynôme. Alors : (1) Il existe un corps de décomposition de f sur K. (2) Si $K \subseteq L$ est un corps de décomposition de f sur K, et si $K \subseteq L'$ est une extension dans laquelle f est scindé, il existe un morphisme de corps $L \to L'$ qui soit l'identité sur K ; de plus, (2b) dans les conditions, si f est irréductible, et si x et x' sont une racine de f dans L et L' respectivement, on peut de plus choisir l'isomorphisme pour envoyer x sur x'. (3) Si en outre $K \subseteq L'$ est aussi un corps de décomposition de f sur K, tout morphisme comme en (2) est un isomorphisme ; autrement dit : si $K \subseteq L$ et $K \subseteq L'$ sont deux corps de décomposition de f sur K, il existe un morphisme $L \to L'$ qui soit l'identité sur K, et un tel morphisme est un isomorphisme ; notamment, deux corps de décomposition de f sur K sont isomorphes.

Démonstration. Pour montrer (1), (2) et (2b), on procède par récurrence sur le degré de f. Si $\deg f = 1$, toutes les affirmations sont triviales (K lui-même est un corps de décomposition de f sur K, et c'est le seul). Sinon, soit f_1 un facteur irréductible de f sur K (qui est f lui-même si f est irréductible) et soit E le corps de rupture de f_1, dans lequel f_1 admet une racine, disons x_1, et si on cherche à prouver (2b) on prendra $x_1 = x$: comme x_1 est racine de f dans E, on peut écrire $f = (t - x_1)f_2$ dans $E[t]$, avec $\deg f_2 < \deg f =: n$, ce qui permet par récurrence d'appliquer les conclusions à f_2.

Pour montrer (1), on utilise l'hypothèse de récurrence pour construire un corps de décomposition L de f_2 sur E : disons $L = E(x_2, \ldots, x_n)$ avec $x_2, \ldots, x_n$ les racines de f_2, et il est clair que f est scindé sur L et on a $L = K(x_1, \ldots, x_n)$,

donc L est un corps de décomposition de f sur K. Pour montrer (2) et (2b), soit x' une racine de f dans L' : d'après 1.6.2(2), il existe un unique plongement de E dans L' envoyant x_1 sur x' : quitte à identifier E à son image, on peut considérer qu'il s'agit de l'identité ; comme L est un corps de décomposition de f_2 sur E, par l'hypothèse de récurrence, il existe un morphisme $L \to L'$ qui soit l'identité sur E, donc sur K, ce qui prouve (2), et ce morphisme envoie x_1 sur x' (on les a identifiés), ce qui prouve aussi (2b).

Enfin, pour ce qui est de (3), le morphisme est un isomorphisme (i.e., est surjectif) puisque son image est un corps contenant K et toutes les racines $x'_1, \ldots, x'_n$ de f dans L', or on a $L = K(x'_1, \ldots, x'_n)$. ☺

On peut obtenir l'existence et l'unicité du corps de décomposition d'une famille finie de polynômes en appliquant le résultat ci-dessus à leur produit (puisque visiblement, scinder $f_1, \ldots, f_n$ revient à scinder leur produit $f_1 \cdots f_n$). Le même résultat vaut pour un nombre possiblement infini de polynômes :

Proposition 1.6.5. Soit K un corps et (f_i) une famille quelconque d'éléments de $K[t]$. Alors : (1) Il existe un corps de décomposition des f_i sur K. (2) Si $K \subseteq L$ est un corps de décomposition des f_i sur K, et si $K \subseteq L'$ est une extension dans laquelle tous les f_i sont scindés, il existe un morphisme de corps $L \to L'$ qui soit l'identité sur K ; de plus, (2b) dans les conditions, si un des f_i est irréductible, et si x et x' sont une racine de f_i dans L et L' respectivement, on peut de plus choisir l'isomorphisme pour envoyer x sur x'. (3) Si en outre $K \subseteq L'$ est aussi un corps de décomposition des f_i sur K, tout morphisme comme en (2) est un isomorphisme ; autrement dit : si $K \subseteq L$ et $K \subseteq L'$ sont deux corps de décomposition des f_i sur K, il existe un morphisme $L \to L'$ qui soit l'identité sur K, et un tel morphisme est un isomorphisme ; notamment, deux corps de décomposition des f_i sur K sont isomorphes.

Esquisse de démonstration. Le (1) se montre comme 1.6.4(1) avec un argument de passage à l'infini : pour chaque polynôme $f_i \in K[t]$, on construit un corps de décomposition de ce polynôme au-dessus de tous les corps de décomposition précédemment obtenus, et tous ces corps sont algébriques d'après 1.3.6 (3) et (4). Le (2) et (2b) se montrent comme 1.6.4(2), de nouveau en passant à l'infini : quitte à supposer que L a été construit comme on vient de l'indiquer, pour chaque polynôme $f_i \in K[t]$, on construit un morphisme entre le corps de décomposition de ce polynôme au-dessus de tous les précédents, et un sous-corps de L', jusqu'à obtenir un morphisme de L dans L'. Pour le (3), il s'agit de nouveau d'observer que si L' est engendré par toutes les racines de tous les f_i, comme elles sont dans l'image du morphisme, le morphisme est surjectif. ☺

L'intérêt principal de la proposition qu'on vient de démontrer est de montrer l'existence et l'unicité de la clôture algébrique :

Définition 1.6.6. Soit K un corps. On appelle **clôture algébrique** de K une extension $K \subseteq L$ algébrique telle que tout polynôme de $K[t]$ soit scindés sur L.

De toute évidence, un corps est algébriquement clos si et seulement si il est égal à sa propre clôture algébrique. Remarquons également qu'une clôture algébrique de K est exactement la même chose qu'un corps de décomposition de *tous* les polynômes à coefficients dans K.

Proposition 1.6.7 (théorème de Steinitz)**.** Soit K un corps quelconque. Alors il existe une clôture algébrique de K, et de plus, 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 de K est algébriquement close.

Démonstration. L'existence et l'unicité résultent de la proposition 1.6.5 appliquée à la famille de tous les polynômes à coefficients dans K.

Enfin, si M est une clôture algébrique de L, qui est lui-même une clôture algébrique de K, on voit que M est algébrique sur K d'après 1.3.6(4), donc tout élément de M est racine d'un polynôme à coefficients dans K, donc il est déjà dans L, et en fait $L = M$, ce qui montre que L est algébriquement clos. ☺

1.6.8. La fermeture algébrique d'un corps K dans un corps algébriquement clos L qui le contient fournit une clôture algébrique de K (vérification facile). À titre d'exemple, puisque $\mathbb{C}$ est algébriquement clos, la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$, c'est-à-dire l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$, est une clôture algébrique de $\mathbb{Q}$.

On notera souvent K^{alg} une clôture algébrique de K, le choix étant peu important puisqu'elles sont toutes isomorphes au-dessus de K comme on vient de le voir (néanmoins, comme l'isomorphisme n'est pas *unique*, le fait d'écrire « une » clôture algébrique est justifié : deux constructions de clôtures algébriques donneront certes des objets isomorphes, mais il n'y a pas de façon « canonique » de les identifier).

1.7 Éléments et extensions algébriques séparables

1.7.1. On rappelle que la **caractéristique** d'un corps k est le générateur positif de l'idéal noyau de l'unique morphisme d'anneaux $\mathbb{Z} \to k$: plus concrètement, c'est le plus petit entier p tel que $p = 0$ dans k (au sens où $1 + 1 + \cdots + 1 = 0$ avec p termes dans la somme), ou bien 0 si un tel entier n'existe pas : c'est soit 0 soit un nombre premier (positif).

Si k est de caractéristique $p > 0$, alors l'application $\mathrm{Frob}_p \colon k \to k$ définie par $x \mapsto x^p$, ou **Frobenius** d'exposant p, est un morphisme de corps, i.e., on a $(x + y)^p = x^p + y^p$ et $(xy)^p = x^p y^p$; en particulier, il est injectif. On notera k^p

l'image de ce morphisme (cf. 1.8.1), qui est donc un sous-corps de k. Par exemple, $k^p[t]$ désigne l'anneau des polynômes dont les coefficients sont des puissances p-ièmes.

L'application $x \mapsto x^{p^e}$ est l'itérée e-ième du Frobenius et peut se noter indifféremment Frob_{p^e} ou Frob_p^e. Son image se note bien sûr k^{p^e}.

1.7.2. Si k est un corps, et $f \in k[t]$ un polynôme en une indéterminée sur k, on dit que f est **séparable** lorsque f est premier avec sa dérivée f' : ceci revient à dire que les racines de f sont simples (=sans multiplicité) dans une extension où f est scindé (cf. 1.6.4). Lorsque f est de plus irréductible (sur k), dire qu'il est séparable signifie simplement que $f' \neq 0$ (puisque f' ne peut diviser f qu'en étant nulle).

Si k est de caractéristique 0, tout polynôme irréductible est séparable. Si k est de caractéristique $p > 0$, tout polynôme $f \in k[t]$ s'écrit de façon unique sous la forme $f(t) = f_0(t^{p^e})$ pour un certain $e \in \mathbb{N}$ et où $f_0' \neq 0$ (en effet, un polynôme de dérivée nulle n'a que des termes d'exposant multiple de p, et on itère) ; avec une telle écriture, si f est séparable alors $e = 0$, et si f est irréductible alors f_0 l'est aussi.

1.7.3. Le fait facile suivant reviendra très souvent : si $g \in k[t]$ où k est de caractéristique p, alors $g(t)^p = g^{\mathrm{Frob}}(t^p)$ où g^{Frob} désigne le polynôme obtenu en élevant chaque coefficient de g à la puissance p (c'est donc un élément de $k^p[t]$). En effet, si on appelle c_n le coefficient devant t^n dans g, on a $(c_n t^n)^p = (c_n)^p (t^n)^p$.

On a bien sûr de même $g(t)^{p^e} = g^{\mathrm{Frob}^e}(t^{p^e})$ où $g^{\mathrm{Frob}^e} \in k^{p^e}[t]$ désigne le polynôme obtenu en élevant chaque coefficient de g à la puissance p^e.

Lemme 1.7.4. Soit k un corps de caractéristique $p > 0$, et soit $h \in k[t]$ un polynôme tel que $h^i \in k^p[t]$ pour un certain $1 \leq i < p$. Alors $h \in k^p[t]$.

Démonstration. Comme i est premier avec p, on peut trouver une relation de Bézout $ui = 1 + vp$ avec $u, v \in \mathbb{N}$. On a alors $(h^i)^u = h \cdot (h^p)^v$ avec $h^i \in k^p[t]$ par hypothèse et $h^p \in k^p[t]$ d'après 1.7.3. On a donc $h \in k^p(t)$ (comme quotient de $(h^i)^u$ par $(h^p)^v$), et $h \in k[t]$, et il suffit d'appliquer la remarque (triviale mais importante) que si $k_0 \subseteq k$ est une extension de corps alors $k_0(t) \cap k[t] = k_0[t]$. ☺

Proposition 1.7.5. Soit k un corps de caractéristique $p > 0$, soit $f_0 \in k[t]$ unitaire irréductible, et soit $f(t) := f_0(t^{p^e})$ où $e > 0$. Alors f est réductible (i.e., n'est pas irréductible) si et seulement si les coefficients de f_0 (ou de façon équivalente, ceux de f) sont des puissances p-ièmes, i.e., si et seulement si $f_0 \in k^p[t]$. De plus, dans ce cas, f est en fait une puissance p-ième (cf. 1.7.3).

Démonstration. Si $f_0 \in k^p[t]$, disons $f_0 = (f_1)^{\mathrm{Frob}}$ (c'est-à-dire le polynôme obtenu en appliquant Frob_p coefficient par coefficient) avec $f_1 \in k[t]$, alors $f(t) = f_0(t^{p^e}) = (f_1(t^{p^{e-1}}))^p$ (cf. 1.7.3), donc f n'est pas irréductible.

Montrons la réciproque : supposons que les coefficients de f_0 ne soient pas tous des puissances p-ièmes, et on veut montrer que f est irréductible. Par récurrence, on se ramène au cas $e = 1$, c'est-à-dire $f(t) = f_0(t^p)$. Comme Frob_p est un isomorphisme entre k et k^p, il suffit de montrer que f^{Frob} est irréductible dans $k^p[t]$. Or on a $f^{\mathrm{Frob}} = f_0(t)^p$ comme au paragraphe précédent : dans $k[t]$, il s'agit d'une factorisation irréductible (car on a supposé f_0 irréductible) ; donc tout diviseur unitaire non-constant de f^{Frob} dans $k[t]$, et en particulier tout facteur irréductible de f^{Frob} dans $k^p[t]$, doit être de la forme f_0^i pour un certain $1 \leq i \leq p$. Mais si $f_0^i \in k^p[t]$ pour $i < p$, le lemme 1.7.4 montre que $f_0 \in k^p[t]$, et on a supposé le contraire : c'est donc que le seul facteur irréductible de f^{Frob} dans $k^p[t]$ est $f_0^p = f^{\mathrm{Frob}}$ lui-même, donc que f^{Frob} est irréductible dans $k^p[t]$ donc que f l'est dans $k[t]$. ☺

1.7.6. Lorsque $k \subseteq K$ est une extension de corps, un élément $x \in K$ algébrique sur k est dit **séparable** (sur k) lorsque son polynôme minimal l'est. D'après ce qu'on a dit ci-dessus, en caractéristique 0, tout algébrique est séparable ; et en caractéristique p, pour tout algébrique x il existe un e unique tel que x^{p^e} soit séparable et de degré égal à l'entier $\deg(x)/p^e$, et en particulier, si $\deg(x)$ n'est pas multiple de p, alors x est séparable.

On remarquera que si $k \subseteq k' \subseteq K$ est une tour d'extensions, un élément $x \in K$ séparable sur k est en particulier séparable sur k' (car son polynôme minimal sur k' divise celui sur k et un polynôme divisant un polynôme séparable est séparable).

Proposition 1.7.7. Soit $k \subseteq K$ une extension de corps de caractéristique $p > 0$, et $x \in K$ algébrique sur k. Exactement l'un des deux cas suivants se produit :

— soit x est séparable, le polynôme minimal de x^p sur k a des coefficients dans k^p, et alors $\deg(x^p) = \deg(x)$ et $k(x) = k(x^p)$,

— soit x n'est pas séparable, le polynôme minimal de x^p sur k a des coefficients qui ne sont pas tous dans k^p, et alors on a déjà vu $\deg(x^p) = \deg(x)/p$.

Démonstration. Soit f_0 le polynôme minimal de x^p sur k, et soit $f(t) = f_0(t^p)$, de sorte que $f \in k[t]$ annule x. D'après la proposition 1.7.5, deux cas peuvent se produire : soit les coefficients de f_0 sont des puissances p-ièmes auquel cas f est une puissance p-ième, soit f est irréductible dans $k[t]$. Dans le premier cas, disons $f = f_1^p$, alors $\deg(f_1) = \deg(f_0)$ et $f_1(x) = 0$, ce qui montre $\deg(x) \leq \deg(x^p)$, mais l'inclusion réciproque est évidente puisque $k(x^p) \subseteq k(x)$, et l'égalité des degrés montre l'égalité des corps. Dans le second cas, f est le polynôme minimal de x sur k, et on a $\deg(f) = p \cdot \deg(f_0)$ donc $\deg(x) = p \cdot \deg(x^p)$. ☺

1.7.8. On peut donner encore une autre condition équivalente au fait qu'un élément $x \in K$ algébrique sur un sous-corps k soit séparable (en caractéristique $p > 0$) :

on vient de voir que cela équivaut à $\deg(x^p) = \deg(x)$ ou à $k(x^p) = k(x)$; mais comme on a de toute manière $[k(x) : k] = [k^p(x^p) : k^p]$ (puisque le Frobenius est un isomorphisme entre $k(x)$ et $k^p(x^p)$), la séparabilité de x équivaut aussi à $[k(x^p) : k] = [k^p(x^p) : k^p]$, c'est-à-dire, d'après 1.4.8, au fait que les extensions $k^p(x^p)$ et k de k^p sont linéairement disjointes (cf. 1.4.1). C'est cette façon de voir les choses qui va inspirer l'énoncé et la démonstration de 1.7.10.

1.7.9. Une extension de corps $k \subseteq K$ algébrique est dite **séparable** (ou que K est séparable sur / au-dessus de k) lorsque tout élément de K est séparable sur k (cf. 1.7.6). C'est, bien sûr, toujours le cas en caractéristique 0.

Proposition 1.7.10. Soit $k \subseteq K$ une extension de corps *finie* de caractéristique p telle que K^p engendre K comme k-espace vectoriel. Alors K est séparable sur k.

Démonstration utilisant 1.4.8. On a $[K^p : k^p] = [K : k]$ car Frob est un isomorphisme de K sur K^p. Par hypothèse, $K = K^p.k$ (cf. 1.4.5 pour la notation, et cf. aussi 1.4.6) : ainsi, $[K^p.k : k] = [K^p : k^p]$, donc d'après 1.4.8 les extensions K^p et k de k^p sont linéairement disjointes. En particulier, si $y \in K$, les extensions $k^p(y^p)$ et k sont linéairement disjointes, ce qui d'après 1.7.8 implique que y est séparable sur k. ☺

Démonstration directe (déroulée). Soit $d = [K : k]$ et soit $x_1, \ldots, x_d$ une base de K comme k-espace vectoriel. Soit $y \in K$: on veut montrer que y est séparable sur k. Écrivons $y^j = \sum_{i=0}^{d-1} c_{i,j} x_i$ sur cette base, pour $0 \leq j \leq d' - 1$ avec $d' = \deg(y)$: le fait que y soit de degré d' entraîne que $1, y, \ldots, y^{d'-1}$ sont linéairement indépendants sur k, autrement dit la matrice des $c_{i,j}$ est de rang d'. Maintenant, en élevant $y^j = \sum_{i=0}^{d-1} c_{i,j} x_i$ à la puissance p, on trouve $y^{pj} = \sum_{i=0}^{d-1} c_{i,j}^p x_i^p$.

L'hypothèse que K^p engendre K comme k-espace vectoriel signifie que tout élément de K peut s'écrire comme combinaison linéaire d'éléments de K^p à coefficients dans k ; comme les éléments de K^p peuvent eux-mêmes s'écrire comme combinaisons linéaires des $x_1^p, \ldots, x_d^p$ à coefficients dans k^p (donc dans k), on voit que $x_1^p, \ldots, x_d^p$ engendrent K comme k-espace vectoriel, donc en sont une base (puisque $[K : k] = d$).

Or la matrice des $c_{i,j}^p$ est de rang d' car le Frobenius est un isomorphisme de k sur k^p et que *le rang d'une matrice ne dépend pas du corps sur lequel on la considère*. Des trois dernières phrases, on déduit que $1, y^p, \ldots, y^{p(d'-1)}$ sont linéairement indépendants sur k, c'est-à-dire que $\deg(y^p) \geq d'$, l'inégalité dans le sens contraire étant évidente on a $\deg(y^p) = \deg(y)$ et y est séparable. ☺

1.7.11. L'hypothèse « finie » est essentielle dans 1.7.10, et ne peut pas être remplacée par « algébrique » : un contre-exemple est fourni par $k = \mathbb{F}_p(t)$ et pour K la réunion des $\mathbb{F}_p(t^{1/p^i})$ pour $i \in \mathbb{N}$ (chaque $\mathbb{F}_p(t^{1/p^i})$ est un corps de fractions

rationnelles à une indéterminée t^{1/p^i}, plongé dans les suivants en identifiant t^{1/p^i} à $(t^{1/p^j})^{p^{j-i}}$ si $j \geq i$: on dit que K est la « clôture parfaite » de k, on l'obtient en prenant toutes les racines p^i-ièmes des éléments de k). Alors $k \subseteq K$ est une extension algébrique ; et K est un corps parfait (cf. 1.8.1), c'est-à-dire que $K^p = K$ (on l'a construit exprès pour), et a fortiori K^p engendre K comme k-espace vectoriel : pourtant, l'extension $k \subseteq K$ n'est aucunement séparable (elle est même « purement inséparable »).

Proposition 1.7.12. Soit $k \subseteq K$ une extension de corps. Si $x_1, \ldots, x_n$ sont des éléments de K tels que x_i est algébrique séparable sur $k(x_1, \ldots, x_{i-1})$ pour chaque $1 \leq i \leq n$, alors $k(x_1, \ldots, x_n)$ est séparable sur k.

Démonstration. En caractéristique 0, il n'y a rien à prouver : plaçons-nous en caractéristique $p > 0$.

Comme x_1 est séparable sur k, on a $k(x_1) = k(x_1^p)$; comme x_2 est séparable sur $k(x_1)$, on a $k(x_1, x_2) = k(x_1)(x_2) = k(x_1)(x_2^p) = k(x_1^p)(x_2^p) = k(x_1^p, x_2^p)$, et en procédant ainsi de suite on voit que $k(x_1, \ldots, x_n) = k(x_1^p, \ldots, x_n^p)$. L'hypothèse de 1.7.10 est donc vérifiée (les monômes en $x_1^p, \ldots, x_n^p$ engendrent $k(x_1, \ldots, x_n)$ comme k-espace vectoriel, cf. 1.3.6(1bis)), donc $k(x_1, \ldots, x_n)$ est séparable sur k. ☺

Corollaire 1.7.13. Soit $K = k(x_i)_{i \in I}$ avec les x_i algébriques séparables sur k. Alors tout K est (algébrique) séparable sur k. (Comparer avec 1.3.6(3).)

Concrètement, donc, les sommes, différences, produits et inverses de quantités algébriques séparables sur k sont algébriques séparables sur k.

Démonstration. Il s'agit de montrer que tout élément de K est séparable sur k : comme tout élément de $K = k(x_i)_{i \in I}$ s'écrit en utilisant un ensemble fini des x_i, i.e., appartient à $k(x_i)_{i \in J}$ pour $J \subseteq I$ fini (cf. 1.2.5), on peut supposer que J est fini, disons $J = \{1, \ldots, n\}$, bref $K = k(x_1, \ldots, x_n)$. Chaque x_i est séparable sur k donc *a fortiori* sur $k(x_1, \ldots, x_{i-1})$ et le résultat découle de 1.7.12. ☺

Corollaire 1.7.14. 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 (la réciproque est claire).

(Comparer avec 1.3.6(4).)

Démonstration. Si $y \in L$ et si $x_1, \ldots, x_n \in K$ sont les coefficients du polynôme minimal de y sur K, alors y est algébrique séparable sur $k(x_1, \ldots, x_n)$ et $x_1, \ldots, x_n$ sont séparables sur k : le résultat découle de 1.7.12. ☺

1.7.15. (Comparer avec 1.3.7.) La proposition 1.7.13 entraîne que si $k \subseteq K$ est une extension de corps, l'extension de k engendrée par tous les éléments de K

algébriques séparables sur k est tout simplement l'*ensemble* de tous les éléments de K algébriques séparables sur k, c'est-à-dire que cet ensemble est un corps, qui est manifestement la plus grande extension intermédiaire algébrique séparable sur k : on l'appelle la **fermeture [algébrique] séparable** de k dans K.

La fermeture séparable de k dans une clôture algébrique de k (cf. 1.6.6) s'appelle **clôture séparable** de k. Si k est égal à sa clôture séparable (i.e., séparablement fermé dans une clôture algébrique), on dit que k est **séparablement clos**.

1.7.16. Une extension algébrique $k \subseteq K$ telle que k soit égal à sa propre fermeture séparable dans K (i.e. séparablement fermé *dans* K) est dite **purement inséparable**. Dans ce cas, en notant $p > 0$ la caractéristique, le polynôme minimal sur k d'un élément quelconque de K est de la forme $t^{p^e} - c$ pour un $c \in k$ (car si f est le polynôme minimal de $x \in K$ et si $f(t) = f_0(t^{p^e})$ avec f_0 séparable comme d'habitude, l'élément $c := x^{p^e}$ de K est annulé par f_0 donc séparable sur k donc dans k, donc f_0 est de la forme $t - c$) ; et réciproquement, si cette condition est vérifiée, l'extension est purement inséparable (car un polynôme de la forme $t^{p^e} - c$ n'est séparable que pour $e = 0$).

1.7.17. On pourrait définir la notion de **degré séparable** d'une extension algébrique $k \subseteq K$, qui est le degré sur k de la fermeture séparable k' de k dans K, soit $[K : k]_{\mathrm{sep}} := [k' : k]$ (et dualement $[K : k]_{\mathrm{ins}} := [K : k']$ le **degré inséparable**). Les degrés séparables (et les degrés inséparables) se multiplient comme les degrés (cf. 1.3.5) : nous ne ferons pas la démonstration, mais le point-clé est que si $k \subseteq K$ est une extension purement inséparable (i.e., telle que k soit séparablement fermé dans K) et $K \subseteq K'$ une extension séparable, et si k' est la fermeture séparable de k dans K', alors $[k' : k] = [K' : K]$, c'est-à-dire que les extensions K et k' de k sont linéairement disjointes (cf. 1.4.8), ce qui se voit de façon analogue à 1.7.10.

1.8 Corps parfaits, théorème de l'élément primitif

Définition 1.8.1. Un corps k est dit **parfait** lorsque *soit* k est de caractéristique 0, *soit* k est de caractéristique p et le morphisme de Frobenius, $\mathrm{Frob}\colon x \mapsto x^p$, est surjectif $k \to k$, i.e. tout élément a une racine p-ième (automatiquement unique car Frob est injectif), ou si on préfère, $k^p = k$.

1.8.2. Ainsi, les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont parfaits (car de caractéristique 0). Il en va de même d'un corps fini $\mathbb{F}_q$ (car le morphisme de Frobenius, injectif d'un ensemble fini vers lui-même, est forcément surjectif). Enfin, un corps algébriquement clos est parfait (car le polynôme $x^p - c$ se scinde).

Un exemple de corps qui *n'est pas* parfait est le corps $\mathbb{F}_p(t)$ des fractions rationnelles en une indéterminée t sur $\mathbb{F}_p$, vu que l'élément t n'a pas de racine

p-ième.

1.8.3. Si k est parfait, tout élément x algébrique sur k (dans un corps le contenant) est séparable : ceci découle de la proposition 1.7.7.

Réciproquement, si tout élément x algébrique sur k (dans un corps le contenant, ou, mieux, dans une clôture algébrique K fixée) est séparable, alors k est parfait : en effet, si $x \in k$, on peut considérer y sa racine p-ième dans la clôture algébrique K : puisque $t^p - x = (t-y)^p$ dans $K[t]$, toutes ses racines sont égales à y, donc le polynôme minimal de y sur k est de la forme $(t-y)^r$ pour un certain $1 \leq r \leq p$, et s'il est séparable c'est que $r = 1$ donc $y \in k$.

Bien sûr, on peut aussi dire qu'un corps k est parfait si et seulement si toute extension algébrique de k est séparable (cf. 1.7.9 et 1.7.13).

Proposition 1.8.4. Si $k \subseteq K$ est une extension algébrique avec k parfait, alors K est aussi parfait.

Démonstration. D'après 1.8.3, il suffit de montrer que tout algébrique sur K est séparable. Mais un algébrique sur K est en particulier algébrique sur k (cf. 1.3.6(4)), donc de nouveau d'après 1.8.3 il est séparable sur k donc sur K. ☺

Proposition 1.8.5 (théorème de l'élément primitif)**.** Soit $K = k(x_1, \ldots, x_n)$ avec $x_1, \ldots, x_n$ algébriques sur k et $x_2, \ldots, x_n$ séparables sur k (on ne suppose pas que x_1 soit séparable). Alors l'extension $k \subseteq K$ est monogène, c'est-à-dire qu'il existe $y \in K$ tel que $K = k(y)$.

Démonstration. Si k est un corps fini, alors K l'est aussi (puisque K est fini sur k), et on peut choisir y un générateur du groupe cyclique $K^\times$ (vu que ses puissances sont tous les éléments de $K^\times$, il engendre certainement K en tant que corps). Excluons donc ce cas.

En procédant par récurrence sur n, on voit qu'il suffit de montrer le cas $n = 2$. Supposons donc $K = k(x_1, x_2)$ avec x_1, x_2 algébriques et x_2 séparable. On va poser $y = x_1 + cx_2$ et chercher à choisir judicieusement $c \in k$ non nul. Pour montrer que $K = k(y)$, il suffira de montrer que x_2 est dans $k(y)$, puisque ensuite $x_1 = y - cx_2$. Pour cela, on va s'intéresser au polynôme minimal de x_2 sur $k(y)$: il s'agit de montrer qu'il a degré 1 (pour c bien choisi).

Soient f_1 et f_2 les polynômes minimaux de x_1 et x_2 sur k. Travaillons dans L une extension de K dans laquelle $f_1 f_2$ est scindé (cf. 1.6.4). L'élément x_2 est racine de $f_2(t)$ et aussi de $g(t) := f_1(y - ct)$, ce dernier étant un polynôme en t à coefficients dans $k(y)$: il est donc racine de leur pgcd h dans $k(y)[t]$. Or toute racine de ce pgcd dans L est à la fois racine de f_2, appelons-la z_2, et aussi de la forme $(y - z_1)/c$ pour une certaine racine z_1 de f_1 ; on a donc $y = x_1 + cx_2 = z_1 + cz_2$, et si $z_2 \neq x_2$ cela implique $c = (z_1 - x_1)/(x_2 - z_2)$. Autrement dit, si on choisit pour c une valeur dans k différente de tous les

$(z_1 - x_1)/(x_2 - z_2)$ pour z_1 parcourant les racines de f_1 et z_2 parcourant celles de f_2 (autres que x_2), ce qui est possible vu que k est infini et qu'on n'exclut qu'un nombre fini de valeurs, alors la seule racine commune de f_2 et g est x_2. Comme de plus f_1 est séparable, cette racine est simple pour f_1 donc pour h, et ainsi x_2 est racine d'un polynôme h dans $k(y)$ ayant une unique seule racine, de surcroît simple, dans un corps L où ce polynôme se scinde (parce que f_2 s'y scinde). C'est donc que $x_2 \in k(y)$, et on a expliqué que cela conclut. ☺

Corollaire 1.8.6. Toute extension finie séparable est monogène. En particulier, toute extension finie d'un corps parfait est monogène.

Démonstration. Soit $k \subseteq K$ une extension finie séparable : d'après 1.3.6(2), elle est engendrée par un nombre fini d'éléments algébriques, ceux-ci sont séparables sur k par définition, et d'après 1.8.5, l'extension est monogène. Si k est parfait, toute extension algébrique de k est séparable. ☺

Proposition 1.8.7. Soit k un corps parfait et $k \subseteq K$ une extension de corps de type fini (cf. 1.2.4). Alors il existe $x_1, \ldots, x_{d+1} \in K$ tels que $K = k(x_1, \ldots, x_{d+1})$ avec $x_1, \ldots, x_d$ algébriquement indépendants sur k (cf. 1.5.1) et x_{d+1} algébrique séparable sur $k(x_1, \ldots, x_d)$ (cf. 1.7.6).

Démonstration. Supposons $K = k(w_1, \ldots, w_n)$ et soit $d = \deg.\,\mathrm{tr}_k(K)$: quitte à permuter les w_i, on peut supposer que $w_1, \ldots, w_d$ sont algébriquement indépendants sur K (cf. 1.5.4(1b)). Alors tout $y \in K$ est algébrique sur $k(w_1, \ldots, w_d)$, donc on peut écrire $f(w_1, \ldots, w_d, y) = 0$ avec $f \in k(t_1, \ldots, t_d)[u]$ irréductible, donc, quitte à chasser les dénominateurs, $f \in k[t_1, \ldots, t_d, u]$ irréductible (cf. 1.1.14).

En particulier, on peut trouver un tel polynôme $f \in k[t_1, \ldots, t_{d+1}]$ irréductible tel que $f(w_1, \ldots, w_{d+1}) = 0$. Considérons un tel polynôme.

Expliquons maintenant pourquoi il existe $1 \leq i \leq d+1$ tel que la dérivée partielle f'_i de f par rapport à la variable t_i ne soit pas identiquement nulle. En effet, si on avait $f'_i = 0$ pour chaque i, alors chaque variable t_i n'apparaîtrait qu'à des puissances multiples de la caractéristique $p > 0$, donc on pourrait écrire $f(t_1, \ldots, t_{d+1}) = f_0(t_1^p, \ldots, t_{d+1}^p)$. Quitte à considérer la racine p-ième de chaque coefficient de f_0 (qui existe car k est algébriquement clos), d'après 1.7.3 (ou son analogue évident à plusieurs variables), on voit que f serait une puissance p-ième, contredisant l'irréductibilité.

Les éléments $w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_{d+1}$ sont algébriquement indépendants sur i. En effet, le fait que $f'_i \neq 0$ assure que t_i apparaît vraiment dans $f(t_1, \ldots, t_{d+1})$ donc w_i est algébrique sur $k(w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_{d+1})$, donc le degré de transcendance de $k(w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_{d+1})$ sur k est le même que celui de $k(w_1, \ldots, w_{d+1})$, qui vaut d, or d éléments ne peuvent engendrer une

extension de degré de transcendance d qu'en étant algébriquement indépendants (cf. 1.5.4 (1a) et (3)).

Ainsi, quitte à permuter w_i avec w_{d+1} (si $i \neq d+1$), on peut s'arranger, tout en gardant $w_1, \ldots, w_d$ algébriquement indépendants, pour avoir $f'_{d+1} \neq 0$: ce fait assure que w_{d+1} est non seulement algébrique mais même séparable sur $k(w_1, \ldots, w_d)$.

Mais en procédant de même pour $w_{d+2}, \ldots, w_n$, on peut s'assurer (à chaque fois quitte à permuter le w_j considéré, $j \geq d+1$, avec un w_i pour $1 \leq i \leq d$) que chacun de $w_{d+1}, \ldots, w_n$ est algébrique séparable sur $k(w_1, \ldots, w_d)$, toujours avec $w_1, \ldots, w_d$ algébriquement indépendants. Posons $x_i = w_i$ pour $1 \leq i \leq d$. Le théorème 1.8.5 appliqué à l'extension de $k(x_1, \ldots, x_d) = k(w_1, \ldots, w_d)$ engendrée par les éléments algébriques séparables $w_{d+1}, \ldots, w_n$ montre que celle-ci est engendrée par un unique élément x_{d+1}, et comme cette extension est séparable d'après 1.7.13, l'élément x_{d+1} est séparable. ☺

1.9 Théorie de Galois : énoncé de résultats

1.9.1. Si K est un corps et L une extension algébrique de K deux éléments x, x' de L sont dits **conjugués** sur K lorsqu'ils ont le même polynôme minimal sur K, autrement dit, lorsque l'un est racine du polynôme minimal de l'autre (il s'agit d'une relation d'équivalence dont les classes sont parfois appelées **classes de conjugaison** au-dessus de K). De façon équivalente, deux éléments x, x' de L sont conjugués lorsque tout polynôme de $K[t]$ qui s'annule sur l'un s'annule aussi sur l'autre.

Les conjugués de $x \in L$ sont généralement considérés dans une clôture algébrique $K^{\mathrm{alg}} = L^{\mathrm{alg}}$ de L (donc de K) : l'intérêt de considérer la clôture algébrique est que le polynôme minimal de x sur K se scinde dans K^{alg}. Si x est de plus séparable (cf. 1.7.6), son polynôme minimal sur K est à racines simples dans K^{alg}, donc le nombre de conjugués de x sur K est égal à $\deg(x)$.

À titre d'exemple, les conjugués sur $\mathbb{Q}$ de $\sqrt{2}$ sont $\sqrt{2}$ et $-\sqrt{2}$; les conjugués sur $\mathbb{R}$ de $42+1729i$ sont lui-même et $42-1729i$; les conjugués sur $\mathbb{Q}$ de $\sqrt[3]{2}$ sont les $\zeta^r \sqrt[3]{2}$ pour $r \in \{0,1,2\}$ avec ζ une racine primitive cubique de l'unité (disons $\exp(2i\pi/3)$ dans les complexes) ; et les conjugués d'un $x \in \mathbb{F}_q$, pour $q = p^d$, au-dessus de $\mathbb{F}_p$, sont les $\mathrm{Frob}_p^r(x) = x^{p^r}$ pour $0 \leq r \leq d-1$.

1.9.2. Une extension de corps $K \subseteq L$ algébrique est dite **normale** lorsqu'elle vérifie les propriétés suivantes dont on peut montrer qu'elles sont équivalentes :

— (en notant L^{alg} une clôture algébrique de L,) 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 (i.e., il y a toutes ses racines),

— L est corps de décomposition (cf. 1.6.3) d'une famille de polynômes sur K,
— (en notant L^{alg} une clôture algébrique de L,) l'image de tout morphisme de corps $L \to L^{\mathrm{alg}}$ qui soit l'identité sur K est égale à L (et le morphisme définit donc un automorphisme de L qui soit l'identité sur K).

À titre d'exemple, $\mathbb{R} \subseteq \mathbb{C}$ ou $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ ou encore $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$ sont des extensions normales (ce sont les corps de décomposition de t^2+1, de t^2-2 et de $t^{p^d}-1$ respectivement) ; en revanche, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ *n'est pas* normale (il s'agit du corps de rupture de t^3-2, c'est une extension de degré 3, donc ne contenant pas de racine primitive cubique ζ de l'unité qui est algébrique de degré 2).

(On appelle **fermeture normale** de L au-dessus de K dans L^{alg} le corps de décomposition des polynômes minimaux sur K de tous les éléments de L, i.e., le sous-corps de L^{alg} engendré par tous les conjugués de tous les éléments de L, ou encore le composé, cf. 1.4.5, de tous les $\sigma(L)$ pour $\sigma\colon L \to L^{\mathrm{alg}}$ un morphisme de corps qui soit l'identité sur K. À titre d'exemple, la fermeture normale de $\mathbb{Q}(\sqrt[3]{2})$ au-dessus de $\mathbb{Q}$ est le corps $\mathbb{Q}(\zeta, \sqrt[3]{2})$ de décomposition de t^3-2.)

1.9.3. Une extension algébrique $K \subseteq L$ qui soit à la fois normale (cf. 1.9.2) et séparable (cf. 1.7.9) est dite **galoisienne**.

À titre d'exemple, une clôture séparable $K \subseteq K^{\mathrm{sep}}$ de K fournit une extension galoisienne (elle est séparable par définition, et elle est normale car un conjugué d'un élément séparable est séparable puisqu'ils ont le même polynôme minimal). On rappelle que si K est parfait, la clôture séparable coïncide avec la clôture algébrique.

1.9.4. Si $K \subseteq L$ est une extension galoisienne, on appelle **groupe de Galois** de l'extension, et on note $\mathrm{Gal}(K \subseteq L)$ l'ensemble des automorphismes de L au-dessus de K, ou K-automorphismes de L, c'est-à-dire l'ensemble des automorphismes de K-algèbres $L \to L$ (automorphismes de L = isomorphismes de L sur lui-même), c'est-à-dire encore l'ensemble des automorphismes de L qui soient l'identité sur K. Lorsque L est la clôture séparable de K, on dit que $\mathrm{Gal}(K \subseteq L)$ est le groupe de Galois **absolu** de K et on le note $\mathrm{Gal}(K)$ ou parfois Γ_K.

Les deux exemples suivant sont essentiels : le groupe de Galois de $\mathbb{R} \subseteq \mathbb{C}$ est le groupe à deux éléments formé de l'identité sur $\mathbb{C}$ et de la conjugaison complexe ; le groupe de Galois de $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$ est le groupe cyclique à d éléments formé des Frob_p^i pour $0 \leq i \leq d-1$.

On admet le théorème suivant, qui récapitule les résultats essentiels de la théorie de Galois :

Théorème 1.9.5. Soit $K \subseteq L$ une extension galoisienne et $G := \mathrm{Gal}(K \subseteq L)$ son groupe de Galois. Alors :

— si $K \subseteq L$ est finie, alors le groupe de Galois G est fini et son ordre $\#G$ est égal au degré $[L : K]$ de l'extension ; d'autre part,
— si $x \in L$ est fixé par tous les éléments du groupe de Galois G, alors x appartient à K (la réciproque fait partie de la définition même de G).

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

— Φ est une injection (décroissante pour l'inclusion), de l'ensemble des corps intermédiaires $K \subseteq E \subseteq L$ dans l'ensemble des sous-groupes de G,
— un inverse à gauche en est fourni par $H \mapsto \mathrm{Fix}(H) := \{x \in L : \forall \sigma \in H \ (\sigma(x) = x)\}$,
— si $K \subseteq L$ est finie, Φ est une bijection (en général, Φ a pour image l'ensemble des sous-groupes « fermés » pour une certaine topologie),
— $\Phi(E)$ est distingué dans G si et seulement si $K \subseteq E$ est galoisienne, et si c'est le cas $\mathrm{Gal}(K \subseteq E)$ est le quotient de $G = \mathrm{Gal}(K \subseteq L)$ par $\Phi(E) = \mathrm{Gal}(E \subseteq L)$,
— $\Phi(E_1.E_2)$ est l'intersection de $\Phi(E_1)$ et de $\Phi(E_2)$, et, si $K \subseteq L$ est finie, $\Phi(E_1 \cap E_2)$ est le sous-groupe de G engendré par $\Phi(E_1)$ et $\Phi(E_2)$ (en général, il s'agit de l'« adhérence » du sous-groupe qu'ils engendrent).

1.9.6. La partie la plus importante du résultat ci-dessus est la suivante : *si un élément de L (séparable et normal sur K) est fixé par le groupe G de tous les K-automorphismes de L, alors cet élément appartient à K*. Il s'agit donc d'une généralisation du fait qu'un complexe stable par conjugaison complexe est réel, et qu'un élément d'un corps fini stable par $\mathrm{Frob}_p\colon x \mapsto x^p$ appartient à $\mathbb{F}_p$.

Une des applications de la théorie de Galois est de montrer que certains objets définis *a priori* sur un « gros » corps L (par exemple la clôture séparable K^{sep} de K) sont, en fait, définis sur le « petit » corps K. Le slogan général s'énonce sous la forme

rationnel = stable par Galois

où « rationnel », dans ce contexte, signifie que l'objet est défini sur le « petit » corps K, et « stable par Galois » signifie que le groupe de Galois fixe l'objet considéré (pour une certaine action provenant de l'action naturelle sur L : par exemple, pour un polynôme, l'action sur les coefficients du polynôme).

1.9.7. Le groupe de Galois d'un polynôme séparable f sur un corps K est le groupe de Galois G du corps de décomposition (cf. 1.6.3) L de f : il s'agit bien d'une extension galoisienne, et par ailleurs, tout $\sigma \in G$ doit envoyer une racine de f sur une racine de f (puisque $\sigma(f(x)) = f(\sigma(x))$ vu que $f \in K[t]$), donc permute les racines de f, et en fait σ est complètement déterminé par cette permutation (puisque L est engendré par les racines de f, un automorphisme de

L est déterminé par son action sur les racines en question). On peut donc dire : *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*.

On peut montrer que la formulation suivante, peut-être plus intuitive, est encore équivalente : le groupe de Galois de f (séparable sur K) est le groupe de toutes les permutations σ des racines $x_1, \ldots, x_n$ de f (dans son corps de décomposition sur K) telles que si $h(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ est une quelconque « relation algébrique » entre les racines définie sur K, autrement dit, vérifie $h(x_1, \ldots, x_n) = 0$, alors on a encore $h(\sigma(x_1), \ldots, \sigma(x_n)) = 0$.

Une telle permutation doit certainement préserver la décomposition de f en facteurs irréductibles sur K (i.e., envoyer une racine d'un facteur irréductible sur une racine du même), et d'après 1.6.4(2b) il opère *transitivement* sur les racines de n'importe quel facteur irréductible, mais il n'est pas forcément évident de comprendre en quoi toute permutation n'est pas forcément possible au sein des racines d'un même polynôme irréductible, et il n'est pas non plus évident de *calculer* effectivement un groupe de Galois.

A minima, on retiendra que, pour L galoisienne sur K, les *orbites* de L sous l'action du groupe de Galois $G := \mathrm{Gal}(K \subseteq L)$ (c'est-à-dire les $\{\sigma(x) : \sigma \in G\}$ pour $x \in L$) sont exactement les classes d'équivalence pour la relation « être conjugués sur K » (cf. 1.9.1) ; ou, si on préfère, on a une bijection entre l'ensemble des polynômes unitaires irréductibles sur K qui se scindent dans L et l'ensemble L/G des orbites de L sous G, la bijection envoyant f sur l'ensemble de ses racines dans L.

1.9.8. Dans beaucoup de cas, le groupe de Galois d'un polynôme $f \in K[t]$ irréductible séparable de degré n est égal au groupe $\mathfrak{S}_n$ de toutes les permutations des racines de f (ceci se produit, bien sûr, exactement quand le corps de décomposition de f a pour degré $n!$ sur K).

Un exemple où ceci se produit est le polynôme $t^3 - 2$ sur $\mathbb{Q}$ dont le corps de décomposition est $\mathbb{Q}(\zeta, \sqrt[3]{2})$ (où ζ est racine primitive cubique de l'unité) qui a degré 6 sur $\mathbb{Q}$: toutes les permutations des racines $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$ est possible (i.e., définit un automorphisme du corps de décomposition).

Un exemple où ceci *ne* se produit *pas* est le polynôme $t^4 + t^3 + t^2 + t + 1$ sur $\mathbb{Q}$ dont les racines sont les racines primitives cinquièmes de l'unité : ici le corps de décomposition est égal au corps de rupture car dès qu'on a une racine ζ les autres sont de la forme ζ^i — cette même remarque prouve qu'un élément du groupe de Galois est déterminé par l'image de la seule racine ζ, et on peut se convaincre que le groupe est exactement $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

Terminons cette section par deux résultats dus à Emil Artin :

Théorème 1.9.9. Soit L un corps et G un groupe *fini* d'automorphismes de L : si $K := \mathrm{Fix}_L(G) := \{x \in L : \forall \sigma \in G \ (\sigma(x) = x)\}$ est le corps des éléments de L fixés par tous les éléments de G, alors $K \subseteq L$ est une extension galoisienne de groupe de Galois G (en particulier, $[L : K] = \#G$).

Démonstration. Soit $x \in L$ et $\sigma_1, \ldots, \sigma_r \in G$ un ensemble d'éléments de G tels que les $\sigma_i(x)$ soient toutes les images de x par les éléments de x chacune comptée exactement une fois. En particulier, si $\tau \in G$ alors $\tau\sigma_1(x), \ldots, \tau\sigma_r(x)$ sont une permutation de $\sigma_1(x), \ldots, \sigma_r(x)$. Par conséquent, τ permute les racines du polynôme $f(t) := \prod_{i=1}^{r}(t - \sigma_i(x))$, donc fixe ses coefficients, c'est-à-dire que $f \in K[t]$; et comme les $\sigma_i(x)$ sont distincts dans L, le polynôme f est séparable ; enfin, le degré de f est $r \leq n := \#G$.

On a donc montré que tout élément x de L est racine d'un polynôme sur K séparable de degré $\leq n := \#G$ et scindé sur L. Ceci montre que L est algébrique séparable et normale sur K, et même, que $[L : K] \leq n$ (car pour tous $x_1, \ldots, x_m \in L$ on a $K(x_1, \ldots, x_m) = K(x)$ pour un certain x d'après 1.8.5, donc on vient de voir que le degré de $K(x_1, \ldots, x_m)$ sur K est $\leq n$, et comme ceci est vrai pour tous $x_1, \ldots, x_m$, on a $[L : K] \leq n$). On a donc affaire à une extension $K \subseteq L$ galoisienne de degré $\leq n$; d'après 1.9.5, le groupe des K-automorphismes de L, ou groupe de Galois de $K \subseteq L$, a pour cardinal exactement $[L : K] \leq n$, et comme on a déjà $\#G = n$ automorphismes, tous ces nombres sont égaux, et $G = \mathrm{Gal}(K \subseteq L)$. ☺

1.9.10. L'intérêt du résultat ci-dessus est de construire des extensions galoisiennes d'intérêt géométrique.

Un exemple important est celui de l'action du groupe $\mathfrak{S}_n$ des permutations des indéterminées $t_1, \ldots, t_n$ sur le corps $L = k(t_1, \ldots, t_n)$ des fractions rationnelles en n indéterminées sur un corps k : si on appelle $K = \mathrm{Fix}_L(\mathfrak{S}_n)$ le corps des fractions rationnelles fixes par toutes les permutations des indéterminées, alors le théorème 1.9.9 assure que $K \subseteq L$ est galoisienne de groupe $\mathfrak{S}_n$ et en particulier $[L : K] = n!$; il est par ailleurs bien connu que K est une extension *transcendante pure* de k engendrée par les polynômes symétriques élémentaires $e_r := \sum_{i_1 < \cdots < i_r} t_{i_1} \cdots t_{i_r}$ des t_i. Le degré de n'importe quel t_i sur K est égal à n car il est racine du polynôme $t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n \in K[t]$, et on peut se convaincre que t_j est alors de degré $n - 1$ sur $K(t_i)$ et plus généralement que t_j est de degré $n - r$ sur $K(t_{i_1}, \ldots, t_{i_r})$ si $i_1, \ldots, i_r, j$ sont deux à deux distincts (en effet, les degrés ne peuvent pas être plus grands que ça, et ils ne peuvent pas être plus petits non plus puisque l'extension $K \subseteq L$ tout entière est de degré $n!$).

Théorème 1.9.11. Soit G un groupe ou même simplement un monoïde (=ensemble muni d'une opération binaire associative avec un élément unité), noté multiplicativement, et L un corps. Soient $\chi_1, \ldots, \chi_n$ des **caractères** de G

dans L, c'est-à-dire des morphismes $G \to L^\times$ (autrement dit, des applications $\chi\colon G \to L^\times$ telles que $\chi(1) = 1$ et $\chi(g_1 g_2) = \chi(g_1)\,\chi(g_2)$). On suppose que les $\chi_1, \dots, \chi_n$ sont deux à deux distincts. Alors en tant qu'applications $G \to L$, ils sont linéairement indépendants (c'est-à-dire que si $a_1\chi_1 + \cdots + a_n\chi_n = 0$ identiquement avec $a_1, \dots, a_n \in L$, alors tous les a_i sont nuls).

Démonstration. Si $n = 1$, le résultat est évident. Supposons qu'on ait une relation de dépendance linéaire $a_1\chi_1 + \cdots + a_n\chi_n = 0$ entre caractères distincts de G dans L, avec n aussi petit que possible : aucun des a_i n'est nul, et on vient de dire que $n \geq 2$. Puisque $\chi_1 \neq \chi_2$, il existe $u \in G$ tel que $\chi_1(u) \neq \chi_2(u)$. De $a_1\chi_1 + \cdots + a_n\chi_n = 0$ on tire $a_1\chi_1(ug) + \cdots + a_n\chi_n(ug) = 0$ pour tout $g \in G$, c'est-à-dire $a_1\chi_1(u)\,\chi_1 + \cdots + a_n\chi_n(u)\,\chi_n = 0$, et si on divise cette relation par $\chi_1(u)$ et qu'on soustrait la relation $a_1\chi_1 + \cdots + a_n\chi_n = 0$ d'origine, on trouve $a_2\big(\frac{\chi_2(u)}{\chi_1(u)} - 1\big)\chi_2 + \cdots + a_n\big(\frac{\chi_n(u)}{\chi_1(u)} - 1\big)\chi_n = 0$, une relation de dépendance linéaire entre $n-1$ caractères distincts, contredisant la minimalité de n. ☺

2 Le Nullstellensatz et les fermés de Zariski

2.1 Anneaux noethériens

2.1.1. Un idéal I d'un anneau A est dit **de type fini** (en tant qu'*idéal*) lorsqu'il est engendré (en tant qu'idéal !, c'est-à-dire en tant que sous-module de A) par un nombre fini d'éléments, autrement dit, $I = (x_1, \dots, x_n) := \{\sum_{i=1}^n a_i x_i : (a_1, \dots, a_n) \in A\}$ est l'ensemble des combinaisons A-linéaires de $x_1, \dots, x_n$ pour certains $x_1, \dots, x_n \in I$. Il revient à dire que I est de type fini en tant que sous-module de A.

Si c'est le cas, en fait, de toute famille $(y_i)_{i\in I}$ d'éléments qui engendrent I on peut extraire une sous-famille finie qui l'engendre. En effet, si I est engendré par $x_1, \dots, x_n$ et est aussi engendré par $(y_i)_{i\in I}$, alors l'écriture de chaque x_j comme combinaison A-linéaire des y_i ne fait intervenir qu'un nombre fini de ceux-ci, donc un nombre fini des y_i suffit à exprimer tous les x_j donc tous les éléments de I.

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

Remarquons qu'un *quotient* d'un anneau noethérien est noethérien. En effet, les idéaux de A/J sont de la forme I/J avec I un idéal de A contenant J, et si I est de type fini alors I/J l'est aussi (il est engendré par les classes modulo J des éléments qui engendrent I).

Proposition 2.1.3 (théorème 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.

Démonstration. Soit $I \subseteq A[t]$ un idéal. Supposons par l'absurde que I n'est pas de type fini. On construit par récurrence une suite $f_0, f_1, f_2, \ldots$ d'éléments de I comme suit. Si $f_0, \ldots, f_{r-1}$ ont déjà été choisis, comme l'idéal $(f_0, \ldots, f_{r-1})$ qu'ils engendrent n'est pas I, on peut choisir f_r de plus petit degré possible parmi les éléments de I non dans $(f_0, \ldots, f_{r-1})$.

Appelons c_i le coefficient dominant de f_i. Comme A est supposé noethérien, il existe m tel que $c_0, \ldots, c_{m-1}$ engendrent l'idéal J engendré par tous les c_i. Montrons qu'en fait $f_0, \ldots, f_{m-1}$ engendrent I (ce qui constitue une contradiction).

On peut écrire $c_m = a_0 c_0 + \cdots + a_{m-1} c_{m-1}$. Par ailleurs, le degré de f_m est supérieur ou égal au degré de chacun de $f_0, \ldots, f_{m-1}$ par minimalité de ces derniers. On peut donc construire le polynôme $g = \sum_{i=0}^{m-1} a_i f_i t^{\deg f_m - \deg f_i}$, qui a les mêmes degré et coefficient dominant que f_m, et qui appartient à $(f_0, \ldots, f_{m-1})$. Alors, $f_m - g$ est de degré strictement plus petit que f_m, il appartient à I mais pas à $(f_0, \ldots, f_{m-1})$: ceci contredit la minimalité dans le choix de f_m. ☺

Corollaire 2.1.4. Soit k un corps ou plus généralement un anneau noethérien. Alors l'anneau $k[t_1, \ldots, t_n]$ des polynômes en n indéterminées sur k est un anneau noethérien, et plus généralement toute k-algèbre de type fini (comme k-algèbre !) $k[x_1, \ldots, x_n]$ est un anneau noethérien.

Démonstration. La proposition précédente montre que si k est noethérien alors $k[t]$ est noethérien, et une récurrence immédiate montre que $k[t_1, \ldots, t_n]$ est noethérien. Or une k-algèbre de type fini est un quotient de $k[t_1, \ldots, t_n]$ (cf. 1.2.2), et on a expliqué qu'un quotient d'un anneau noethérien est noethérien. ☺

2.2 Idéaux maximaux d'anneaux de polynômes

Lemme 2.2.1. Soit k un corps algébriquement clos et $k \subseteq K$ une extension. On suppose que $h_1, \ldots, h_m \in k[t_1, \ldots, t_n]$ ont un zéro commun dans K (c'est-à-dire qu'il existe $z_1, \ldots, z_n \in K$ tels que $h_i(z_1, \ldots, z_n) = 0$ pour $1 \leq i \leq m$) : alors ils en ont un dans k (c'est-à-dire qu'il existe $y_1, \ldots, y_n \in k$ vérifiant $h_i(y_1, \ldots, y_n) = 0$ pour $1 \leq i \leq m$).

Démonstration. Quitte à remplacer K par $k(z_1, \ldots, z_n)$ où $z_1, \ldots, z_n$ est un zéro commun aux h_i, on peut supposer que K est une extension de type fini de k. D'après la proposition 1.8.7, comme k est parfait puisque algébriquement clos, on peut écrire $K = k(x_1, \ldots, x_d, u)$ avec $x_1, \ldots, x_d$ algébriquement indépendants et u algébrique sur $k(x_1, \ldots, x_d) =: k(\underline{x})$, disons $f(\underline{x}, u) = 0$ avec $f \in k(\underline{x})[t]$ le polynôme minimal de u sur $k(\underline{x})$.

Soient $z_1, \dots, z_n \in K$ vérifiant $h_i(z_1, \dots, z_n) = 0$. On peut écrire $z_j = g_j(\underline{x}, u)$ pour un certain $g_j \in k(\underline{x})[t]$. Le fait qu'on ait $h_i(z_1, \dots, z_n) = 0$ signifie $h_i(g_1, \dots, g_n) \equiv 0$ modulo f, autrement dit $h_i(g_1, \dots, g_n) = q_i f$ dans $k(\underline{x})[t]$.

Choisissons maintenant $v_1, \dots, v_d \in k$ qui n'annulent les dénominateurs d'aucun des coefficients d'aucun de f, g_j ou q_i ni le coefficient dominant de f (on laisse en exercice facile le fait que sur un corps infini, on peut trouver un n-uplet de points où n'importe quel ensemble fini de polynômes en n variables ne s'annule pas).

Remplaçons $x_1, \dots, x_d$ par $v_1, \dots, v_d$ dans l'écriture $h_i(g_1, \dots, g_n) = q_i f$: soient $\tilde{f}, \tilde{g}_j, \tilde{q}_i \in k[t]$ les polynômes ainsi substitués et soit $w \in k$ une racine de $\tilde{f}$ (noter que le degré de $\tilde{f}$ est le même que celui de f en la variable t puisque le coefficient dominant ne s'annule pas en $v_1, \dots, v_d$) : on a $h_i(\tilde{g}_1, \dots, \tilde{g}_n) = \tilde{q}_i \tilde{f}$, donc en évaluant en w ce polynôme, on trouve 0. Ceci montre que $x_j := \tilde{g}_j(w)$ répond au problème posé $h_i(x_1, \dots, x_n) = 0$. ☺

2.2.2. À titre d'exemple, si $h_1, \dots, h_m \in \mathbb{Q}[t_1, \dots, t_n]$ ont un zéro commun dans $\mathbb{C}$, alors ils en ont un dans l'ensemble $\mathbb{Q}^{\mathrm{alg}}$ des complexes algébriques sur $\mathbb{Q}$ (cf. 1.3.7 et 1.6.8).

2.2.3. Soit k un corps. On va s'intéresser aux idéaux

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

pour $(x_1, \dots, x_n) \in k^n$, et on va expliquer qu'ils sont maximaux (cf. 1.1.4).

Tout d'abord, expliquons pourquoi l'idéal $\mathfrak{m}_{(x_1,\dots,x_n)} := \{f \in k[t_1, \dots, t_n] : f(x_1, \dots, x_n) = 0\}$ est bien l'idéal $(t_1 - x_1, \dots, t_n - x_n)$ engendré par les $t_i - x_i$, puis on verra qu'il est maximal. Comme $t_i - x_i$ s'annule sur $(x_1, \dots, x_n)$, on a $\mathfrak{m}_{(x_1,\dots,x_n)} \supseteq (t_1 - x_1, \dots, t_n - x_n)$. Mais si un morphisme $k[t_1, \dots, t_n] \to R$ de k-algèbres envoie chaque $t_i - x_i$ sur 0, il envoie t_i sur x_i donc $f(t_1, \dots, t_n)$ sur $f(x_1, \dots, x_n)$ donc son noyau contient $\mathfrak{m}_{(x_1,\dots,x_n)}$, et en particulier ceci s'applique au morphisme de quotient par $(t_1 - x_1, \dots, t_n - x_n)$: donc $\mathfrak{m}_{(x_1,\dots,x_n)} \subseteq (t_1 - x_1, \dots, t_n - x_n)$ et on a égalité. De plus, comme le morphisme $k[t_1, \dots, t_n] \to k$ envoyant $f(t_1, \dots, t_n)$ sur $f(x_1, \dots, x_n)$ est surjectif vers un corps et a pour noyau $\mathfrak{m}_{(x_1,\dots,x_n)}$, ce dernier est un idéal maximal.

Proposition 2.2.4. Soit k un corps algébriquement clos. Les idéaux maximaux de $k[t_1, \dots, t_n]$ sont exactement les idéaux $\mathfrak{m}_{(x_1,\dots,x_n)} := \{f \in k[t_1, \dots, t_n] : f(x_1, \dots, x_n) = 0\}$ pour $(x_1, \dots, x_n) \in k^n$.

Démonstration. Si $\mathfrak{M}$ est un idéal maximal de $k[t_1, \dots, t_n]$, alors $K := k[t_1, \dots, t_n]/\mathfrak{M}$ est une extension du corps algébriquement clos k. Par ailleurs, d'après 2.1.4, on peut écrire $\mathfrak{M} = (h_1, \dots, h_m)$ pour certains polynômes

$h_1, \ldots, h_m \in k[t_1, \ldots, t_n]$. En notant $z_j \in K$ la classe de t_j modulo $\mathfrak{M}$, on a $h_i(z_1, \ldots, z_n) = 0$ dans K par définition. D'après 2.2.1, il existe donc $x_1, \ldots, x_n \in k$ tels que $h_i(x_1, \ldots, x_n) = 0$ pour chaque i. Ceci signifie que $h_i \in \mathfrak{m}_{(x_1,\ldots,x_n)}$ pour chaque i, donc que $\mathfrak{M} \subseteq \mathfrak{m}_{(x_1,\ldots,x_n)}$. Par maximalité de $\mathfrak{M}$, cette inclusion est en fait une égalité, ce qu'on voulait prouver. ☺

Proposition 2.2.5 (« lemme de Zariski »)**.** Soit k un corps et $k \subseteq K$ une extension de type fini *comme k-algèbre* (cf. 1.2.1) : alors K est en fait une extension *finie* (cf. 1.3.4).

Démonstration. Soit K^{alg} une clôture algébrique de K et k^{alg} la fermeture algébrique de k dans K^{alg} (cf. 1.3.7) qui est donc algébriquement close (cf. 1.6.8). Soient $z_1, \ldots, z_n \in K$ tels que $K = k[z_1, \ldots, z_n]$. Considérons le morphisme d'évaluation $k^{\mathrm{alg}}[t_1, \ldots, t_n] \to K^{\mathrm{alg}}$ envoyant f sur $f(z_1, \ldots, z_n)$: son image est $k^{\mathrm{alg}}[z_1, \ldots, z_n]$ (cf. 1.2.2).

Or $k^{\mathrm{alg}}[z_1, \ldots, z_n]$ est un *corps*, ce qui peut se voir d'après 1.4.6 (c'est le corps composé $k^{\mathrm{alg}}.K$), ou bien directement (si $u \in k^{\mathrm{alg}}[z_1, \ldots, z_n]$ n'est pas nul, les coefficients de son écriture en fonction de $z_1, \ldots, z_n$ appartiennent à une extension finie k' de k d'après 1.3.6(1), or $k'[z_1, \ldots, z_n]$ est un anneau intègre car il est inclus dans K^{alg}, et de dimension finie $\leq [k' : k]$ sur $k[z_1, \ldots, z_n] = K$ puisque engendré comme K-espace vectoriel par n'importe quel système générateur de k' comme k-espace vectoriel, donc d'après 1.1.13, $k'[z_1, \ldots, z_n]$ est un corps et ceci montre que u y est inversible).

Le paragraphe précédent implique que le noyau $\mathfrak{M}$ du morphisme d'évaluation est maximal. D'après la proposition précédente, $\mathfrak{M} = \mathfrak{m}_{(x_1,\ldots,x_n)}$ pour certains $(x_1, \ldots, x_n) \in k^{\mathrm{alg}}$, et le fait que $t_i - x_i \in \mathfrak{M}$ signifie exactement que $z_i = x_i$ dans K^{alg}, c'est-à-dire que finalement $z_1, \ldots, z_n$ appartiennent à k^{alg}, et 1.3.6(1) montre que $K = k[z_1, \ldots, z_n]$ est fini sur k. ☺

2.3 Le Nullstellensatz

2.3.1. Soit k un corps. On se pose la question de savoir si $h_1, \ldots, h_m \in k[t_1, \ldots, t_n]$ ont un zéro commun (un « zéro commun » étant un $(x_1, \ldots, x_n)$ dans k^n ou peut-être dans $(k^{\mathrm{alg}})^n$ tels que $h_i(x_1, \ldots, x_n) = 0$). Une chose est évidente : si $h_1, \ldots, h_m$ engendrent l'idéal unité, c'est-à-dire si on peut écrire $q_1 h_1 + \cdots + q_m h_m = 1$ pour certains $q_1, \ldots, q_m \in k[t_1, \ldots, t_n]$, alors $h_1, \ldots, h_m$ n'ont pas de zéro commun (ni dans k ni même dans k^{alg}) : en effet, en évaluant $q_1 h_1 + \cdots + q_m h_m = 1$ sur un hypothétique zéro commun on obtiendrait l'absurdité $0 = 1$.

Le résultat suivant affirme que, sur un corps algébriquement clos (ou si on cherche un zéro commun dans un corps algébriquement clos), c'est exactement le bon critère.

(« Nullstellensatz », de l'allemand « der Satz » = la phrase, le théorème, « die Stelle » = l'endroit, la place, « die Nullstelle » = le zéro d'une fonction ou d'un polynôme ; donc : « théorème du lieu d'annulation ».)

Proposition 2.3.2 (« 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 (il existe $x_1, \dots, x_n \in k$ tels que $h_i(x_1, \dots, x_n) = 0$ pour tout i).

Démonstration. Soit $\mathfrak{M}$ un idéal maximal contenant $(h_1, \dots, h_m)$ (qui existe d'après 1.1.7 puisque $(h_1, \dots, h_m)$ n'est pas l'idéal unité). D'après 2.2.4, il existe $x_1, \dots, x_n \in k$ tels que $\mathfrak{M} = \mathfrak{m}_{(x_1,\dots,x_n)}$, notamment $h_i \in \mathfrak{m}_{(x_1,\dots,x_n)}$ pour chaque i, et ceci signifie exactement $h_i(x_1, \dots, x_n) = 0$. ☺

Théorème 2.3.3 (« 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 $h_1, \dots, h_m$ (autrement dit si $h_i(x_1, \dots, x_n) = 0$ pour chaque i implique $g(x_1, \dots, x_n) = 0$) alors il existe $\ell \in \mathbb{N}$ tel que g^ℓ appartienne à l'idéal $(h_1, \dots, h_m)$ engendré par les h_i.

Démonstration. Le cas $g = 0$ est trivial, donc supposons le contraire.

Introduisons une nouvelle indéterminée u, et considérons les polynômes $h_1, \dots, h_m$ et $ug - 1$ dans $k[t_1, \dots, t_n, u]$. L'hypothèse signifie exactement qu'ils n'ont pas de zéro commun dans k^{n+1}. Le Nullstellensatz faible 2.3.2 implique donc qu'ils engendrent l'idéal unité de $k[t_1, \dots, t_n, u]$, c'est-à-dire qu'il existe $q_1, \dots, q_m, r \in k[t_1, \dots, t_n, u]$ tels que $q_1h_1 + \cdots + q_mh_m + r(ug - 1) = 1$. Remplaçons u par $\frac{1}{g} \in k(t_1, \dots, t_n)$ dans cette égalité : on a $\tilde{q}_1h_1 + \cdots + \tilde{q}_mh_m = 1$ où les $\tilde{q}_i \in k(t_1, \dots, t_n)$ sont les q_i ainsi substitués. Mais les $\tilde{q}_i$ admettent g^ℓ comme dénominateur commun (disons $\tilde{q}_i = p_i/g^\ell$ avec $p_i \in k[t_1, \dots, t_n]$) où ℓ est la plus grande puissance de u intervenant dans n'importe lequel des p_i. En chassant ces dénominateurs, on trouve $p_1h_1 + \cdots + p_mh_m = g^\ell$, ce qu'on voulait montrer. ☺

2.4 Fermés de Zariski

2.4.1. Un idéal $\mathfrak{r}$ d'un anneau A est dit **radical** lorsque l'anneau $A/\mathfrak{r}$ est réduit (cf. 1.1.8), c'est-à-dire que si $x^n \in \mathfrak{r}$ implique $x \in \mathfrak{r}$ (pour $x \in A$ et $n \in \mathbb{N}$).

La proposition 1.1.9 appliquée à un anneau quotient A/I se traduit de la façon suivante : l'ensemble des éléments dont une certaine puissance appartient à I est un idéal : cet idéal est aussi l'intersection des idéaux premiers de A contenant I ; et cet idéal est lui-même radical. On l'appelle le radical de l'idéal I et on le note $\sqrt{I}$.

Un idéal premier (cf. 1.1.3), et *a fortiori* un idéal maximal, est en particulier un idéal radical.

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

2.4.2. Si $\mathscr{F}$ est une partie de $k[t_1, \dots, t_d]$, on définit un ensemble $Z(\mathscr{F}) = \{(x_1, \dots, x_d) \in (k^{\mathrm{alg}})^d : (\forall f \in \mathscr{F})\, f(x_1, \dots, x_d) = 0\}$, autrement dit, l'ensemble des zéros communs dans k^{alg} de tous les éléments de $\mathscr{F}$.

Remarques évidentes : si $\mathscr{F} \subseteq \mathscr{F}'$ alors $Z(\mathscr{F}) \supseteq Z(\mathscr{F}')$ (la fonction Z est « décroissante pour l'inclusion ») ; on a $Z(\mathscr{F}) = \bigcap_{f \in \mathscr{F}} Z(f)$ (où $Z(f)$ est un raccourci de notation pour $Z(\{f\})$).

Si I est l'idéal engendré par $\mathscr{F}$ alors $Z(I) = Z(\mathscr{F})$ (car si tous les éléments de $\mathscr{F}$ s'annulent quelque part, toutes leurs combinaisons $k[t_1, \dots, t_n]$-linéaires s'annulent aussi). On peut donc se contenter de regarder les $Z(I)$ avec I idéal de $k[t_1, \dots, t_d]$. Encore un peu mieux : si $\sqrt{I} = \{f : (\exists n)\, f^n \in I\}$ désigne le radical de l'idéal I, on a $Z(\sqrt{I}) = Z(I)$ (car si f^n s'annule en un point alors f s'annule aussi) ; on peut donc se contenter de considérer les $Z(I)$ avec I idéal radical.

2.4.3. On appellera **fermé de Zariski** (défini sur k) dans $(k^{\mathrm{alg}})^d$ une partie E de la forme $Z(\mathscr{F})$ pour une certaine partie $\mathscr{F}$ de $k[t_1, \dots, t_d]$, dont on a vu qu'on pouvait supposer qu'il s'agit d'un idéal radical.

Un fermé de Zariski de la forme $Z(f)$ s'appelle une **hypersurface**.

Le vide est un fermé de Zariski ($Z(1) = \varnothing$) ; l'ensemble $(k^{\mathrm{alg}})^d$ tout entier est un fermé de Zariski ($Z(0) = (k^{\mathrm{alg}})^d$). Le singleton de tout $x \in k^d$ (à coordonnées dans k, donc) est un fermé de Zariski défini sur k : en effet, $Z(\mathfrak{m}_x) = \{x\}$, où $\mathfrak{m}_x$ est l'idéal $(t_1 - x_1, \dots, t_d - x_d)$ (cf. 2.2.3) où $x = (x_1, \dots, x_d)$, autrement dit le noyau de la fonction $f \mapsto f(x)$ d'évaluation en x.

Si $(E_i)_{i \in \Lambda}$ sont des fermés de Zariski, alors $\bigcap_{i \in \Lambda} E_i$ est un fermé de Zariski : plus précisément, si $(I_i)_{i \in \Lambda}$ sont des idéaux de $k[t_1, \dots, t_d]$, alors $Z(\sum_{i \in \Lambda} I_i) = \bigcap_{i \in \Lambda} Z(I_i)$. Si E, E' sont des fermés de Zariski, alors $E \cup E'$ est un fermé de Zariski : plus précisément, si I, I' sont des idéaux de $k[t_1, \dots, t_d]$, alors $Z(I \cap I') = Z(I) \cup Z(I')$ (l'inclusion $\supseteq$ est évidente ; pour l'autre inclusion, si $x \in Z(I \cap I')$ mais $x \notin Z(I)$, il existe $f \in I$ tel que $f(x) \neq 0$, et alors pour tout $f' \in I'$ on a $f(x)\, f'(x) = 0$ puisque $f f' \in I \cap I'$, donc $f'(x) = 0$, ce qui prouve $x \in Z(I')$).

2.4.4. Réciproquement, si E est une partie de $(k^{\mathrm{alg}})^d$, on note $\mathfrak{I}(E) = \{f \in k[t_1, \dots, t_d] : (\forall (x_1, \dots, x_d) \in E)\, f(x_1, \dots, x_d) = 0\}$ l'ensemble de tous les polynômes à coefficients dans k qui s'annulent partout sur E.

C'est un idéal de $k[t_1, \dots, t_d]$ (car si des polynômes s'annulent sur E, toutes leurs combinaisons $k[t_1, \dots, t_n]$-linéaires s'y annulent aussi), et même un idéal radical (car si f^n s'annule sur E alors f s'annule aussi).

Remarques évidentes : si $E \subseteq E'$ alors $\mathfrak{I}(E) \supseteq \mathfrak{I}(E')$ (la fonction $\mathfrak{I}$ est « décroissante pour l'inclusion ») ; on a $\mathfrak{I}(E) = \bigcap_{x \in E} \mathfrak{M}_x$ (où $\mathfrak{M}_x$ désigne l'idéal maximal $\mathfrak{I}(\{x\})$ des polynômes s'annulant en x — attention car x n'est

pas forcément dans k^d ici), et en particulier $\mathfrak{I}(E) \neq k[t_1, \ldots, t_d]$ dès que $E \neq \varnothing$.

On a de façon triviale $\mathfrak{I}(\varnothing) = k[t_1, \ldots, t_d]$. De façon un peu moins évidente, on a $\mathfrak{I}((k^{\mathrm{alg}})^d) = (0)$ (démonstration par récurrence sur d, laissée en exercice).

2.4.5. Lorsque $E \subseteq (k^{\mathrm{alg}})^d$ et $\mathscr{F} \subseteq k[t_1, \ldots, t_d]$, on a $E \subseteq Z(\mathscr{F})$ ssi $\mathscr{F} \subseteq \mathfrak{I}(E)$, puisque les deux signifient « tout polynôme dans $\mathscr{F}$ s'annule en tout point de E ».

En particulier, en appliquant cette remarque à $\mathscr{F} = \mathfrak{I}(E)$, on a $E \subseteq Z(\mathfrak{I}(E))$ pour toute partie E de $(k^{\mathrm{alg}})^d$; et en appliquant la remarque à $E = Z(\mathscr{F})$, on a $\mathscr{F} \subseteq \mathfrak{I}(Z(\mathscr{F}))$. De $E \subseteq Z(\mathfrak{I}(E))$ on déduit $\mathfrak{I}(E) \supseteq \mathfrak{I}(Z(\mathfrak{I}(E)))$ (car $\mathfrak{I}$ est décroissante), mais par ailleurs $\mathfrak{I}(E) \subseteq \mathfrak{I}(Z(\mathfrak{I}(E)))$ en appliquant l'autre inclusion à $\mathfrak{I}(E)$: donc $\mathfrak{I}(E) = \mathfrak{I}(Z(\mathfrak{I}(E)))$ pour toute partie E de $(k^{\mathrm{alg}})^d$; de même, $Z(\mathscr{F}) = Z(\mathfrak{I}(Z(\mathscr{F})))$ pour tout ensemble $\mathscr{F}$ de polynômes.

Une partie E de $(k^{\mathrm{alg}})^d$ vérifie $E = Z(\mathfrak{I}(E))$ si et seulement si elle est de la forme $Z(\mathscr{F})$ pour un certain $\mathscr{F}$ (= : c'est un fermé de Zariski défini sur k), et dans ce cas on peut prendre $\mathscr{F} = \mathfrak{I}(E)$, qui est un idéal radical.

Reste à comprendre quels sont les idéaux I de $k[t_1, \ldots, t_d]$ qui vérifient $I = \mathfrak{I}(Z(I))$. Lorsque k est algébriquement clos, le *Nullstellensatz fort* (cf. 2.3.3) affirme que $\mathfrak{I}(Z(I)) = \sqrt{I}$. Pour en déduire le résultat pour k quelconque, on aura besoin du lemme suivant :

Lemme 2.4.6. Soit k un corps et $k \subseteq k'$ une extension quelconque. Soit I un idéal de $k[t_1, \ldots, t_d]$. Soit I' l'idéal engendré par I dans $k'[t_1, \ldots, t_d]$ (c'est simplement le k'-espace vectoriel engendré par I) : alors $I' \cap k[t_1, \ldots, t_d] = I$.

Démonstration. Soit $(v_i)_{i \in \Lambda}$ une base de k' comme k-espace vectoriel contenant l'élément $v_0 := 1$: alors (v_i) est aussi une base de $k'[t_1, \ldots, t_d]$ comme $k[t_1, \ldots, t_d]$-module. L'idéal I' contient l'ensemble $I^* := \bigoplus_{i \in \Lambda} v_i I$ des éléments de $k'[t_1, \ldots, t_d]$ dont toutes les coordonnées sur cette base appartiennent à I, qui est bien le k'-espace vectoriel engendré par I ; or on vérifie facilement que cet ensemble I^* est un idéal (le produit d'un élément de I^* par un élément de $k'[t_1, \ldots, t_d]$ est dans I^* car si $f \in I$ et $g \in k[t_1, \ldots, t_d]$ alors $(v_i f) \cdot (v_j g) = (v_i v_j) f g$ appartient à I^* puisque $v_i v_j$ s'écrit comme combinaison k-linéaire des v_ℓ), donc en fait $I' = I^*$. Si un élément de I^* appartient à $k[t_1, \ldots, t_d]$, c'est que toutes ses coordonnées sur la base (v_i) sont 0 sauf sur v_0, donc il appartient bien à I. ☺

Proposition 2.4.7. Soit k un corps et k^{alg} une clôture algébrique. On utilise les notations Z et $\mathfrak{I}$ introduites en 2.4.2 et 2.4.4.

Si I est un idéal de $k[t_1, \ldots, t_d]$, alors $\mathfrak{I}(Z(I))$ est le radical $\sqrt{I}$ de I. Si E est une partie de $(k^{\mathrm{alg}})^d$, alors $Z(\mathfrak{I}(E))$ est le plus petit (pour l'inclusion) fermé de Zariski défini sur k qui contient E.

De plus, les fonctions Z et $\mathfrak{I}$ définissent des bijections réciproques décroissantes (pour l'inclusion) entre idéaux radicaux de $k[t_1, \ldots, t_d]$ et fermés de Zariski de $(k^{\mathrm{alg}})^d$ définis sur k.

Démonstration. Si I est un idéal de $k[t_1,\dots,t_d]$, on a vu que $\mathfrak{I}(Z(I)) \supseteq I$ et $\mathfrak{I}(Z(I))$ est radical, donc $\mathfrak{I}(Z(I)) \supseteq \sqrt{I}$. Réciproquement, si $g \in \mathfrak{I}(Z(I))$, alors (quitte à prendre $h_1,\dots,h_m$ qui engendrent I, cf. 2.1.4) le théorème 2.3.3 montre que g^ℓ, pour un certain $\ell \in \mathbb{N}$, appartient à l'idéal I' engendré par I dans $k^{\mathrm{alg}}[t_1,\dots,t_d]$ (c'est-à-dire engendré par $h_1,\dots,h_m$ dans $k^{\mathrm{alg}}[t_1,\dots,t_d]$). Comme $g^\ell \in k[t_1,\dots,t_d]$, le lemme précédent montre $g^\ell \in I$, et on a bien prouvé $g \in \sqrt{I}$. Donc finalement $\mathfrak{I}(Z(I)) = \sqrt{I}$.

Si E est une partie de $(k^{\mathrm{alg}})^d$, on a vu que $Z(\mathfrak{I}(E)) \supseteq E$, donc $Z(\mathfrak{I}(E))$ est un fermé de Zariski contenant E ; mais si $Z(\mathscr{F})$ est un fermé de Zariski contenant E, soit $Z(\mathscr{F}) \supseteq E$, alors $Z(\mathscr{F}) = Z(\mathfrak{I}(Z(\mathscr{F}))) \supseteq Z(\mathfrak{I}(E))$, donc $Z(\mathfrak{I}(E))$ est bien le plus petit fermé de Zariski contenant E.

Si I est un idéal radical, $Z(I)$ est un fermé de Zariski, et on vient de voir que $\mathfrak{I}(Z(I)) = I$; et si $E = Z(\mathscr{F})$ est un fermé de Zariski, $\mathfrak{I}(E)$ est un idéal radical, et on a vu que $Z(\mathfrak{I}(E)) = Z(\mathfrak{I}(Z(\mathscr{F}))) = Z(\mathscr{F}) = E$. Ceci montre bien que Z et $\mathfrak{I}$ sont des bijections réciproques entre les ensembles qu'on a dit, et on a observé qu'elles sont décroissantes. ☺

2.4.8. (1) On aurait pu être tenté d'associer dès le départ à $\mathscr{F}$ l'ensemble $Z(\mathscr{F}) \cap k^d$ des zéros dans k^d, plutôt que $(k^{\mathrm{alg}})^d$, des éléments de $\mathscr{F}$: le problème avec ce point de vue est qu'on peut avoir $Z(I) \cap k^d = \varnothing$ alors que I n'est pas l'idéal unité : penser au cas de l'idéal engendré par t^2+1 dans $\mathbb{R}[t]$ (qui n'est pas l'idéal unité puisque t^2+1 n'est pas inversible, et qui n'a pourtant pas de zéro dans $\mathbb{R}$). Avec le point de vue choisi ici, on a $Z(t^2+1) = \{\pm\sqrt{-1}\} \subseteq \mathbb{C}$. On remarquera bien que $\{\sqrt{-1}\}$ seul n'est pas un fermé de Zariski défini sur $\mathbb{R}$ (c'est, en revanche, un fermé de Zariski défini sur $\mathbb{C}$).

Lorsqu'on a besoin de désigner les éléments de $Z(I) \cap k^d$, c'est-à-dire les solutions dans k^d, on dira que ce sont les **points rationnels** du fermé de Zariski $Z(I)$: cette terminologie vient de la situation $k = \mathbb{Q}$ et a été étendue à n'importe quel corps. (À titre d'exemple, $(\frac{4}{5},\frac{3}{5})$ est un point rationnel du « cercle » $Z(x^2+y^2-1)$ sur $\mathbb{Q}$, cf. 3.1.4.) D'après le théorème 1.9.5 (cf. surtout 1.9.6), si k est parfait (cf. 1.8.1 et 1.8.3), on peut dire que les points rationnels de $Z(I)$ sont ceux qui sont fixés par le groupe de Galois absolu, i.e., par tous les automorphismes de k^{alg} au-dessus de k.

(2) Par opposition à « point rationnel », un élément de $Z(I)$ peut s'appeler un **point géométrique** : de façon générale, le terme « géométrique » a souvent la signification « défini sur la clôture algébrique ». Les points géométriques (=solutions d'équations polynomiales *dans la clôture algébrique*) sont donc ceux avec lesquels nous avons travaillé tout du long de cette section.

(3) On parle enfin de **point fermé** pour désigner les $Z(\mathfrak{m})$ avec $\mathfrak{m}$ un idéal *maximal* de $k[t_1,\dots,t_d]$ contenant I (si $I \neq (1)$, il y en a toujours d'après 1.1.7) : on a vu en 2.2.4 que si k est algébriquement clos, les points maximaux coïncident

avec les [singletons des] points géométriques=rationnels ; mais en général, ce ne sont pas toujours des singletons (par exemple, en une seule variable t, le fermé de Zariski $Z(t^2+1)$ sur $\mathbb{R}$ est un point fermé qui contient deux points géométriques, $\pm\sqrt{-1}$). La terminologie « point fermé » vient de ce que ce sont des *fermés* de Zariski définis sur k qui soient aussi petits que possible.

Le corps $k[t_1,\dots,t_d]/\mathfrak{m}$ s'appelle **corps résiduel** du point fermé $Z(\mathfrak{m})$, souvent noté $\varkappa_\mathfrak{m}$, et la classe modulo $\mathfrak{m}$ d'un polynôme s'appelle **évaluation** du polynôme au point fermé en question. (Dans le cas [du singleton] d'un point rationnel, l'évaluation est bien l'évaluation au sens usuel.) Remarquons que si $\varkappa_\mathfrak{m}=k$ alors le point fermé est [le singleton d'un point] rationnel (voir la fin de la démonstration de 2.2.4). En général, le degré $[\varkappa_\mathfrak{m}:k]$ s'appellera **degré** du point fermé $Z(\mathfrak{m})$.

Les points rationnels sont des points fermés particuliers (sur un corps algébriquement clos, ce sont les seuls, comme on vient de le rappeler), et chaque point géométrique x appartient à un unique point fermé (considérer $Z(\mathfrak{I}(x))$ dans 2.4.7), et on peut vérifier que si k est parfait, les points fermés sont exactement les *orbites* sous le groupe de Galois absolu (comparer avec 1.9.7).

2.4.9. Si I est un idéal radical de $k[t_1,\dots,t_d]$ si bien que $\mathfrak{I}(Z(I))=I$ comme on vient de le voir en 2.4.7, on peut donner une interprétation de $k[t_1,\dots,t_d]/(I)$ comme suit :

Considérons l'application qui à un polynôme $f\in k[t_1,\dots,t_d]$ associe la restriction à $Z(I)$ de ce polynôme, vu comme une application de $(k^{\mathrm{alg}})^d$ vers k^{alg} ; autrement dit,

$$\begin{aligned} k[t_1,\dots,t_d] &\to (k^{\mathrm{alg}})^{Z(I)} \\ f &\mapsto ((x_1,\dots,x_d)\mapsto f(x_1,\dots,x_d)) \end{aligned}$$

Il s'agit manifestement d'un morphisme d'anneaux (en munissant $(k^{\mathrm{alg}})^{Z(I)}$ des opérations point à point) dont le noyau est $\mathfrak{I}(Z(I))$ par définition. Il s'ensuit que son image, c'est-à-dire les restrictions à $Z(I)$ des polynômes dans $k[t_1,\dots,t_d]$, s'identifie à $k[t_1,\dots,t_d]/\mathfrak{I}(Z(I))$, c'est-à-dire $k[t_1,\dots,t_d]/I$. Cet anneau quotient s'appelle l'**anneau des fonctions régulières** du fermé de Zariski $Z(I)$ (une fonction régulière est donc simplement la restriction d'un polynôme).

2.4.10. On dit qu'un fermé de Zariski $Z(I)$ est **irréductible** lorsqu'il ne peut pas s'écrire comme réunion de deux fermés de Zariski différents de lui, i.e., si $Z(I)=Z(I_1)\cup Z(I_2)$ alors $Z(I_1)=Z(I)$ ou bien $Z(I_2)=Z(I)$.

À titre de contre-exemple, $Z(xy)=Z(x)\cup Z(y)$ (car xy s'annule si et seulement si x s'annule ou y s'annule) n'est pas irréductible dans le plan de coordonnées (x,y) : c'est la réunion des deux axes de coordonnées ; le problème

vient du fait que le polynôme xy n'est pas irréductible, ou de façon équivalente (cf. 1.1.5) que l'idéal qu'il engendre n'est pas premier. Ce contre-exemple suggère le résultat suivant :

Proposition 2.4.11. Un fermé de Zariski $Z(I)$, avec I un idéal radical, est irréductible si, et seulement si, l'idéal I est premier (i.e., l'anneau des fonctions régulières sur $Z(I)$ est intègre).

En particulier, un fermé de Zariski de la forme $Z(f)$ (c'est-à-dire, une *hypersurface*) est irréductible si et seulement si f est nul ou irréductible.

Démonstration. Supposons I premier (donc automatiquement radical) : on veut montrer que $Z(I)$ est irréductible. Supposons $Z(I) = Z(I_1) \cup Z(I_2)$ avec I_1, I_2 deux idéaux radicaux : on veut montrer que $Z(I_1) = Z(I)$ ou $Z(I_2) = Z(I)$. Supposons le contraire, c'est-à-dire d'après la proposition 2.4.7 que $I \neq I_1$ et $I \neq I_2$. Il existe alors $f_1 \in I_1 \setminus I$ et $f_2 \in I_2 \setminus I$. On a alors $f_1 f_2 \notin I$ car I est premier, et pourtant $f_1 f_2$ s'annule sur $Z(I_1)$ et $Z(I_2)$ donc sur $Z(I)$, une contradiction à 2.4.7.

Réciproquement, supposons $Z(I)$ irréductible : on veut montrer que I est premier. Soient f_1, f_2 tels que $f_1 f_2 \in I$: posons $I_1 := I + (f_1)$ et $I_2 := I + (f_2)$ les idéaux engendrés par I et f_1, f_2 respectivement. On a $Z(I_1) \subseteq Z(I)$ et $Z(I_2) \subseteq Z(I)$, et plus précisément $Z(I_1) = Z(I) \cap Z(f_1)$ et $Z(I_2) = Z(I) \cap Z(f_2)$ (on a signalé que Z transforme les sommes d'idéaux en intersections) ; on a par ailleurs $Z(I) = Z(I_1) \cup Z(I_2)$ (car si $x \in Z(I)$ alors $f_1(x)\, f_2(x) = 0$ donc soit $f_1(x) = 0$ soit $f_2(x) = 0$, et dans le premier cas $x \in Z(I_1)$ et dans le second $x \in Z(I_2)$). Puisqu'on a supposé $Z(I)$ irréductible, on a, disons, $Z(I_1) = Z(I)$, c'est-à-dire $Z(I) \subseteq Z(f_1)$, ce qui signifie $f_1 \in I$ d'après 2.4.7. Ceci montre bien que I est premier.

L'affirmation du dernier paragraphe est une conséquence de ce qu'on a dit en 1.1.5 (et du fait que $k[t_1, \ldots, t_d]$ est factoriel, cf. 1.1.14). ☺

2.4.12. Il est important de noter qu'un polynôme $f \in k[t_1, \ldots, t_n]$ peut être irréductible mais cesser de l'être quand on le considère à coefficients dans un corps plus gros (notamment, tout polynôme de degré > 1 en $n = 1$ variable se factorise dans k^{alg}). Lorsque ceci *ne* se produit *pas*, on dit que le polynôme est **géométriquement irréductible** ou **absolument irréductible**. Plus précisément :

- Un polynôme $f \in k[t_1, \ldots, t_n]$ est dit géométriquement (ou absolument) irréductible lorsque f est irréductible dans $k^{\mathrm{alg}}[t_1, \ldots, t_n]$. Ceci implique, évidemment, qu'il est irréductible. En $n = 1$ variable, les seuls polynômes géométriquement irréductibles sont ceux de degré 1.
- Un fermé de Zariski $Z(I)$ avec I idéal radical de $k[t_1, \ldots, t_n]$ est dit géométriquement (ou absolument) irréductible lorsque l'idéal $I.k^{\mathrm{alg}}$ engendré par I (comme k^{alg}-espace vectoriel ou comme idéal, cela revient

au même, cf. 2.4.6) dans $k^{\mathrm{alg}}[t_1, \ldots, t_n]$ est premier. Notamment, si $I = (f)$ est principal (engendré par un unique polynôme), cela signifie exactement que f est soit nul soit géométriquement irréductible.

(On renvoie à 3.1.9 pour un exemple illustrant ces notions.)

2.4.13. Si I est un idéal premier de $k[t_1, \ldots, t_d]$, si bien que $Z(I)$ est un fermé de Zariski irréductible d'après 2.4.11, on appelle **corps des fonctions rationnelles** du fermé de Zariski $Z(I)$ le corps des fractions (cf. 1.1.10) de l'anneau $k[t_1, \ldots, t_d]/I$ des fonctions régulières (cf. 2.4.9) sur $Z(I)$ (cet anneau étant intègre justement car I est premier).

Concrètement, puisque $k[t_1, \ldots, t_d]/I$ peut se voir comme les restrictions à $Z(I)$ des fonctions polynomiales sur $Z(I)$, il s'agit du corps des expressions de la forme f/g avec f, g deux telles fonctions et $g \neq 0$ (noter que g peut s'annuler en certains points de $Z(I)$ mais ne s'y annule pas *identiquement*).

Le degré de transcendance sur k de ce corps s'appellera la **dimension** du fermé de Zariski (irréductible) $Z(I)$.

2.5 Extension des scalaires des algèbres sur un corps

2.5.1. Soit $k \subseteq k'$ une extension de corps et A une k-algèbre : on voudrait associer à A une k'-algèbre A' obtenue en « étendant les scalaires » de k à k' (les « scalaires », dans cette expression, sont les éléments de k).

2.5.2. Soit $k \subseteq k'$ une extension de corps et V un k-espace vectoriel. Soit $(e_i)_{i\in I}$ une base de V et V' le k'-espace vectoriel de base $(e_i)_{i\in I}$ (c'est-à-dire l'ensemble des combinaisons linéaires formelles $\sum_{i\in I} \lambda_i e_i$ avec $\lambda_i \in k'$ tous nuls sauf un nombre fini). On a une application k-linéaire $V \to V'$ « naturelle » qui envoie e_i sur e_i (donc $\sum_{i\in I} \lambda_i e_i$ avec $\lambda_i \in k$ sur la même somme où les λ_i sont maintenant considérés dans k') ; cette application est, bien entendue, injective, et son image engendre V' comme k'-espace vectoriel (puisqu'elle contient les e_i). Appelons-la $\iota\colon V \to V'$.

Alors, quel que soit le k'-espace vectoriel W, toute application k-linéaire $u\colon V \to W$ se factorise de façon unique à travers ι, c'est-à-dire qu'il existe une unique application k'-linéaire $u'\colon V' \to W$ telle que $u = u' \circ \iota$. Ou, si on préfère, l'application $\mathrm{Hom}_{k'}(V', W) \to \mathrm{Hom}_k(V, W)$ de composition à droite par ι, qui à une application k'-linéaire $u'\colon V' \to W$ associe l'application k-linéaire $u\colon V \to W$ donnée par $u \circ \iota$, est une bijection. Il suffit pour s'en convaincre de se rappeler que $\mathrm{Hom}_k(V, W)$ et $\mathrm{Hom}_{k'}(V', W)$ peuvent tous les deux s'identifier à W^I (l'ensemble des fonctions de I dans W) grâce au choix de la base $(e_i)_{i\in I}$: autrement dit, on doit poser $u'(e_i) = u(e_i)$, et ceci construit bien u'. On pourra dire qu'il s'agit là d'une « propriété universelle » de V'.

En particulier, *la construction effectuée de V' ne dépend pas du choix de*

la base : si on construit V_1' et V_2' en utilisant deux bases différentes de V, non seulement on obtient deux espaces vectoriels isomorphes, mais il y a un *unique* isomorphisme entre eux qui soit compatible avec les applications $\iota_1 \colon V \to V_1'$ et $\iota_2 \colon V \to V_2'$ construites en même temps.

Cet espace V' s'appelle l'**extension des scalaires** de V de k à k' et se note $V \otimes_k k'$. Sa dimension sur k' est, par construction, égale à la dimension de V sur k. On notera $x \otimes 1$ l'élément $\iota(x)$ défini ci-dessus (dont les coordonnées sur la base e_i sont celles de x), et plus généralement $x \otimes c$ pour $c \in k'$ l'élément $c\iota(x)$ dont les coordonnées sur la base e_i sont celles de x multipliées par c.

2.5.3. La « propriété universelle » de ι permet d'associer à une application k-linéaire $u \colon V \to W$ entre k-espaces vectoriels une application k'-linéaire $u' \colon V' \to W'$ entre leurs extensions des scalaires $V' := V \otimes_k k'$ et $W' := W \otimes_k k'$. À savoir : on considère $\iota_W \circ u$ (où $\iota_W \colon W \to W'$ est $x \mapsto x \otimes 1$ pour $x \in W$) et la propriété universelle de ι_V assure qu'on peut l'écrire de façon unique sous la forme $u' \circ \iota_V$. On dira que u' est obtenu à partir de u par « extension des scalaires » de k à k' (ou par « fonctorialité »). Concrètement, u' est définie par la même matrice que u (ou, si on veut éviter de parler de matrices possiblement infinies, les mêmes coefficients sur des bases).

La même propriété universelle de ι vaut encore pour les applications bilinéaires, et plus généralement, multilinéaires : si V_1, V_2 sont deux k-espaces vectoriels et $V_1' := V_1 \otimes_k k'$ et $V_2' := V_2 \otimes_k k'$ sont obtenus par extension des scalaires, alors pour tout k'-espace vectoriel W, toute application k-bilinéaire $b \colon V_1 \times V_2 \to W$ se factorise de façon unique sous la forme $b(x_1, x_2) = b'(\iota(x_1), \iota(x_2))$ (c'est-à-dire $b'(x_1 \otimes 1, x_2 \otimes 1)$) avec $b' \colon V_1' \times V_2' \to W$ qui soit k'-bilinéaire (la démonstration est la même : les applications k-bilinéaires $V_1 \times V_2 \to W$ ou k'-bilinéaires $V_1' \times V_2' \to W$ sont en bijection avec $W^{I_1 \times I_2}$ une fois choisies des bases $(e_i)_{i \in I_1}$ et $(f_j)_{j \in I_2}$ de V_1 et V_2). La même chose vaut encore avec trois espaces vectoriels ou plus.

2.5.4. On a défini $V \otimes_k k'$ comme le k'-espace vectoriel dont une base (sur k', donc) est donnée par une base $(e_i)_{i \in I}$ de V (sur k). Il n'est bien entendu pas interdit de considérer $V \otimes_k k'$ comme un espace vectoriel sur k : dans ce cas, une base en est donnée par les $(e_i \otimes b_j)_{(i,j) \in I \times J}$ avec $(b_j)_{j \in J}$ une base de k' comme k-espace vectoriel (on s'en convainc en écrivant un élément quelconque comme combinaison k'-linéaire de la base $(e_i)_{i \in I}$ et en écrivant ensuite les coefficients eux-mêmes comme combinaisons k-linéaires des b_j ; de façon plus générale, si E est un k'-espace vectoriel et toujours $(b_j)_{j \in J}$ une base de k' comme k-espace vectoriel, alors une base de E comme k-espace vectoriel est donnée par les $(b_j e_i)_{(i,j) \in I \times J}$).

Soulignons au passage qu'*il n'est pas vrai que tous les éléments de $V \otimes_k k'$ soient de la forme $x \otimes c$* pour $x \in V$ et $c \in k'$: il est seulement vrai que ces

éléments *engendrent* $V \otimes_k k'$ comme k-espace vectoriel.

Signalons de plus, sans plus développer, que l'extension des scalaires qu'on a définie ci-dessus fait partie d'une construction plus générale appelée **produit tensoriel**. Le produit tensoriel de deux espaces vectoriels V et W sur un corps k est l'espace vectoriel $V \otimes_k W$ dont une base est le produit d'une base de V et d'une base de W (on vient d'expliquer pourquoi on est dans ce cas) ; on a une application bilinéaire $\beta\colon V \times W \to V \otimes_k W$ qui envoie un couple d'éléments des deux bases sur l'élément de la base d'arrivée défini par ce même couple (dans le cas qu'on a considéré, $\beta(x, c) = c\iota(x)$). Cette application bilinéaire possède la propriété « universelle » que toute application k-bilinéaire $V \times W \to E$ se factorise de façon unique en la composée de β et d'une application k-linéaire $V \otimes_k W \to E$: autrement dit, une application k-bilinéaire $V \times W \to E$ et une application k-linéaire $V \otimes_k W \to E$ sont essentiellement « la même chose ». Cette même propriété permet de définir de façon plus générale le produit tensoriel de deux modules quelconques sur un anneau quelconque, mais nous ne le ferons pas.

Proposition 2.5.5 (« exactitude » de l'extension des scalaires sur un corps)**.** Soit $k \subseteq k'$ une extension de corps et $U \subseteq V$ un sous-k-espace vectoriel d'un k-espace vectoriel V dont le quotient sera noté $W := V/U$. Notons U', V', W' les extensions des scalaires de U, V, W de k à k', et $U' \to V'$ et $V' \to W'$ les applications k'-linéaires obtenues par extension des scalaires à partir de l'injection d'inclusion (i.e., l'identité) $U \to V$ et la surjection canonique $V \to W$. Alors (a) $V' \to W'$ est surjective, (b) son noyau est exactement l'image de $U' \to V'$ et (c) cette dernière est injective. (**Note :** l'affirmation (c) ici dépend crucialement du fait que k est un corps.)

Démonstration. Soit $(e_i)_{i\in I}$ une base de U, qu'on complète en une base de V, disons $(e_i)_{i\in I\cup J}$ (avec $I \cap J = \varnothing$), l'image des $(e_i)_{i\in J}$ définissant alors une base de W. Ces k-bases de U, V, W donnent k'-bases de U', V', W'. Les applications $U' \to V'$ et $V' \to W'$ s'obtiennent alors respectivement en envoyant e_i sur e_i si $i \in I$ pour la première, et pour la seconde en envoyant e_i sur $\bar{e}_i$ si $i \in J$ et 0 si $i \in I$: avec cette description, les affirmations (a), (b) et (c) sont triviales. ☺

2.5.6. Supposons maintenant, toujours que $k \subseteq k'$ est une extension de corps, mais maintenant que A est une k-algèbre. On a défini un k'-espace vectoriel $A' := A \otimes_k k'$ par « extension des scalaires » de k à k'. L'application k-bilinéaire $A \times A \to A$ de multiplication (envoyant (a, b) sur ab), composée avec $\iota\colon A \to A'$, se factorise de façon unique d'après la « propriété universelle » pour les applications bilinéaires qu'on a vue plus haut : il existe donc une unique multiplication k'-bilinéaire sur A' qui vérifie $\iota(a)\,\iota(b) = \iota(ab)$. L'associativité

de A donne l'associativité de A' (puisque l'application trilinéaire $(a,b,c) \mapsto a(bc)-(ab)c$ est nulle, son unique factorisation par ι l'est encore).

Concrètement, cette algèbre $A' = A \otimes_k k'$ peut être construite ainsi : on part d'une base $(e_i)_{i\in I}$ de A, on écrit chaque produit $e_{i_1}e_{i_2}$ sous la forme $e_{i_1}e_{i_2} = \sum_{j\in I} c_{i_1,i_2,j}e_j$ (les $c_{i_1,i_2,j}$ s'appellent les « constantes de structure » de A sur cette base), et l'algèbre A' est la k'-algèbre obtenue en reprenant ces mêmes relations mais sur un k'-espace vectoriel de base $(e_i)_{i\in I}$. Pour une algèbre de type fini, on verra une description encore plus simple ci-dessous.

On a par ailleurs toujours la « propriété universelle » suivante : si B est une k'-algèbre, alors tout morphisme $\psi\colon A \to B$ de k-algèbres (c'est-à-dire k-linéaire préservant le produit) se factorise de façon unique comme la composée de $\iota A \to A'$ par un morphisme de k'-algèbres $\psi'\colon A' \to B$ (comme on a déjà vu la factorisation unique pour des morphismes d'espaces vectoriels, il n'y a plus qu'à vérifier que $\psi'\colon A' \to B$ préserve la multiplication, ce qui résulte du fait que $\psi(ab)-\psi(a)\,\psi(b)$ est nulle donc son unique factorisation par ι l'est aussi).

2.5.7. Si $k \subseteq k'$ est toujours une extension de corps et si maintenant $A = k[t_1,\dots,t_d]/I$ alors on peut décrire $A' := A \otimes_k k'$ comme $k'[t_1,\dots,t_d]/I'$ où I' est l'idéal engendré par I dans $k'[t_1,\dots,t_d]$, qui est aussi le k'-espace vectoriel engendré par I d'après 2.4.6. En effet, le cas où $I = 0$, c'est-à-dire quand $A = k[t_1,\dots,t_d]$, est clair, puisque les monômes forment une base sur k de $k[t_1,\dots,t_d]$ et une base sur k' de $k'[t_1,\dots,t_d]$, avec la même multiplication, et la proposition 2.5.5 permet d'en déduire le cas général (l'affirmation (c) montre que $I' = I \otimes_k k'$, l'affirmation (a) montre que $k'[t_1,\dots,t_d] \to (k[t_1,\dots,t_d]/I) \otimes_k k'$ est surjective et l'affirmation (b) montre que son noyau est précisément I').

Autrement dit, concrètement, si $h_1,\dots,h_m \in k[t_1,\dots,t_d]$ et si $A = k[t_1,\dots,t_d]/(h_1,\dots,h_m)$ (ce qui est la structure générale d'une algèbre de type fini sur k d'après 1.2.2 et 2.1.4), on a $A \otimes_k k' = k'[t_1,\dots,t_d]/(h_1,\dots,h_m)$. Ce qui n'était pas évident *a priori* sur cette écriture, mais qui résulte de ce qu'on a fait ci-dessus, est que, à isomorphisme près, cette définition ne dépend pas de la « présentation » de A comme $k[t_1,\dots,t_d]/(h_1,\dots,h_m)$ (c'est-à-dire du choix des générateurs, les images des t_i, et des relations entre eux, c'est-à-dire les h_i).

À titre d'exemple, $\mathbb{C} = \mathbb{R}[t]/(t^2+1)$ donc $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[t]/(t^2+1) = \mathbb{C}[t]/((t+\sqrt{-1})(t-\sqrt{-1})) \cong \mathbb{C}\times\mathbb{C}$ (cet exemple montre qu'étendre les scalaires d'un corps ne donne pas forcément un corps, ni même un anneau intègre — on va justement réexpliquer ce phénomène au paragraphe suivant).

2.5.8. La définition de l'extension des scalaires permet de reconsidérer la notion d'extensions de corps linéairement disjointes introduite en 1.4 ainsi que l'ensemble des résultats de cette section :

La proposition 1.4.4 signifie que deux extensions de corps $k \subseteq K$ et $k \subseteq L$ contenues dans une même troisième M sont linéairement disjointes *si et seulement*

si le morphisme $K \otimes_k L \to M$ (application L-linéaire déduite de la factorisation de l'application K-linéaire $K \to M$ en utilisant la propriété universelle) est injective. La proposition 1.4.6 signifie que lorsque L est algébrique sur k, l'extension composée $K.L$ est simplement l'image de cette application $K \otimes_k L \to M$. La proposition 1.4.7 en conclut que, toujours avec L algébrique sur k, on a K et L sont linéairement disjointes au-dessus de k si et seulement si $K.L = K \otimes_k L$, ou si on préfère, si et seulement si $K \otimes_k L$ est un corps (observer que si $K \otimes_k L$ est un corps, le morphisme $K \otimes_k L \to M$ est forcément injectif).

La proposition 1.4.9 signifie (en changeant les notations) que *lorsque k' est algébrique sur k* on a $k(t_1, \ldots, t_d) \otimes_k k' = k'(t_1, \ldots, t_d)$, à comparer avec $k[t_1, \ldots, t_d] \otimes_k k' = k'[t_1, \ldots, t_d]$ vu ci-dessus et valable sans hypothèse sur l'extension $k \subseteq k'$. (Pour montrer que la restriction sur k' est vraiment pertinente dans le cas des fractions rationnelles, signalons que $k(x) \otimes_k k(y)$, si x, y sont deux indéterminées, est le sous-anneau de $k(x, y)$ formé des fractions rationnelles qui admettent un dénominateur produit d'un polynôme en x et d'un polynôme en y.) Voici une généralisation de ce fait :

Proposition 2.5.9. Soit k un corps et A une k-algèbre, et soit k' une extension algébrique de k. Supposons que $A \otimes_k k'$ soit *intègre* (en particulier, A lui-même est intègre). Alors son corps des fractions $\mathrm{Frac}(A \otimes_k k')$ s'identifie avec $\mathrm{Frac}(A) \otimes_k k'$. De plus, dans ces conditions, $\mathrm{Frac}(A)$ et k' sont linéairement disjointes comme extensions de k contenues dans $\mathrm{Frac}(A \otimes_k k')$, et ce dernier est leur composé.

Démonstration. Le fait que A soit intègre si $A \otimes_k k'$ l'est résulte du fait que si $aa' = 0$ dans A alors $(a \otimes 1)(a' \otimes 1) = (aa') \otimes 1 = 0$, or $a \otimes 1$ n'est nul que pour $a = 0$.

Soit maintenant $K' := \mathrm{Frac}(A \otimes_k k')$. D'après 2.5.5(c), on peut voir $A \otimes_k k'$ comme une sous-k'-algèbre de K' (à savoir le k'-espace vectoriel engendré par les $a \otimes 1$ pour $a \in A$). Notamment, on peut voir A (identifié à l'ensemble des $a \otimes 1$) comme une sous-k-algèbre de K', et k' (identifié à l'ensemble des $1 \otimes u$ pour $u \in k'$) comme un sous-corps de K', contenu dans $A \otimes_k k'$. Puisque A est contenu dans le corps K', il en va de même de son corps des fractions $K := \mathrm{Frac}(A)$. On veut montrer que $K \otimes_k k' = K'$: pour cela, d'après ce qui a été dit ci-dessus (et comme k' est algébrique sur k), il s'agit de prouver que K et k' sont linéairement disjointes comme extensions de k contenues dans K' et que leur composée est K'.

Le fait que l'extension composée soit K' est clair car K' est engendré en tant que corps par A et k', donc *a fortiori* par K et k'. Il reste à voir que K et k' sont linéairement disjointes, autrement dit, que si les u_j sont des éléments de k' linéairement indépendants sur k et les c_j des éléments de K tels que $\sum_j c_j u_j = 0$ dans K', alors en fait les c_j sont nuls.

Mais on peut écrire $c_j = a_j/q$ où $a_j \in A$ et $q \in A$ est non nul fixé. On a donc $\sum_j a_j u_j = 0$ dans K', et en fait l'élément $a_j u_j$ de K' s'identifie à l'élément $a_j \otimes u_j$

de $A \otimes_k k'$ comme on vient de l'expliquer. Mais vu que les u_j sont linéairement indépendants sur k, cet élément ne peut être nul que si tous les a_j sont nuls (quitte, par exemple, à prendre une base de A sur k et à compléter les u_j en une base de k' sur k).

(Le fait que $A \otimes_k k'$ soit intègre a servi, dans cette démonstration, à tout situer dans le corps K'.) ☺

3 Corps de courbes algébriques

3.1 Définition et premiers exemples

3.1.1. Soit k un corps. On appelle **corps de fonctions de dimension** n sur k une extension de corps de k qui soit de type fini (cf. 1.2.4) et de degré de transcendance n sur k (cf. 1.5.5). Notamment, pour $n = 1$, on parle de **corps de fonctions de courbe** sur k.

Par abus de langage, on dira parfois simplement que K est une « courbe » (algébrique) sur k ; ou bien on dira que K est le corps des fonctions [rationnelles] de la courbe C et on notera alors $K = k(C)$ (on ne définit pas ce qu'« est » C, voir les exemples ci-dessous).

Il existe un certain nombre de variations entre auteurs autour de cette définition, pour essentiellement deux raisons : **(a)** le cadre dans lequel on considère les courbes n'est pas forcément le même (dans ce cours, nous avons choisi de définir les courbes à travers leur corps des fonctions, c'est-à-dire leurs fonctions rationnelles, plutôt que leur *anneau(x)* de fonctions régulières, c'est-à-dire leurs fonctions polynomiales : l'avantage est que cela simplifie l'étude ; l'inconvénient est que l'étude des courbes singulières n'est pas possible : par exemple, la courbe d'équation $y^2 = x^3$ dans le plan va simplement revenir à celle de la droite qui la paramètre par $t \mapsto (x, y) = (t^2, t^3)$, et de même on ne peut pas retirer des points à une courbe ; pour cette raison, ce que nous appelons « courbe » s'appellerait « courbe normale projective » ou « courbe projective lisse » chez d'autres auteurs), et **(b)** les hypothèses effectuées ne sont pas forcément les mêmes (notamment, beaucoup d'auteurs restreignent les courbes à ce qu'on appellera plus bas les courbes « géométriquement irréductibles »). On sera éventuellement amené à restreindre la définition qui vient d'être donnée.

3.1.2. La courbe la plus simple est donnée par le corps $k(t)$ des fractions rationnelles en une indéterminée t (l'extension *transcendante pure* de degré de transcendance 1) : on l'appelle **droite projective** (ou simplement « droite ») sur k et on peut la noter $\mathbb{P}^1_k$ ou simplement $\mathbb{P}^1$ (ainsi, $k(\mathbb{P}^1_k) := k(t)$).

Il faut imaginer les éléments de $k(t)$ comme des fonctions rationnelles sur la droite affine : on verra plus loin comment définir les points de la droite, mais on

peut au moins dire ceci : si x est un élément de k ou bien le symbole spécial ∞, et si $f \in k(t)$, on définit $f(x)$ comme l'**évaluation** (=la valeur) de f en x ou bien le symbole spécial ∞ si f a un pôle en x (lorsque $x = \infty$, l'évaluation de f en x peut se définir comme celle de la fraction rationnelle $f(\frac{1}{t})$ en 0 ; sur les réels ou les complexes, c'est simplement la limite de f en ∞ ou bien ∞ si f n'est pas borné).

Rappelons que tout élément f non nul de $k(t)$ possède une écriture unique sous la forme $c\prod_{h\in\mathscr{P}} h(t)^{v_h}$ où $c \in k^\times$, les v_h sont des entiers (relatifs) tous nuls sauf un nombre fini, et $\mathscr{P}$ est l'ensemble des polynômes unitaires irréductibles dans $k[t]$. Si k est *parfait*, tout $h \in \mathscr{P}$ peut encore s'écrire sous la forme $\prod_{\xi\in M}(t-\xi)$ où M est une orbite de k sous $\Gamma_k := \mathrm{Gal}(k \subseteq k^{\mathrm{alg}})$ (puisque deux éléments de k sont conjugués si et seulement si ils sont dans la même orbite sous Γ_k, notamment d'après 1.9.7 ou 1.6.4(2b)). On peut donc écrire tout élément non nul de $k(t)$ de façon unique sous la forme $c\prod_{\xi\in k^{\mathrm{alg}}}(t-\xi)^{v_\xi}$ où $c \in k^\times$, les v_ξ sont des entiers (relatifs) tous nuls sauf un nombre fini, et v_ξ est invariant sous Γ_k (i.e., $v_{\sigma(\xi)} = v_\xi$ pour tout $\sigma \in \Gamma_k$ et $\xi \in k^{\mathrm{alg}}$). Un des thèmes de ce qui va suivre est de généraliser ce type d'écriture au corps des fonctions d'une courbe quelconque : en attendant, signalons que v_h ou v_ξ s'appellera la **valuation** en h ou ξ de la fonction f considérée, et on verra à partir de 3.2.3 en quoi ce genre de fonction est important.

3.1.3. Si $P \in k[x,y]$ est un polynôme irréductible en deux indéterminées x, y et faisant effectivement intervenir y, on peut le voir comme un élément de $k(x)[y]$, qui est encore irréductible (cf. 1.1.14), ce qui définit donc un corps de rupture $k(x)[y]/(P)$ (cf. 1.3.2 et 1.6.2) qu'on notera généralement $k(x, y : P = 0)$; c'est aussi le corps des fractions de $k[x,y]/(P)$ (puisque c'est un corps contenant $k[x,y]/(P)$ et engendré par lui), et du coup, c'est aussi $k(y)[x]/(P)$ dès lors que la variable x intervient effectivement.

On souhaite dire qu'il s'agit du corps de fonctions $k(C)$ de la « courbe plane » $C := \{P = 0\}$: à ce stade-là, il s'agit d'une notation purement formelle, mais on peut faire les remarques suivantes pour l'éclaircir.

On a introduit en 2.4.2 la notation $Z(P) := \{(x,y) \in (k^{\mathrm{alg}})^2 : P(x,y) = 0\}$ pour l'ensemble des zéros de P (dans une clôture algébrique !) : appelons C_P cet ensemble. Comme P est irréductible, l'idéal (P) est premier (cf. 1.1.3), donc radical (cf. 2.4.1) : la proposition 2.4.7 implique donc que (P) est l'idéal des polynômes qui s'annulent identiquement sur C_P, et on a expliqué en 2.4.9 que les éléments de $k[x,y]/(P)$ peuvent s'identifier aux fonctions régulières sur C_P, c'est-à-dire les restrictions à C_P des éléments de $k[x,y]$ (vus comme des fonctions $(k^{\mathrm{alg}})^2 \to k^{\mathrm{alg}}$). Le corps $k(C) = \mathrm{Frac}(k[x,y]/(P))$ dont on vient de parler peut donc se voir comme l'ensemble des quotients de deux fonctions régulières (i.e., polynomiales) sur C_P dont le dénominateur n'est pas identiquement nul sur C_P :

il est donc raisonnable d'appeler ce corps « corps des fonctions sur C_P ».

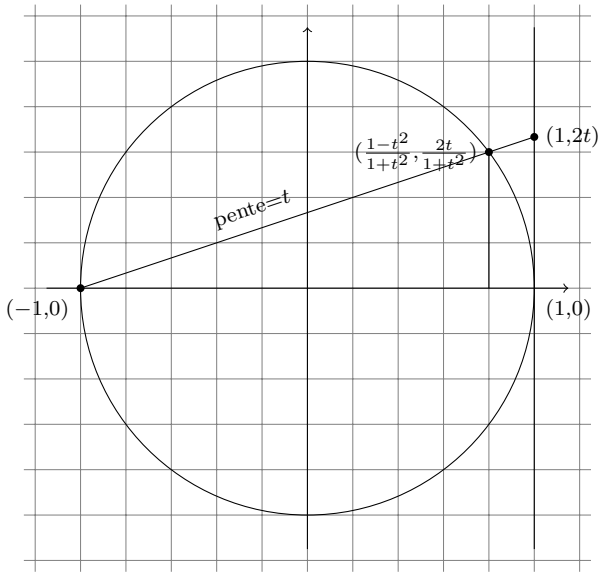
L'extension de corps $k(x) \subseteq k(C)$ (quand on voit $k(C)$ comme $k(x)[y]/(P)$) correspondra à la projection $C \to \mathbb{P}^1$ sur la première coordonnée.

Donnons quelques exemples plus précis, puis discutons ce qui se passe dans des cas adjacents.

3.1.4. Considérons l'exemple de $P = x^2 + y^2 - 1$ sur un corps k de caractéristique $\neq 2$ (on pensera notamment au corps des réels).

Le polynôme P est irréductible dans $k[x, y]$. En effet, comme il est de degré total 2, une factorisation non triviale serait nécessairement en degrés $1 + 1$; en considérant les termes de plus haut degré (i.e., 1) des facteurs, dont le produit doit être $x^2 + y^2$, on voit qu'ils doivent être de la forme $x + \sqrt{-1}\, y$ et $x - \sqrt{-1}\, y$ (en notant $\sqrt{-1}$ une racine carrée de -1 dans k, qui doit exister pour que la factorisation soit possible) ; or avoir $(x+\sqrt{-1}\, y+c)(x-\sqrt{-1}\, y+c') = x^2+y^2-1$ impose simultanément $c + c' = 0$ et $c - c' = 0$ et $cc' = -1$, conditions manifestement impossibles à satisfaire en caractéristique $\neq 2$. On est donc dans le cadre considéré plus haut.

La courbe plane C d'équation $P = 0$ est le « cercle unité », dont le corps des fonctions est le corps $\mathrm{Frac}(k[x, y]/(x^2+y^2-1)) = k(x, y : x^2+y^2 = 1)$ de rupture de $x^2 + y^2 - 1$ sur $k(x)$. En fait, il s'avère que ce corps est *isomorphe* au corps $k(t)$ des fractions rationnelles en une indéterminée : ceci résulte du « paramétrage rationnel du cercle » représenté géométriquement par la figure suivante



Un petit calcul d'inspiration géométrique (cf. les formules exprimant $(\cos\theta, \sin\theta)$ en fonction de $\tan\frac{\theta}{2}$), valable en fait sur tout corps k de caractéristique $\neq 2$, montre que toute solution (x, y) de $x^2 + y^2 = 1$ autre que

$(-1,0)$ peut s'écrire de la forme $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ avec $t \in k$ (uniquement défini, et vérifiant $t^2 \neq -1$), qui peut être réciproquement calculé comme $t = \frac{y}{x+1}$.

Mais ces mêmes formules peuvent s'interpréter comme définissant un *isomorphisme* entre $k(C) := k(x, y : x^2 + y^2 = 1)$ et $k(\mathbb{P}^1) = k(t)$, à savoir l'isomorphisme envoyant x et y (maintenant des éléments de $k(C)$) sur $\frac{1-t^2}{1+t^2}$ et $\frac{2t}{1+t^2}$ (éléments de $k(t)$) respectivement : le fait qu'on ait bien $\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1$ assure que ce morphisme est bien défini (rappel : pour définir un morphisme de $k(x)[y]/(P)$ vers un anneau B quelconque il suffit de définir un morphisme de $k(x)[y]$ vers B qui annule l'image de P), et en vérifiant que $t \mapsto \frac{y}{x+1}$ est sa réciproque, on voit que c'est un isomorphisme.

Toute cette situation se résume en disant que le cercle $C = \{x^2 + y^2 = 1\}$ est une courbe **rationnelle** (sur le corps k quelconque de caractéristique $\neq 2$), ou rationnellement paramétrée. Le cadre dans lequel nous considérons les courbes fait qu'on « ne voit pas » la différence entre les courbes rationnelles et la droite. (Un exemple encore plus simple d'une courbe rationnelle est fourni par la parabole $\{x = y^2\}$, rationnellement paramétrée par y, c'est-à-dire qu'ici $k(x)[y]/(y^2 - x)$ est simplement $k(y)$, dans lequel $k(x)$ est vu comme le sous-corps $k(y^2)$.)

De façon générale, le même raisonnement que pour le cercle va fonctionner pour une conique « non-dégénérée » sur un corps de caractéristique $\neq 2$, i.e., la courbe définie par un polynôme de degré 2 qui ne se factorise pas même sur la clôture algébrique (géométriquement, ceci signifie que la conique ne sera pas réunion de deux droites, même sur la clôture algébrique), *à condition d'avoir un point rationnel* (cf. 2.4.8(1)) qui puisse jouer le rôle de $(-1, 0)$ dans le paramétrage par des droites de pente variable. L'exemple qui suit montre que cette hypothèse n'est pas anecdotique.

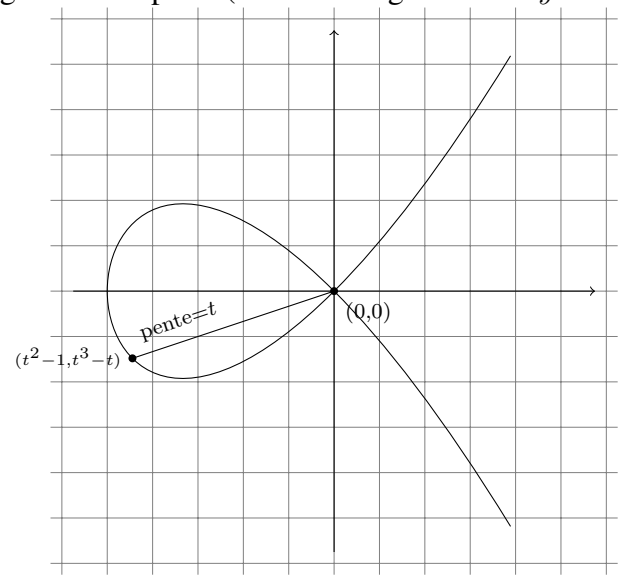
3.1.5. Considérons maintenant l'exemple de $P = x^2 + y^2 + 1$ sur un corps k de caractéristique $\neq 2$ dans lequel -1 n'est pas somme de deux carrés (de nouveau, on pensera principalement au corps des réels). Le même argument que pour $x^2 + y^2 - 1$ montre que ce polynôme P est irréductible, mais cette fois $k(C) := k(x, y : x^2 + y^2 = -1)$ ***n'est pas*** isomorphe à $k(t)$. En effet, un tel isomorphisme déterminerait deux éléments $x, y \in k(t)$ vérifiant $x^2 + y^2 = -1$; mais quitte à chasser les dénominateurs on obtient $x, y, z \in k[t]$ tels que $x^2 + y^2 + z^2 = 0$, et en prenant le dénominateur réduit, x, y, z ne s'annulent pas simultanément en 0, disons $z(0) \neq 0$ pour fixer les idées, et quitte à poser $u = x(0)/z(0)$ et $v = y(0)/z(0)$ on obtient $u^2 + v^2 = -1$, contredisant l'hypothèse faite sur k.

En particulier, $\mathbb{R}(x, y : x^2 + y^2 = -1)$ fournit un exemple d'une extension de corps de $\mathbb{R}$ de type fini et de degré de transcendance 1 mais qui n'est pas transcendante pure.

La courbe décrite par cet exemple est ce qu'on appelle généralement une « conique sans point(s) » (c'est-à-dire : sans point *rationnel*).

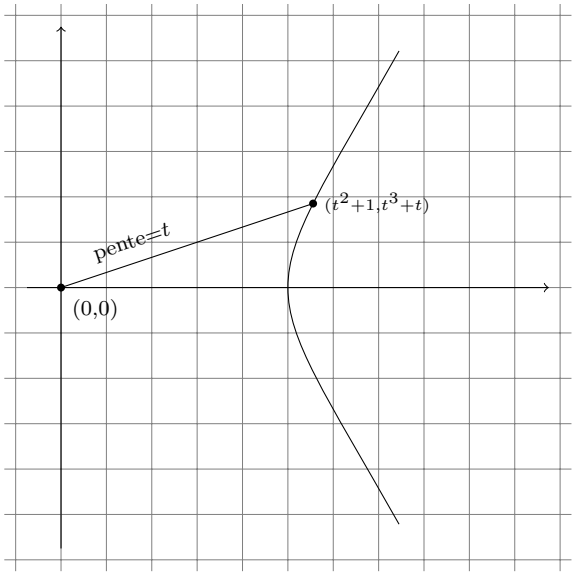
3.1.6. Mentionnons encore quelques exemples de courbes rationnelles données par des fermés de Zariski ayant des points *singuliers*. On dit qu'un point (à coordonnées dans la clôture algébrique !) du fermé de Zariski $\{P = 0\}$ (avec $P \in k[x, y]$ non constant) est **singulier** lorsque P'_x et P'_y s'y annulent simultanément.

— La courbe d'équation $y^2 = x^3 + x^2$ sur un corps de caractéristique $\neq 2$. (Note : le polynôme $x^3 + x^2 - y$ est irréductible car un facteur de degré 1 serait de la forme $x - c$ en regardant les termes de plus haut degré, et on se convainc facilement que cette courbe ne contient pas de droite verticale $x = c$.) Cette courbe porte le nom standard de « **cubique nodale** », et le point $(0, 0)$ est y appelé un « point double ordinaire ». (Formellement un point est un point double ordinaire de $\{P = 0\}$ avec P irréductible lorsque P'_x et P'_y s'y annulent mais que le polynôme $P''_{x,x} + P''_{x,y}u + P''_{y,y}u^2$ — qui définit les directions des tangentes — n'a pas de zéro multiple sur la clôture algébrique.) On peut la paramétrer rationnellement en utilisant t la pente d'une droite variable par le point double ordinaire $(0, 0)$ et en cherchant les coordonnées de son autre point d'intersection avec la courbe : en injectant $y = tx$ dans $y^2 = x^3 + x^2$ on trouve le paramétrage $(x, y) = (t^2 - 1, t^3 - t)$. On remarquera que ce paramétrage parcourt deux fois le point $(0, 0)$ (une fois pour $t = +1$ et une fois pour $t = -1$), essentiellement une fois par direction tangente en ce point (les deux tangentes sont $y = x$ et $y = -x$).

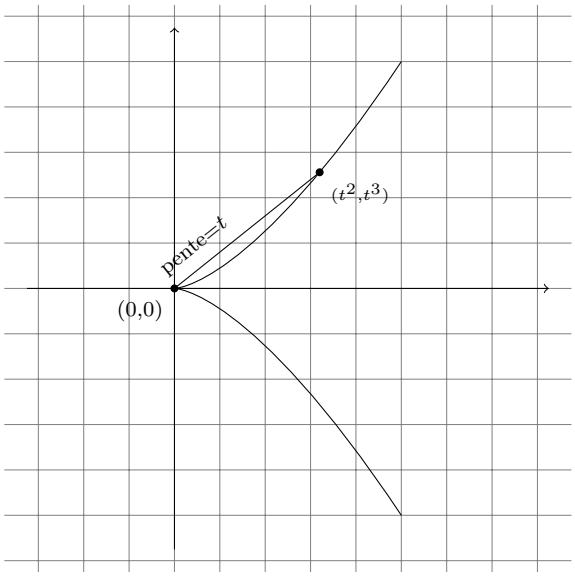


— La courbe d'équation $y^2 = x^3 - x^2$ sur un corps de caractéristique $\neq 2$ dans lequel -1 n'est pas un carré, par exemple le corps des réels. (De nouveau, on vérifie que ce polynôme est irréductible.) Le point $(0, 0)$ est de nouveau un « point double ordinaire », mais cette fois ses deux tangentes ne sont pas rationnelles (« rationnelles » au sens « définies sur k »). On

peut toujours paramétrer rationnellement la courbe utilisant t la pente d'une droite variable par le point double ordinaire $(0,0)$ et en cherchant les coordonnées de son autre point d'intersection avec la courbe : en injectant $y = tx$ dans $y^2 = x^3 - x^2$ on trouve le paramétrage $(x, y) = (t^2+1, t^3+t)$. On remarquera que cette fois le point $(0,0)$ est atteint par des coordonnées qui ne sont pas dans k (à savoir $\pm\sqrt{-1}$).



— La courbe d'équation $y^2 = x^3$ (toujours irréductible). Cette courbe porte le nom de « **cubique cuspidale** » parce que le point $(0,0)$ est un « cusp » ou point de rebroussement. Le même procédé de paramétrage que ci-dessus donne $x = t^2$ et $y = t^3$ (par ailleurs trouvable directement). Cette fois-ci, il y a bien bijection, sur n'importe quel corps k, entre les solutions de $y^2 = x^3$ et les éléments de k.



Dans chacun de ces exemples, le corps $k(C)$ des fonctions de la courbe est simplement le corps $k(t)$ (pour le paramétrage qu'on a donné), mais le fermé de Zariski $\{P = 0\}$ présente des complications géométriques, et on pourrait se convaincre que l'anneau $k[x, y]/(P)$ des fonctions régulières sur $\{P = 0\}$ ***n'est pas*** l'anneau $k[t]$ (bien qu'il ait $k(t)$ comme corps des fractions).

3.1.7. On a mentionné ci-dessus l'exemple de la parabole $\{x = y^2\}$, courbe rationnelle dont le corps des fonctions $k(x)[y]/(y^2 - x)$ est simplement $k(y)$ à l'intérieur duquel $k(x)$ est vu comme le sous-corps $k(y^2)$. Plus généralement, on a la courbe $\{x = y^n\}$, courbe rationnelle dont le corps des fonctions $k(x)[y]/(y^n - x)$ est simplement le corps des fractions rationnelles (=transcendant pur) $k(y)$ à l'intérieur duquel $k(x)$ (lui aussi transcendant pur) est vu comme le sous-corps $k(y^n)$. Si n n'est pas multiplie de la caractéristique et que k a une racine primitive n-ième de l'unité ζ, alors $y \mapsto \zeta y$ définit un automorphisme de $k(y)$ dont le corps fixe est exactement $k(y^n) = k(x)$. D'après le théorème 1.9.9, ceci implique que l'extension $k(y^n) \subseteq k(y)$ est galoisienne de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$, ou, mieux $\{\zeta^i\}$, qu'on peut vraiment voir comme des transformations sur la courbe (envoyant le point géométrique de coordonnées (x, y) sur $(x, \zeta^i y)$).

(Si n est multiple de la caractéristique, l'extension $k(y^n) \subseteq k(y)$ ne sera pas séparable, mais ça n'empêche pas $k(y)$ d'être un corps de fonctions d'une courbe tout à fait sympathique.)

En caractéristique $p > 0$, un autre exemple important est celui de la courbe d'équation $x = y^p - y$: de nouveau, $k(x)[y]/(x - y^p + y)$ est simplement $k(y)$ (transcendant pur) à l'intérieur duquel $k(x)$ se plonge par $x \mapsto y^p - y$; cette fois, c'est $y \mapsto y + 1$ qui définit un automorphisme de $k(y)$ fixant exactement $k(x)$.

3.1.8. Lorsque $P \in k[x, y]$ n'est pas irréductible, disons $P = P_1 P_2$ avec P_1, P_2

non constants, alors $Z(P) = Z(P_1) \cup Z(P_2)$: autrement dit, on a affaire non pas à une seule courbe mais à une réunion de courbes (certains auteurs appellent encore « courbe » cet objet). Si on s'est placé dans le cadre où (P) est radical, alors P_1, P_2 sont premiers entre eux, car s'ils avaient un diviseur commun Q non-trivial, on aurait $P_1\,P_2/Q \in k[x,y]$ non nul modulo P (puisque Q est non-trivial) mais de carré nul (puisque c'est le produit de P par $(P_1/Q)(P_2/Q) \in k[x,y]$), ce qui contredit la radicalité supposée. Cet argument valant encore dans $k(x)[y]$, on a $k(x)[y]/(P) \cong k(x)[y]/(P_1) \times k(x)[y]/(P_2)$ par le théorème chinois : autrement dit, $k(x)[y]/(P)$ n'est pas un corps dans ces conditions (et $k[x,y]/(P)$ n'est pas un anneau intègre : il a P_1, P_2 comme diviseurs de zéro).

Pour souligner que cette situation ne se produit pas, on pourra parler de « courbes irréductibles » (avec la définition que nous avons prise, c'est redondant). On rappelle (cf. 2.4.10) qu'un fermé de Zariski $Z(I)$ est dit « irréductible » lorsqu'il n'est pas réunion de deux fermés strictement plus petits.

3.1.9. Mentionnons encore une situation à garder à l'esprit : si $P = y^2+1 \in k[x,y]$ sur un corps k dans lequel -1 n'est pas un carré, par exemple le corps des réels, alors P est bien irréductible, mais il cesse de l'être sur la clôture algébrique où $P = (y+\sqrt{-1})(y-\sqrt{-1})$: on dit que ce polynôme est irréductible mais non *géométriquement* irréductible, cf. 2.4.12. (Dans les exemples vus précédemment, x^2+y^2+1, x^2+y^2-1, $y^2-x^3-x^2$, $y^2-x^3+x^2$ et y^2-x^3, l'irréductibilité de P n'était jamais perdue en montant à un corps plus gros.)

Le corps $k(x,y\,:\,P=0) = k(x)[y]/(P)$ des fonctions de la courbe est simplement $k(\sqrt{-1},x)$ (par exemple, $\mathbb{R}(x)[y]/(y^2+1)$ est $\mathbb{C}(x)$).

Il faut imaginer cette courbe de la façon suivante : c'est la réunion de deux droites « géométriques » (c'est-à-dire définies sur la clôture algébrique), $y=\sqrt{-1}$ et $y=-\sqrt{-1}$, ces droites étant permutées par le groupe de Galois (qui échange $\sqrt{-1}$ et $-\sqrt{-1}$). Autrement dit, on a affaire à un fermé de Zariski qui est irréductible (cf. 2.4.11) mais qui cesse de l'être sur la clôture algébrique (cf. 2.4.12).

Lorsque P est géométriquement (=absolument) irréductible, on dira que la courbe plane $\{P=0\}$ l'est. Une conséquence de cette propriété sur le corps $K := k(x,y\,:\,P=0)$ est que, d'après la proposition 2.5.9, dans le corps $K.k^{\mathrm{alg}} = k^{\mathrm{alg}}(x,y\,:\,P=0)$, les sous-corps K et k^{alg} sont linéairement disjoints sur k. Cette propriété sera parfois utile.

3.1.10. Bien sûr, il n'y a pas de raison de se limiter aux courbes *planes* ou même, dans une certaine mesure, de se limiter aux courbes du tout : si $I \subseteq k[t_1,\ldots,t_d]$ est un idéal premier quelconque, alors $X := Z(I)$ est un fermé de Zariski irréductible, et le corps des fractions de l'anneau intègre $k[t_1,\ldots,t_d]/I$ des fonctions régulières sur X mérite de s'appeler **corps des fonctions rationnelles** de X, qu'on peut noter $k(X)$. Le degré de transcendance $\deg.\,\mathrm{tr}_k\,k(X)$ sera appelé

dimension de X, mais nous ne considérerons vraiment que le cas des courbes, c'est-à-dire, de la dimension 1 : celui-ci a de particulier qu'on pourra alors voir un élément de $k(X)$ comme une vraie fonction de X vers $\mathbb{P}^1$, quitte à lui la valeur ∞ sur les pôles (alors qu'en dimension ≥ 2 une fonction rationnelle peut ne pas être définie sans pour autant avoir un pôle : penser à x/y en $(x, y) = (0, 0)$).

La même remarque que ci-dessus vaut : si le fermé de Zariski X est géométriquement (=absolument) irréductible (cf. 2.4.12), son corps des fractions $K := \mathrm{Frac}(k[t_1, \ldots, t_d]/I)$ a la propriété, d'après la proposition 2.5.9, que dans le corps $K.k^{\mathrm{alg}} = \mathrm{Frac}(k^{\mathrm{alg}}[t_1, \ldots, t_d]/(I.k^{\mathrm{alg}}))$, les sous-corps K et k^{alg} sont linéairement disjoints sur k. En dimension 1 on dira que la courbe associée au corps K est elle-même géométriquement irréductible.

3.1.11. Si $I \subseteq k[t_1, \ldots, t_d]$ est un idéal premier tel que $Z(I)$ soit de dimension 1, c'est-à-dire que le corps des fractions K de l'anneau intègre $k[t_1, \ldots, t_d]/I$ soit un corps de fonctions de courbe au sens où on l'a défini, la proposition 1.8.7 montre que, au moins si k est un corps *parfait*, on peut toujours se ramener à la situation qui vient d'être décrite. (Et si k n'est pas parfait, on peut défendre l'idée que la définition donnée en 3.1.1 n'est pas la bonne et qu'on devrait supposer K algébrique *séparable* sur une extension transcendante pure $k(x)$.) En un certain sens, donc, toutes les courbes algébriques sont « planes » (mais de nouveau, ceci dépend hautement du point de vue choisi pour étudier les courbes).

On peut dire mieux : en étudiant la démonstration de la proposition 1.8.7 (et du théorème 1.8.5 dont elle dépend), on voit que celle-ci est constructive (elle peut être rendue algorithmique) : on va obtenir explicitement deux coordonnées $x, y \in K$ telles que $K = k(x, y)$ avec x transcendant et y algébrique séparable sur $k(x)$, c'est-à-dire une façon de tracer la courbe dans le plan ; en fait, c'est même une projection linéaire qui conviendra, puisque dans la démonstration de 1.8.5 on n'a pris que des combinaisons linéaires des indéterminées, donc x et y sont finalement des combinaisons linéaires des (classes des) coordonnées t_i de départ. Cette projection peut, cependant, introduire des singularités (il existe des courbes algébriques qui ne peuvent pas être représentées comme des courbes planes non-singulières).

3.2 Anneaux de valuations

Définition 3.2.1. Soit K un corps. On appelle **anneau de valuation** de K un sous-anneau R de K vérifiant la propriété suivante :

$$\text{pour tout } x \in K, \text{ on a soit } x \in R \text{ soit } x^{-1} \in R.$$

Lorsque k est un sous-corps de K contenu dans R, on peut dire que R est un anneau de valuation **au-dessus** de k.

Lorsque de plus $R \neq K$, on dit qu'il s'agit d'un anneau de valuation *non-trivial*.

3.2.2. Dans les conditions ci-dessus, R est un anneau intègre (puisque c'est un sous-anneau d'un corps), et il est clair que K est le corps des fractions de R (cf. 1.1.10 ; tout élément de K est quotient d'éléments de R puisqu'il est même toujours de la forme x ou $\frac{1}{x}$!). On peut donc parler dans l'absolu d'un « anneau de valuation », c'est un anneau de valuation de son corps des fractions.

On dira qu'un élément x de K a une *valuation plus grande* (pour R) qu'un élément y lorsque $x = yz$ avec $z \in R$; on dira, bien sûr, qu'ils ont la *même valuation* lorsque $x = yz$ avec $z \in R^\times$ (lire : z inversible dans R), ce qui signifie bien sûr exactement que x a une valuation plus grande que y et réciproquement. Il s'agit là d'une relation d'équivalence sur K : les classes d'équivalences des éléments non nuls s'appellent les *valuations* : on notera $v_R(x)$ ou simplement $v(x)$ pour la valuation de x ; la classe de $0 \in R$ sera mise à part et notée ∞ (on écrira $v(0) = \infty$ mais on ne considère généralement pas qu'il s'agisse d'une valuation). La définition d'un anneau de valuation fait qu'on a défini une relation d'ordre *total* sur l'ensemble des valuations (plus ∞ qui est le plus grand élément).

On définit $v(x) + v(y)$ comme $v(xy)$ et on note 0 pour $v(1)$ (ou $v(c)$ pour n'importe quel $c \in R^\times$) : cette définition a bien un sens comme on le vérifie facilement, et fait de l'ensemble des valuations (sans compter le symbole spécial ∞) un *groupe* abélien, appelé **groupe des valuations** (ou **des valeurs**) de R (ou de K pour R), qui n'est autre que le groupe quotient $\Gamma := K^\times / R^\times$. Avec l'ordre qu'on a mis ci-dessus, il s'agit d'un *groupe abélien totalement ordonné*, c'est-à-dire que si $u \geq u'$ alors $u + w \geq u' + w$ quel que soit w.

Lorsque le groupe des valuations est $\mathbb{Z}$, c'est-à-dire qu'il est engendré par un unique élément (on peut alors choisir un générateur strictement positif, qui est forcément le plus petit élément strictement positif, et qu'on peut noter 1), on dira que R est un anneau de valuation **discrète**.

Proposition 3.2.3. Si R est un anneau de valuation de K et $v\colon K \to \Gamma \cup \{\infty\}$ la valuation associée, on a les propriétés suivantes :

(o) $v(x) = \infty$ si et seulement si $x = 0$,

(i) $v(xy) = v(x) + v(y)$,

(ii) $v(x + y) \geq \min(v(x), v(y))$,

et de plus,

(ii.b) $v(x + y) = \min(v(x), v(y))$ si $v(x) \neq v(y)$,

qui est une conséquence des précédentes.

L'anneau R peut se retrouver à partir de la valuation comme $\{x \in K : v(x) \geq 0\}$.

Réciproquement, si Γ est un groupe abélien totalement ordonné et $v\colon K \to \Gamma \cup \{\infty\}$ une fonction surjective vérifiant (o), (i) et (ii), alors $R := \{x \in K :$

$v(x) \geq 0\}$ est un anneau de valuation qui a v pour valuation associée : on dit alors que v est une **valuation** sur K ou sur R.

En particulier, on peut définir un anneau de valuation discrète comme un anneau R muni d'une fonction $v\colon \mathrm{Frac}(R) \to \mathbb{Z} \cup \{\infty\}$ qui vérifie (o), (i) et (ii) et qui atteint la valeur 1.

Démonstration. Si v est la valuation associée à un anneau de valuation R, alors l'affirmation (o) est la définition du symbole ∞, et l'affirmation (i) est la définition de l'addition dans Γ ; pour montrer (ii), on peut supposer (puisque Γ est totalement ordonné) que $v(x) \geq v(y)$, c'est-à-dire $x = yz$ avec $z \in R$, auquel cas on a $x + y = y(1 + z)$ avec $1 + z \in R$, ce qui montre bien $v(x + y) \geq v(y)$.

Pour déduire $v(x + y) = \min(v(x), v(y))$ de (ii) dans le cas où $v(x) \neq v(y)$, on peut supposer $v(x) > v(y)$, et donc $v(x + y) \geq v(y)$; mais par ailleurs, $y = (x + y) - x$ (et bien sûr $v(-1) = 0$ vu que $(-1)^2 = 1$) si bien que $v(y) \geq \min(v(x + y), v(x))$, or on a $v(x) > v(y)$ donc en fait $v(x + y) = v(y)$, ce qu'on voulait.

Le fait que $R = \{x \in K : v(x) \geq 0\}$ est la définition de l'ordre (et le fait que $0 = v(1)$).

Enfin, si v vérifie (o), (i) et (ii) et $R := \{x \in K : v(x) \geq 0\}$, alors R est un sous-anneau de K car il contient 0 d'après (o), est stable par addition d'après (ii) et par multiplication d'après (i) ; et c'est un anneau de valuation car si $x \notin R$ c'est que $v(x) < 0$ donc $v(x^{-1}) = -v(x) > 0$ (en utilisant (i)), donc $x^{-1} \in R$. Et la valuation associée à R est bien v car $x = yz$ pour $z \in R$ entraîne $v(x) \geq v(y)$ par (i), et notamment $v(x) = v(y)$ si et seulement si $x = yz$ pour un certain $z \in R^\times$: alors $v\colon K^\times \to \Gamma$ définit un isomorphisme de groupes ordonnés de $K^\times/R^\times$ sur Γ.

Pour ce qui est de l'affirmation du dernier paragraphe, constater que $v\colon K^\times \to \mathbb{Z}$ est surjective si et seulement si elle atteint la valeur 1. ☺

3.2.4. Les valuations de K et les anneaux de valuations de K sont donc exactement interchangeables, et on se permettra d'utiliser la terminologie de l'un pour l'autre. Par exemple, dire qu'une valuation est non-triviale signifie qu'elle ne prend pas que les valeurs 0 et ∞. Dire qu'une valuation est au-dessus de k (sous-corps de K) signifie qu'elle est nulle sur $k^\times$ (ou positive sur k, ce qui revient au même).

3.2.5. Une conséquence fréquemment utilisée des propriétés des valuations est qu'une somme $x_1 + \cdots + x_n$ dans laquelle un des termes a une valuation *strictement plus petite* que tous les autres n'est jamais nulle. (En effet, si $v(x_i) < v(x_j)$ pour tout $j \neq i$, alors $v(x_i) < v(y)$ où $y := \sum_{j \neq i} x_j$ d'après la propriété (ii), et (ii.b) entraîne alors que la valuation de la somme est égale à celle de x_i, donc n'est pas ∞.).

3.2.6. Si A est un anneau et $v\colon A \to \Gamma \cup \{\infty\}$ (où Γ est un groupe abélien totalement ordonné) une fonction vérifiant (o), (i) et (ii) de 3.2.3, alors A est intègre (à cause de (i)), et il est facile de vérifier que v se prolonge de façon unique en une valuation sur son corps des fractions K en posant $v(x/y) = v(x) - v(y)$ (ce qui est manifestement nécessaire et bien défini). Cette observation peut simplifier la recherche ou l'étude des valuations sur un corps défini comme corps des fractions. Le plus souvent, dans la situation qu'on vient de décrire, on considère v positive sur A, et alors $A \subseteq R_v$ en notant R_v l'anneau de valuation.

3.2.7. Les exemples les plus importants de valuations sont celles introduites en 3.1.2 ci-dessus (les v_h ou v_ξ introduits à cet endroit sont des exemples de valuations de $k(t)$ au-dessus de k, et en 3.4 on verra même que ce sont presque les seules non-triviales ; ce sont par ailleurs des valuations *discrètes*).

Un autre exemple très semblable (important pour l'arithmétique, quoique moins pour la géométrie) est donné par les valuations p-adiques sur les rationnels : si $\frac{a}{b}$ est un rationnel et p un nombre premier, on peut définir $v_p(\frac{a}{b})$ comme l'exposant de la plus grande puissance de p qui divise a moins l'exposant de la plus grande puissance de p qui divise b. On peut montrer qu'il s'agit là de toutes les valuations non-triviales sur $\mathbb{Q}$. (Les v_h sur $k(t)$ évoquées ci-dessus sont l'analogue exact de ces v_p sur $\mathbb{Q}$ en utilisant la décomposition des polynômes en facteurs irréductibles au lieu de la décomposition des entiers en facteurs premiers.) Il s'agit là aussi de valuations discrètes ; en revanche, elles ne sont pas au-dessus d'un corps.

Pour donner au moins quelques exemples de valuations qui ne soient pas discrètes, sur l'anneau $k[x, y]$ des polynômes en deux indéterminées on peut définir $v(x^i y^j) = (i, j)$ à valeurs dans le groupe $\mathbb{Z}^2$ muni de l'ordre lexicographique donnant le poids le plus fort à la première coordonnée (il s'agit bien d'un groupe totalement ordonné) : ceci s'étend de façon unique en une valuation sur ($k[x, y]$, puis) $k(x, y)$, qui n'est pas une valuation discrète. Si θ est un nombre réel strictement positif et irrationnel, on peut aussi définir $v(x^i y^j) = i + j\theta$ à valeurs dans $\mathbb{Z} \oplus \mathbb{Z}\theta \subseteq \mathbb{R}$ muni de son ordre hérité des réels, ce qui, de nouveau, définit une valuation sur ($k[x, y]$, puis) $k(x, y)$, qui n'est pas une valuation discrète. Ce type d'exemple ne nous intéressera guère, car on va voir en 3.3.2 ci-dessous que toutes les valuations non-triviales sur les courbes sont discrètes.

Proposition 3.2.8. Les deux propriétés suivantes sur un anneau non nul R sont équivalentes :

(i) R a un unique idéal maximal,

(ii) le complémentaire dans R de l'ensemble $R^\times$ des unités de R est un idéal (forcément maximal),

(iii) pour tout $x \in R$, soit x est inversible, soit $1 - cx$ est inversible pour tout $c \in R$.

Un anneau vérifiant ces propriétés est appelé un anneau **local**.

Démonstration. Soit $R^\times$ l'ensemble des unités de R. Comme une unité engendre l'idéal (unité !) R, tout idéal autre que R est inclus dans le complémentaire $R\setminus R^\times$.

Si (i) R a un unique idéal maximal $\mathfrak{m}$, alors tout élément $x \in R$ qui *n'est pas* une unité engendre un idéal (x) qui est inclus dans $\mathfrak{m}$ d'après 1.1.7, donc $x \in \mathfrak{m}$: ceci montre $(R \setminus R^\times) \subseteq \mathfrak{m}$, et l'inclusion réciproque résulte du paragraphe précédent, donc $(R \setminus R^\times) = \mathfrak{m}$ et en particulier on a (ii).

Réciproquement, si (ii) $R \setminus R^\times$ est un idéal, on a expliqué qu'il contient tout autre idéal strict, et en particulier, il est l'unique idéal maximal, ce qui montre (i).

Considérons l'ensemble $\operatorname{rad} R$ des $x \in R$ tels que $1 - cx$ soit inversible pour tout $c \in R$. Sans aucune hypothèse sur R, on peut faire les observations suivantes : si $x \in \operatorname{rad} R$ et $a \in R$ alors $ax \in \operatorname{rad} R$ (car $1 - cax$ est de la forme $1 - c'x$ où $c' = ca$) ; dire que $1 - cx$ est inversible pour tout $c \in R$ équivaut à dire que $u - cx$ est inversible pour tout $c \in R$ et tout $u \in R^\times$ (cette dernière condition est *a priori* plus forte, mais comme $u - cx = u(1 - c'x)$ où $c' = u^{-1}c$, le fait que $x \in \operatorname{rad} R$ entraîne bien cette condition plus forte) ; enfin, si $x, y \in \operatorname{rad} R$ alors $1 - c(x + y) = (1 - cx) - cy$ est de la forme $u - cy$ où $u \in R^\times$ donc est inversible : tout ceci montre que $\operatorname{rad} R$ est un *idéal*[5] de R. Manifestement, les conditions $x \in R^\times$ et $x \in \operatorname{rad} R$ sont toujours incompatibles (prendre pour c l'inverse de x) dans un anneau non-nul.

On vient de voir que $\operatorname{rad} R$ est un idéal strict, i.e., contenu dans $R \setminus R^\times$: si (iii) leur union est R, alors ils sont complémentaires, donc le complémentaire de $R \setminus R^\times$ est un idéal, ce qui montre (ii).

Enfin, si (ii) $R \setminus R^\times$ est un idéal $\mathfrak{m}$, et si $x \notin R^\times$, c'est-à-dire $x \in \mathfrak{m}$, alors $cx \in \mathfrak{m}$ quel que soit $c \in R$, donc $1-cx$ est dans $R^\times$, et on a bien montré (iii). ☺

3.2.9. Un exemple d'anneau local est celui formé des fractions rationnelles $f/g \in k(t_1, \ldots, t_n)$ dont un dénominateur g (ou, si on préfère, le dénominateur réduit) ne s'annule pas à l'origine (on vérifie facilement qu'il s'agit d'un anneau) : son idéal maximal est alors formé de celles dont le *numérateur* s'annule à l'origine.

Plus généralement, si $\mathfrak{p}$ est un idéal premier de $k[t_1, \ldots, t_n]$, l'anneau des fractions rationnelles de la forme f/g avec $f, g \in k[t_1, \ldots, t_n]$ et $g \notin \mathfrak{p}$ (i.e., le dénominateur réduit n'est pas identiquement nul sur $V(\mathfrak{p})$) est un anneau local dont l'idéal maximal est formé des fractions avec $f \in \mathfrak{p}$ et $g \notin \mathfrak{p}$.

Proposition 3.2.10. Un anneau de valuation est un anneau local.

Démonstration. Pour $x \in R$, on sait que $x \notin R^\times$ équivaut à $v(x) > 0$. Il s'ensuit que l'ensemble de ces x est un idéal (c'est un groupe additif d'après la propriété

5. On l'appelle **idéal de Jacobson** de R, et on peut montrer que c'est toujours l'intersection des idéaux *maximaux* de R : comparer avec 1.1.9.

(ii) de 3.2.3, et il est absorbant pour la multiplication d'après la propriété (i)). On conclut par 3.2.8. ☺

3.2.11. Le corps quotient d'un anneau local R par son idéal maximal $\mathfrak{m}$ s'appelle le **corps résiduel** de R ; en particulier, ceci s'applique à un anneau de valuation avec $\mathfrak{m} := \{x \in R : v(x) > 0\}$ comme on vient de l'expliquer. Lorsque v est une valuation sur un corps K, on peut bien sûr parler de son corps résiduel, défini comme le quotient de l'anneau de valuation $R := \{x \in K : v(x) \geq 0\}$ par l'unique idéal maximal de ce dernier.

On note parfois $\mathcal{O}_v$ pour l'anneau de valuation d'une valuation v et $\mathfrak{m}_v$ pour son idéal maximal, et enfin $\varkappa_v$ pour son corps résiduel $\mathcal{O}_v/\mathfrak{m}_v$. On remarquera que si la valuation v est au-dessus de k, alors $\varkappa_v$ est une extension de k.

Une valuation non-triviale au-dessus de k sur un corps K de fonctions sur k comme en 3.1.1 s'appelle une **place** (ou, s'il faut être plus explicite, une k-place) de K. (Cette terminologie est essentiellement utilisée pour le corps des fonctions d'une courbe $K = k(C)$, i.e., en degré de transcendance 1, auquel cas on peut indifféremment parler de places de C.) On notera parfois $\mathscr{V}_K$ (ou, s'il faut être plus explicite, $\mathscr{V}_{K/k}$) l'ensemble des k-places de K.

Proposition 3.2.12. Soit K un corps, soit $A \subseteq K$ un sous-anneau et soit $\mathfrak{p}$ un idéal premier (cf. 1.1.3) de A. Alors il existe un anneau de valuation R de K tel que $A \subseteq R \subseteq K$ et que $\mathfrak{m} \cap A = \mathfrak{p}$ en notant $\mathfrak{m}$ l'idéal maximal de R (cf. 3.2.10).

Démonstration. Soit A' l'ensemble des quotients $\frac{a}{q}$ avec $a \in A$ et $q \notin \mathfrak{p}$: on rappelle que le produit de deux éléments qui ne sont pas dans $\mathfrak{p}$ n'est pas dans $\mathfrak{p}$, ce qui permet de voir que A' est stable par addition et multiplication (en utilisant les formules usuelles $\frac{a}{q} + \frac{a'}{q'} = \frac{aq'+a'q}{qq'}$ et $\frac{a}{q} \cdot \frac{a'}{q'} = \frac{aa'}{qq'}$) ; il contient bien sûr 0 et 1 et est donc un sous-anneau de K vérifiant $A \subseteq A' \subseteq K$. L'idéal $\mathfrak{p}'$ de A' formé des $\frac{p}{q}$ avec $p \in \mathfrak{p}$ et $q \notin \mathfrak{p}$ est maximal et est même l'unique idéal maximal de A' (tout élément qui n'est pas dans $\mathfrak{p}'$ est inversible dans A' par construction ; on pourrait remarquer au passage que le corps $A'/\mathfrak{p}'$ est le corps des fractions de $A/\mathfrak{p}$) ; notons par ailleurs que $\mathfrak{p}' \cap A = \mathfrak{p}$ (car si $\frac{p}{q} =: a \in A$ avec les notations d'avant, $p = aq \in \mathfrak{p}$ implique $a \in \mathfrak{p}$ vu que $q \notin \mathfrak{p}$).

On remplace maintenant A par A' et $\mathfrak{p}$ par $\mathfrak{p}'$: comme on vient de le voir, ceci permet de supposer que A est un anneau *local*, dont l'unique idéal maximal est noté $\mathfrak{p}$.

Soit $\mathscr{F}$ l'ensemble des sous-anneaux R de K contenant A et tels que $1 \notin \mathfrak{p}R$ (où $\mathfrak{p}R$ est l'idéal de R engendré par $\mathfrak{p}$). Alors $\mathscr{F}$ est non vide (il contient A) et si $\mathscr{T}$ est une partie de $\mathscr{F}$ totalement ordonnée par l'inclusion (= : chaîne) alors $R := \bigcup_{S \in \mathscr{T}} S$ est encore dans $\mathscr{F}$ (la réunion d'une chaîne de sous-anneaux est un sous-anneau pour la même raison que dans la preuve de 1.1.7, ce sous-anneau contient évidemment A, et si on pouvait écrire 1 comme combinaison linéaire à

coefficients dans R d'éléments de $\mathfrak{p}$, ces coefficients seraient déjà dans un S de $\mathscr{T}$, une contradiction). Ainsi, le principe 1.1.6 s'applique et il existe R maximal pour l'inclusion. On va montrer que R répond au problème posé.

Tout d'abord, vérifions que R est un anneau local : comme $\mathfrak{p}R \neq R$ par hypothèse, il est inclus (cf. 1.1.7) dans un idéal maximal $\mathfrak{m}$. Si on répète la construction du premier paragraphe de cette preuve, on peut considérer l'anneau R' des quotients $\frac{a}{q}$ avec $a \in R$ et $q \notin \mathfrak{m}$: la maximalité de R impose qu'en fait $R' = R$ c'est-à-dire que tout élément n'appartenant pas à $\mathfrak{m}$ est inversible dans R. L'idéal maximal $\mathfrak{m}$ est donc unique, i.e., R est un anneau local, comme annoncé.

De plus, on a $\mathfrak{m} \cap A = \mathfrak{p}$ puisque l'inclusion $\supseteq$ est claire et que $\mathfrak{p}$ est un idéal maximal de A. Il reste simplement à vérifier que R est un anneau de valuation.

Si $x \in K$ n'appartient pas à R, alors $R[x]$ est un sous-anneau de K contenant R (donc A) et strictement plus grand que R : par maximalité de ce dernier, c'est que $1 \in \mathfrak{p}R[x]$, c'est-à-dire qu'on peut écrire $1 = a_0 + a_1 x + \cdots + a_n x^n$ avec $a_i \in \mathfrak{p}R$, et en particulier $a_i \in \mathfrak{m}$. Mais $1 - a_0 \notin \mathfrak{m}$ est inversible dans R puisque R est local, donc on peut multiplier l'égalité précédente par son inverse, et quitte à appeler $b_i = a_i/(1 - a_0)$, on a $1 = b_1 x + \cdots + b_n x^n$ avec $b_i \in \mathfrak{m}$. Choisissons une telle relation avec n le plus petit possible. De même, si x^{-1} n'appartient pas à R, on choisit une relation $1 = c_1 x^{-1} + \cdots + c_m x^{-m}$ avec $c_i \in \mathfrak{m}$ et m le plus petit possible. Sans perte de généralité, on peut supposer $n \geq m$: alors quitte à multiplier la dernière relation par $b_n x^n$ et la soustraire à la précédente, on obtient une relation $1 = b'_1 x + \cdots + b'_{n-1} x^{n-1}$, toujours avec $b'_i \in \mathfrak{m}$, ce qui contredit la minimalité de n. On a donc bien montré que $x \in K$ implique soit $x \in R$ soit $x^{-1} \in R$. ☺

3.2.13. En particulier, si $I \subseteq J$ sont deux idéaux premiers de $k[t_1, \ldots, t_d]$, si bien que $Z(I) \supseteq Z(J)$ sont deux fermés de Zariski irréductibles (cf. 2.4.11), alors le corps des fonctions rationnelles $K = \mathrm{Frac}(k[t_1, \ldots, t_d]/I)$ de $Z(I)$ (cf. 3.1.10) a au moins une valuation v qui soit positive sur $A := k[t_1, \ldots, t_d]/I$ et strictement positive sur son idéal premier J/I (et exactement sur ces éléments de A). Cette situation nous importera notamment dans le cas où $Z(I)$ est une courbe (par exemple $I = (P)$ avec $P \in k[x, y]$ irréductible comme on a vu en 3.1.3) et $Z(J)$ un point de la courbe (plus exactement, un point fermé, cf. 2.4.8(3)).

Proposition 3.2.14. Soit K un corps et soit $A \subseteq K$ un sous-anneau. Alors l'intersection B de tous les anneaux de valuations de K contenant A coïncide exactement avec l'ensemble des éléments $x \in K$ qui sont **entiers [algébriques]** sur A au sens où il existe un $f \in A[t]$ *unitaire* non constant tel que $f(x) = 0$.

(Cet ensemble B, qui est donc un sous-anneau de K, s'appelle la **fermeture intégrale** de A dans K, ou **clôture intégrale** lorsque K est le corps des fractions de A.)

En particulier, si k est un sous-corps de K, alors l'intersection de tous les anneaux de valuations de K au-dessus de k est la fermeture algébrique (cf. 1.3.7) de k dans K.

Démonstration. Montrons d'abord que si $x \in K$ est entier sur A alors x appartient à n'importe quel anneau de valuation R de K contenant A. Or si $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ avec $a_i \in A$ (et notamment $a_i \in R$), on ne peut pas avoir $v_R(x) < 0$ car on a $v(x^i) = i\, v(x)$, et si $a \in R$, comme $v(a) \geq 0$, on a $v(ax^i) \geq i\, v(x)$; par conséquent, si on a une relation $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, la valuation du terme x^n est $n\, v(x)$ donc strictement plus petite que celle de n'importe quel autre terme de la somme, ce qui interdit qu'elle puisse être nulle (cf. 3.2.5). Ceci montre une inclusion.

Montrons réciproquement que si x n'est pas entier sur A alors il existe un anneau de valuation de K contenant A auquel x n'appartient pas. Pour cela, posons $y = x^{-1} \in K$, et considérons l'anneau $A[y]$ qu'il engendre avec A et l'idéal $yA[y]$ qu'il engendre dans cet anneau. On a $1 \notin yA[y]$ sans quoi il y aurait une relation du type $1 = a_1 y + \cdots + a_n y^n$, donc $x^n = a_1 x^{n-1} + \cdots + a_n$ et x serait entier sur A, or on a supposé le contraire. L'idéal $yA[y]$ est donc strict et il existe donc (cf. 1.1.7) un idéal maximal $\mathfrak{p}$ de $A[y]$ le contenant (donc contenant y). D'après 3.2.12, il existe R anneau de valuation de K contenant $A[y]$ et dont l'idéal maximal contienne $\mathfrak{p}$. En particulier, $v_R(y) > 0$, donc $v_R(x) < 0$, ce qui signifie $x \notin R$, ce qu'on voulait montrer. ☺

Les anneaux de valuation *discrète* (ceux dont le groupe des valeurs est $\mathbb{Z}$) ont des propriétés supplémentaires que n'ont pas les anneaux de valuation en général :

Proposition 3.2.15. Soit $\mathcal{O}$ un anneau de valuation *discrète*, dont on note $\mathfrak{m}$ l'idéal maximal (cf. 3.2.10) et v la valuation. Alors :

(a) un élément $t \in \mathcal{O}$ engendre $\mathfrak{m}$ en tant qu'idéal si et seulement si $v(t) = 1$ (où 1 désigne le plus petit élément strictement positif du groupe des valeurs, qui identifie ce dernier à $\mathbb{Z}$), et en fixant t un élément comme on vient de dire (et il en existe),

(b) tout élément $x \neq 0$ de K a une représentation unique sous la forme $x = ut^r$ avec $u \in \mathcal{O}^\times$ et $r \in \mathbb{Z}$, auquel cas on a $r = v(x)$,

(c) de même, tout idéal $I \neq (0)$ de $\mathcal{O}$ est l'idéal $\{x \in \mathcal{O} : v(x) \geq r\}$ engendré par t^r (en particulier, $\mathcal{O}$ est principal) pour un certain $r \in \mathbb{N}$.

Un élément t tel que $v(t) = 1$ s'appelle une **uniformisante** de l'anneau de valuation discrète $\mathcal{O}$.

Démonstration. Montrons le (a). Si t engendre $\mathfrak{m}$, alors clairement $v(t) = 1$ car pour tout x tel que $v(x) > 0$, on peut écrire $x = tz$ pour un certain $z \in \mathcal{O}$ (puisque $x \in \mathfrak{m}$ et que t engendre cet idéal), donc $v(x) \leq v(t)$ et t est bien

de la valuation strictement positive la plus petite possible. Réciproquement, si $v(t) = 1$ (la valuation strictement positive la plus petite possible), et si $x \in \mathfrak{m}$, alors $v(x) \geq v(t)$ par la minimalité supposée de $v(t)$, c'est-à-dire $x/t \in \mathcal{O}$, ce qui prouve bien $x \in t\mathcal{O}$.

L'existence de t est simplement une conséquence de la définition de la valuation (ou de l'élément 1 dans le groupe des valeurs).

Montrons maintenant le (b). Si $v(x) = r$ alors $u := x/t^r$ est de valuation nulle, c'est-à-dire dans $\mathcal{O}^\times$. Réciproquement, si $x = ut^r$, on a $v(x) = v(u) + rv(t) = r$ puisque $v(u) = 0$ et $v(t) = 1$.

Remarquons que les multiples de ut^r dans $\mathcal{O}$ sont les éléments de la forme $uu't^{r+r'}$ c'est-à-dire les éléments de valuation $\geq r$.

Montrons enfin le (c). Si $x \in I$ a la plus petite valuation possible pour un élément de I, disons $x = ut^r$ comme on vient de voir, et alors $t^r \in I$ donc I contient l'idéal engendré par t^r, qui d'après le paragraphe précédent est $\{x \in \mathcal{O} : v(x) \geq r\}$; mais réciproquement, tout élément de I a une valuation supérieure ou égale à $v(x) = r$ par minimalité supposée de x, donc il y a bien égalité entre I et l'idéal $\{x \in \mathcal{O} : v(x) \geq r\}$ engendré par t^r. ☺

3.3 Places des courbes

Lemme 3.3.1. Soit K un corps de fonctions de courbe sur k (cf. 3.1.1) et v une valuation de K au-dessus de k (cf. 3.2.3).

(A) Si x vérifie $0 \neq v(x) < \infty$, alors x est transcendant sur k et le corps K est *fini* sur $k(x)$.

(B) Si $x_1, \ldots, x_n$ vérifient $0 < v(x_1) < v(x_2) < \cdots < v(x_n) < \infty$, alors $x_1, \ldots, x_n$ sont linéairement indépendants sur $k(x_n)$, et en particulier le degré $[K : k(x_n)]$ (lequel est fini d'après (A)) est supérieur ou égal à n.

(C) Si x vérifie $0 < v(x) < \infty$, alors $[\varkappa_v : k] \leq [K : k(x)]$ (en particulier, il est fini d'après (A)), où $\varkappa_v := \mathcal{O}_v/\mathfrak{m}_v$ est le corps résiduel de la place v.

(Voir aussi le théorème 3.6.2 plus bas pour une généralisation de (B) et (C).)

Démonstration. Pour ce qui est de (A), on peut le déduire de 3.2.14, mais on va le faire directement. Commençons par supposer $v(x) < 0$ et cherchons à montrer la transcendance de x : on a $v(x^i) = i\,v(x)$, et si $a \in k^\times$, comme $v(a) = 0$ (puisque la valuation est au-dessus de k), on a $v(ax^i) = i\,v(x)$; par conséquent, si on a une relation $x^n + a_1x^{n-1} + \cdots + a_n = 0$, la valuation du terme x^n est $n\,v(x)$ donc strictement plus petite que celle de n'importe quel autre terme de la somme, ce qui interdit qu'elle puisse être nulle (cf. 3.2.5). Le cas $v(x) > 0$ s'en déduit en passant à x^{-1} (l'inverse d'un algébrique étant encore algébrique, cf. 1.3.7). Enfin, une fois connu le fait que x est transcendant, donc une *base* de transcendance de K sur k

(cf. 1.5.4 (1a) et (3)), l'extension $k(x) \subseteq K$ est algébrique, et comme elle est aussi de type fini, elle est *finie* (cf. 1.3.6(2)). Ceci démontre (A).

Passons à l'affirmation (B) : supposons qu'on ait $f_1 x_1 + \cdots + f_n x_n = 0$ avec $f_i \in k(x_n)$ non tous nuls. Posons $x := x_n$. On a vu ci-dessus que x était transcendant sur k, c'est-à-dire que les f_i sont des fractions rationnelles en x. Quitte à chasser les dénominateurs, on peut supposer $f_i \in k[x]$ et que x ne les divise pas tous. Soit $c_i = f_i(0)$ le terme constant de f_i (non tous nuls, donc), mettons $f_i = c_i + x g_i$ où $g_i \in k[x]$, et soit j le plus petit possible tel que $c_j \neq 0$: ainsi, on a $c_j x_j + \cdots + c_n x_n + g_1 x x_1 + \cdots + g_n x x_n = 0$. Or la valuation $v(c_j x_j) = v(x_j)$ est strictement plus petite que celle de n'importe quel autre terme dans cette somme (puisque $v(g_i) \geq 0$ et $v(x x_i) = v(x_n) + v(x_i) > v(x_n) \geq v(x_j)$), ce qui interdit que la somme puisse être nulle (cf. 3.2.5). Ceci démontre (B).

Pour ce qui est de (C) : considérons des éléments $b_1, \ldots, b_n$ de $\varkappa_v$ qui sont linéairement indépendants sur k, et soient $y_i \in \mathcal{O}_v$ qui représente la classe $b_i \in \varkappa_v = \mathcal{O}_v/\mathfrak{m}_v$: on aura montré (C) si on montre que $y_1, \ldots, y_n$ sont linéairement indépendants sur $k(x)$. Supposons qu'on ait $f_1 y_1 + \cdots + f_n y_n = 0$ avec $f_i \in k(x)$ non tous nuls. On a vu en (A) que x était transcendant sur k, c'est-à-dire que les f_i sont des fractions rationnelles en x. Quitte à chasser les dénominateurs, on peut supposer $f_i \in k[x]$ et que x ne les divise pas tous. Soit $c_i = f_i(0) \in k$ le terme constant de f_i (non tous nuls, donc), mettons $f_i = c_i + x g_i$ où $g_i \in k[x]$. On a $c_1 y_1 + \cdots + c_n y_n + g_1 x y_1 + \cdots + g_n x y_n = 0$. Tous les termes de cette somme sont dans $\mathcal{O}_v$: en réduisant modulo $\mathfrak{m}_v$, les $g_i x y_i$ disparaissent car $x \in \mathfrak{m}_v$ par hypothèse, et les y_i se réduisent en b_i. On a donc $c_1 b_1 + \cdots + c_n b_n = 0$, une contradiction. Ceci démontre (C). ☺

Proposition 3.3.2. Soit K un corps de fonctions de courbe sur k (cf. 3.1.1). Alors toutes les valuations (cf. 3.2.3) non-triviales de K au-dessus de k (=places de K) sont *discrètes* — c'est-à-dire qu'il existe un plus petit élément strictement positif dans le groupe des valeurs et que tous les éléments en sont des multiples entiers, si bien que le groupe des valeurs peut s'identifier à $\mathbb{Z}$ pour son ordre usuel.

Notamment, tous les anneaux de valuation non-triviaux de K au-dessus de k vérifient les propriétés annoncées en 3.2.15 (par exemple, ce sont des anneaux *principaux*).

Démonstration. Soit $v \colon K \to \Gamma \cup \{\infty\}$ une valuation non-triviale de K au-dessus de k. Le fait que v est non-triviale assure qu'il existe $x \in K$ tel que $0 \neq v(x) < \infty$, et alors le (A) du lemme 3.3.1 montre que K est fini sur $k(x)$. Quitte à remplacer x par $\frac{1}{x}$, on peut supposer $v(x) > 0$. Montrons qu'il existe un élément $z \in K$ avec $v(z)$ strictement positif minimal : si ce n'est pas le cas de x, il existe x' tel que $0 < v(x') < v(x) < \infty$, et si x' n'est toujours pas minimal, il existe x'' tel que $0 < v(x'') < v(x') < v(x) < \infty$, et ainsi de suite : ce processus

doit terminer en au plus $[K : k(x)]$ étapes d'après le (B) du lemme, donc il existe un $z \in K$ avec $v(z)$ strictement positif minimal. Notons $1 := v(z)$.

Il reste à montrer que tout élément u de Γ est un multiple entier de 1. C'est trivial si $u = 0$ donc quitte à remplacer éventuellement u par $-u$ on peut supposer $u > 0$. Toujours d'après le (B) du lemme, il n'est pas possible qu'on ait $u > r \cdot 1$ (en notant $r \cdot 1$ pour $1 + 1 + \cdots + 1$ avec r termes) pour tout $r \in \mathbb{N}$. Il existe donc r minimal tel que $r \cdot 1 \leq u$, et comme $u - (r \cdot 1) \geq 0$, par minimalité de 1 dans Γ, il est soit nul soit ≥ 1, mais le dernier cas implique $(r+1) \cdot 1 \leq u$ ce qui contredit la minimalité de r : on a donc $u = r \cdot 1$, ce qu'on voulait montrer. ☺

3.3.3. La propriété (C) du lemme 3.3.1 montre que, pour toute place v d'un corps de fonctions K de courbe sur k, le corps résiduel $\varkappa_v$ est une extension finie, donc algébrique, de k. Le degré $[\varkappa_v : k]$ s'appelle aussi **degré** de la place v. S'il vaut 1, c'est-à-dire si $\varkappa_v = k$, la place v est dite **rationnelle**. C'est notamment le cas si k est *algébriquement clos*.

3.3.4. Toujours pour K un corps de fonctions de courbe sur k, si $f \in K$ et si $v \in \mathscr{V}_K$ (i.e., v est une place de K), on peut définir $f(v) \in \varkappa_v$ (l'**évaluation** de f en la place v) comme valant :

— la classe de $f \in \mathcal{O}_v$ modulo $\mathfrak{m}_v$, lorsque $v(f) \geq 0$,

— le symbole spécial [6] ∞ lorsque $v(f) < 0$ (on peut dire que f a un **pôle** en v).

Ceci permet de voir un élément de K comme une fonction sur $\mathscr{V}_K$ (mais comme elle prend des valeurs dans des ensembles $\varkappa_v$ différents, ce n'est pas très agréable, sauf si k est algébriquement clos auquel cas on a bien affaire à une fonction $\mathscr{V}_K \to k \cup \{\infty\}$).

On dira symétriquement que f a un **zéro** en la place v lorsque $v(f) > 0$, c'est-à-dire que $f(v) = 0$ (le 0 de $\varkappa_v$ étant défini comme l'idéal $\mathfrak{m}_v := \{x \in \mathcal{O}_v : v(x) > 0\}$).

Pour récapituler, on pour $f \in K$ et $v \in \mathscr{V}_K$, on a trois possibilités exclusives :

— $v(f) > 0$, ce qui équivaut à $f(v) = 0$, ce qui équivaut à $f \in \mathfrak{m}_v$: on dit que f a un zéro en v ;

— $v(f) < 0$, ce qui équivaut à $f(v) = \infty$, ce qui équivaut à $f \notin \mathcal{O}_v$: on dit que f a un pôle en v ;

— $v(f) = 0$, ce qui équivaut à $f(v) \in \varkappa_v^\times$, ce qui équivaut à $f \in \mathcal{O}_v^\times$.

La valuation $v(f)$ peut également être appelée **multiplicité** du zéro de f en v (même si cette terminologie est un peu abusive ou bizarre si en fait $v(f) < 0$), et inversement, au moins si $v(f) < 0$, l'entier $-v(f)$ peut être appelé multiplicité du pôle de f en v.

6. Le symbole ∞ introduit ici (pour désigner un pôle d'une fonction) est différent de celui introduit en 3.2.2 pour la valuation de 0 : on pourrait noter ce dernier $+\infty$ ou ∞_Γ pour éviter la confusion, mais en pratique il y a peu de chances de se tromper.

On rappelle qu'on a donné le nom d'**uniformisante** en v à un $f \in K$ tel que $v(f) = 1$ (c'est-à-dire, avec la terminologie qu'on vient d'introduire, une fonction qui a un zéro d'ordre exactement 1 en v). On parle aussi de **paramètre local** pour K en v.

3.3.5. D'après la proposition 3.2.14, la fermeture algébrique $\tilde{k}$ de k dans K coïncide avec l'ensemble des fonctions $f \in K$ telles que $v(f) \geq 0$ pour toute place $v \in \mathscr{V}_K$, autrement dit, les fonctions qui n'ont pas de pôle. En passant à l'inverse, il s'agit également de l'ensemble des fonctions qui n'ont pas de zéro (plus la fonction identiquement nulle). Ces fonctions seront dites **constantes**. Pour dire les choses autrement, les conditions conditions suivantes sur $f \in K$ sont équivalentes :

— f est transcendant sur k,
— il existe au moins une place v de K où f ait un pôle,
— f n'est pas nul, et il existe au moins une place v de K où f ait un zéro,
— f n'est pas constante,

(la dernière étant la définition du mot « constant » dans ce contexte). Le corps $\tilde{k}$ peut s'appeler **corps des constantes** de K (sur k).

(Notons au passage que puisque $\tilde{k} \neq K$, c'est-à-dire que K est de degré de transcendance 1 sur k, il existe toujours des places — chose qui n'était pas triviale *a priori* !)

3.3.6. En général, $\tilde{k}$ peut être strictement plus grand que k : un exemple de ce phénomène a été donné en 3.1.9 (où $\tilde{k} = k(\sqrt{-1})$, par exemple $k = \mathbb{R}$ et $\tilde{k} = \mathbb{C}$). On sera souvent amené à faire l'hypothèse que $\tilde{k} = k$, c'est-à-dire que k est *algébriquement fermé* (cf. 1.3.7) dans K ; ceci se produit notamment lorsque $K = k(C)$ est défini (au sens de 3.1.3 ou plus généralement de 3.1.10) par un polynôme $P \in k[x, y]$ ou un fermé de Zariski $Z(I)$ *géométriquement* irréductible (cf. 2.4.12) : en effet, on a signalé en 3.1.10 que si c'est le cas, disons avec $K = \mathrm{Frac}(k[t_1, \ldots, t_d]/I)$, d'après la proposition 2.5.9, dans le corps $K.k^{\mathrm{alg}} = \mathrm{Frac}(k^{\mathrm{alg}}[t_1, \ldots, t_d]/(I.k^{\mathrm{alg}}))$, les sous-corps K et k^{alg} sont linéairement disjoints sur k et en particulier, leur intersection $\tilde{k}$ est égale à k.

(On peut bien sûr aussi se ramener à $\tilde{k} = k$ en redéfinissant simplement k comme égal à $\tilde{k}$, à condition qu'on ne tienne pas à garder le corps de base fixé.)

3.3.7. La remarque suivante peut être utile : tous les corps résiduels $\varkappa_v$ sont des extensions de $\tilde{k}$ (puisque $\tilde{k}$ est l'intersection de tous les $\mathcal{O}_v$, on a des morphismes d'anneaux $\tilde{k} \to \varkappa_v$). Notamment, $[\tilde{k} : k]$ divise tous les $\deg(v) = [\varkappa_v : k]$ (cf. 3.3.3), et en particulier, s'il existe une place *rationnelle* (c'est-à-dire $\deg(v) = 1$), ou simplement deux places de degrés premiers entre eux, on a $\tilde{k} = k$.

3.4 Les places de la droite projective

3.4.1. On a vu en 3.1.2 comment fabriquer des valuations non-triviales (au-dessus de k) du corps $k(t)$ des fractions rationnelles en une indéterminée sur k : à savoir, si h est un polynôme unitaire irréductible de $k[t]$, on appelle $v_h(f)$ l'exposant de h dans la factorisation de f en polynômes irréductibles (si $f \in k[t]$, c'est bien l'exposant de la décomposition en produit d'irréductibles, et pour une fraction rationnelle f/g on peut définir $v_h(f/g) = v_h(f) - v_h(g)$ sachant qu'au plus un de ces termes sera non-nul lorsque f/g est en forme irréductible, cf. 3.2.6). Si on préfère, au moins si k est parfait, on peut aussi le noter $v_\xi(f)$ (ou $\mathrm{ord}_\xi(f)$), où ξ est une racine quelconque de h dans une clôture algébrique k^{alg} fixée (puisque le polynôme h se factorise dans k^{alg} comme le produit des $t - \xi_i$ où ξ_i parcourt les conjugués de ξ, cf. 1.9.7 et aussi 3.1.2).

Il est facile de vérifier que ces v_h sont bien des valuations au sens de 3.2.3 (il suffit par exemple de vérifier les propriétés définissant une valuation sur des polynômes, ce qui est immédiat, et de les déduire pour les fractions rationnelles). On peut aussi vérifier directement que $\mathcal{O}_h := \{f \in k(t) : v_h(f) \geq 0\}$ (c'est-à-dire l'ensemble des fractions rationnelles dont h ne divise pas le dénominateur réduit) est bien un anneau de valuation.

3.4.2. Le corps résiduel $\varkappa_h$ de la place v_h n'est autre que le corps de rupture $k[t]/(h)$ de h sur k (si $\deg h = 1$, c'est simplement k). En effet, on a *a priori* $\varkappa_h = \mathcal{O}_h/(h)$ (cf. 3.2.15(a)) ; mais en fait tout élément de $\mathcal{O}_h$ peut s'écrire sous la forme f/g avec g non multiple de h, et quitte à utiliser une relation de Bézout $ug + wh = 1$ (avec $u, w \in k[t]$), on voit que f/g est la somme de $uf \in k[t]$ et de $w\frac{f}{g}h \in h\mathcal{O}_h$, si bien que finalement $\mathcal{O}_h/(h) = k[t]/(h)$.

Ce qu'on a appelé degré de la place v_h est donc simplement le degré de h ; et les places rationnelles parmi les v_h sont celles avec $\deg h = 1$, c'est-à-dire, en fait, l'évaluation en un certain point $x \in k$ (si $h(t) = t - x$: on rappelle que le reste de la division euclidienne de $f \in k[t]$ par $t - x$ est simplement $f(x)$). Plus généralement, le paragraphe précédent montre que la valeur de f en la place v_ξ définie par un $\xi \in k^{\mathrm{alg}}$ (c'est-à-dire par son polynôme minimal h) peut s'identifier à la valeur $f(\xi)$ dans le corps $k(\xi) = k[t]/(h)$.

3.4.3. Il existe une autre valuation non-triviale de $k(t)$ au-dessus de k, à savoir celle qui à une fraction rationnelle f/g associe la différence $\deg(g) - \deg(f)$ du degré du dénominateur et du degré du numérateur. On la notera v_∞ (ou ord_∞).

L'anneau de valuation $\mathcal{O}_\infty$ associé est l'anneau des fractions rationnelles dont le degré du dénominateur est supérieur ou égal à celui du numérateur, et le corps résiduel est simplement k, le morphisme d'évaluation dans $\mathcal{O}_\infty/(\frac{1}{t}) = k$ étant donné par la valeur de la fraction rationnelle en ∞ (telle que définie en 3.1.2). On peut s'en convaincre en remplaçant t par $\frac{1}{t}$, ce qui définit un automorphisme de $k(t)$ transformant la place v_0 en v_∞ et vice versa.

On vient de construire un certain nombre de places de $k(t)$: en fait, ce sont

les seules :

Proposition 3.4.4. Soit k un corps. Alors les places (=valuations non-triviales au-dessus de k) du corps $k(t)$ des fractions rationnelles en une indéterminée sont exactement les places v_h (associant à $f \in k(t)$ l'exposant de h dans la factorisation de f en polynômes irréductibles) et v_∞ (qui à une fraction rationnelle associe le degré du dénominateur moins le degré du numérateur).

Démonstration. On a vu que les places qu'on a dites en sont bien, et elles sont visiblement distinctes. Soit maintenant v une place de $k(t)$.

Considérons d'abord le cas $v(t) \geq 0$. Alors $v(f) \geq 0$ pour tout polynôme $f \in k[t]$ (puisque $\mathcal{O}_v$ est un anneau). Il existe nécessairement un $f \in k[t]$ tel que $v(f) > 0$ sans quoi la valuation serait triviale. Mais si $v(f) > 0$, l'un de ses facteurs (unitaires) irréductibles, disons h, vérifie aussi $v(h) > 0$. On a nécessairement $v(q) = 0$ pour tout autre polynôme unitaire irréductible q car si $v(q)$ était strictement positif, une relation de Bézout $uq + wh = 1$ avec $u, w \in k[t]$ donnerait $v(1) > 0$ ce qui est absurde. Bref, h est le seul polynôme unitaire irréductible dont la valuation est non-nulle, et il est alors clair que, $v(f)$ pour $f \in K$ quelconque, est le produit de $v(h)$ par l'exposant de h dans la factorisation de f en polynômes irréductibles. Puisque la valeur 1 doit être atteinte par la valuation, on a forcément $v(h) = 1$, et on a fini.

Considérons maintenant le cas $v(t) < 0$. Alors $v(f) = \deg f \cdot v(t)$ pour tout polynôme f (puisque le terme dominant a une valuation strictement plus petite que n'importe quel autre terme de la somme). On a donc $v(f/g) = (\deg f - \deg g)\, v(t)$ pour toute fraction rationnelle f/g, et nécessairement $v(t) = -1$ puisque la valeur 1 doit être atteinte. ☺

3.4.5. Lorsque k est algébriquement clos, les places de $\mathbb{P}^1_k$ (:= la droite projective sur k, c'est-à-dire la courbe dont le corps des fonctions est $k(t)$) peuvent donc s'identifier aux éléments de k (le point $x \in k$ étant identifié à la valuation qui à $f \in k(t)$ associe l'ordre $v_x(f) =: \mathrm{ord}_x(f)$ du zéro, ou l'opposé de l'ordre du pôle, de f en x) plus un élément supplémentaire ∞ (correspondant à la valuation $v_\infty =: \mathrm{ord}_\infty$ à l'infini). C'est cette vision (« la droite des points de k plus un point à l'infini ») qu'on a à l'esprit en traitant $\mathbb{P}^1_k$ de « droite projective ».

Lorsque k n'est plus supposé algébriquement clos, les places de $\mathbb{P}^1_k$ sont un peu plus compliquées ; il faut imaginer que chaque polynôme unitaire irréductible $h \in k[t]$ définit une place qui correspond intuitivement à l'*ensemble* de ses racines dans la clôture algébrique : si k est parfait, il s'agit exactement des *orbites* sous le groupe de Galois absolu (comparer avec 1.9.7 et 2.4.8(3)). Par exemple, les places de $\mathbb{P}^1_{\mathbb{R}}$ autres que ∞ sont soit les réels soit les *paires* de complexes conjugués (en particulier, la place associée à l'unitaire irréductible t^2+1 correspond à l'ensemble $\{\pm\sqrt{-1}\}$ de ses racines, la multiplicité de $t^2 + 1$ dans la factorisation d'une

fraction rationnelle réelle est l'ordre du zéro ou l'opposé de l'ordre du pôle en $+\sqrt{-1}$ ou $-\sqrt{-1}$ indifféremment).


Il ne faut pas s'imaginer que la place ∞ soit intrinsèquement différente des autres. Elle ne l'est qu'à cause du choix particulier de l'indéterminée t dans $k(t)$. Mais si $a, b, c, d \in k$ sont quatre éléments de k vérifiant $ad - bc = 1$, et si on pose $t' := \frac{at+b}{ct+d} \in k(t)$, il est facile de voir que t' est aussi un transcendant et $k(t') = k(t)$ (puisqu'on peut retrouver t à partir de t' par $t = \frac{dt'-b}{-ct'+a}$), et la place qui était notée ∞ dans $k(t)$ devient $\frac{a}{c}$ quand on voit ce même corps comme $k(t')$ (autrement dit, il faut comprendre que quand t « vaut » ∞, alors t' « vaut » $\frac{a}{c}$), et inversement la place qui est notée ∞ dans $k(t')$ correspond à $-\frac{d}{c}$ dans $k(t)$. (Pour dire la même chose autrement, on a un isomorphisme $k(t') \xrightarrow{\sim} k(t)$ donné par $f \mapsto f(\frac{at+b}{ct+d})$, et la composition par cet isomorphisme transforme la valuation v_∞ sur $k(t)$ en la valuation $v_{a/c}$ sur $k(t')$.) Bref, la place ∞ est simplement la place où *la coordonnée choisie* (i.e., le transcendant choisi pour engendrer $k(\mathbb{P}^1_k)$) a son pôle.

3.5 L'indépendance des valuations

3.5.1. Pour comprendre le théorème suivant, il faut se rappeler que si v est une valuation, dire que $v(f - g)$ est grand signifie que f et g sont « très proches au sens de v » : par exemple, pour des fractions rationnelles, $v_\xi(f - g) \geq r$ signifie que les développements limités de f et g en ξ coïncident jusqu'à l'ordre $r - 1$ (c'est-à-dire jusqu'à un terme d'erreur en $O((t - \xi)^r)$ si ξ est fini, et en $O(t^{-r})$ si $\xi = \infty$).

On peut d'ailleurs dire que f et g sont « r-proches pour v » lorsque $v(f-g) \geq r$, et constater qu'il s'agit d'une relation d'équivalence compatible avec l'addition.

Le résultat suivant a donc la signification intuitive : donnés des développements limités $f_1, \ldots, f_n$ en des places $v_1, \ldots, v_n$, on peut trouver une unique fonction f qui les approche simultanément à n'importe quel ordre r_i fixé.

Théorème 3.5.2 (« approximation faible »)**.** Soit K un corps, soient $v_1, \ldots, v_n$ des valuations discrètes sur K deux à deux distinctes, et soient $f_1, \ldots, f_n \in K$ et $r_1, \ldots, r_n \in \mathbb{Z}$. Alors il existe $f \in K$ tel que $v_i(f - f_i) \geq r_i$ pour chaque i. On peut d'ailleurs obtenir $v_i(f - f_i) = r_i$ si on veut.

Démonstration. On procède en plusieurs étapes.

Primo, observons que pour chaque couple (i, j) avec $i \neq j$ il existe $x \in K$ tel que $v_i(x) \geq 0$ et $v_j(x) < 0$ ou vice versa ($v_i(x) < 0$ et $v_j(x) \geq 0$). Ceci résulte du fait que les anneaux $\mathcal{O}_i$ et $\mathcal{O}_j$ des valuations v_i et v_j sont distincts (vu que l'anneau détermine la valuation, cf. 3.2.3), donc il existe x qui appartient à l'un mais pas à l'autre, c'est-à-dire $x \in \mathcal{O}_i$ et $x \notin \mathcal{O}_j$ ou vice versa.

Secundo, montrons que pour chaque couple (i,j) avec $i \neq j$ il existe $x \in K$ tel que $v_i(x) > 0$ et $v_j(x) < 0$. Or on vient de voir qu'on pouvait trouver z qui vérifie soit $v_i(z) \geq 0$ et $v_j(z) < 0$ soit vice versa. Dans le premier cas, prenons y tel que $v_i(y) > 0$: en posant $x = yz^s$, on a $v_i(x) > 0$, et $v_j(x) = v_j(y) + s\, v_j(z)$ qui sera strictement négatif pour s assez grand. Dans le second cas ($v_i(z) < 0$ et $v_j(z) \geq 0$), prenons y tel que $v_j(y) < 0$: en posant $x = y/z^s$, on a $v_j(x) < 0$, et $v_i(x) = v_i(y) - s\, v_i(z)$ qui sera strictement positif pour s assez grand vu que $v_i(z) < 0$. On a donc bien trouvé x qui répond au problème posé.

Tertio, montrons que pour chaque i il existe $x \in K$ tel que $v_i(x) > 0$ et $v_j(x) < 0$ pour *chaque* $j \neq i$. On peut sans perte de généralité supposer $i = 1$ et on procède par récurrence sur n : par hypothèse de récurrence, on trouve y tel que $v_1(y) > 0$ et $v_j(y) < 0$ pour $1 < j < n$, et par le point précédent, on trouve z tel que $v_1(z) > 0$ et $v_n(z) < 0$. On pose $x = y + z^s$. On a déjà $v_1(x) > 0$. Pour ce qui est des v_j, si $v_j(z) < 0$ (ce qui est notamment le cas de $j = n$), on a $v_j(x) < 0$ lorsque s est assez grand pour assurer $s\, v_j(z) < v_j(y)$; et si au contraire $v_j(z) \geq 0$ mais que $v_j(y) < 0$, on a aussi $v_j(x) < 0$. Donc dans tous les cas, pour s assez grand, x répond aux conditions demandées.

Quarto, montrons que pour chaque i et chaque r il existe $h \in K$ tel que $v_i(h-1) \geq r$ et $v_j(h) \geq r$ pour chaque $j \neq i$. On vient de voir qu'il existe $x \in K$ tel que $v_i(x) > 0$ et $v_j(x) < 0$ pour chaque $j \neq i$: on pose $h = (1+x^s)^{-1}$ pour s assez grand : on a $h - 1 = x^s/(1+x^s)$ et $v_i(1+x^s) = 0$ donc $v_i(h-1) = s\, v_i(x)$ peut être rendu arbitrairement grand ; et $v_j(h) = -v_j(1+x^s) = -s\, v_j(x)$ peut aussi être rendu arbitrairement grand.

Quinto, en appelant h_i un élément comme on vient de le trouver au point précédent ($v_i(h_i - 1) \geq r$ et $v_j(h_i) \geq r$ pour chaque $j \neq i$) pour un r à déterminer, on pose $f = f_1 h_1 + \cdots + f_n h_n$. On a alors $f - f_i = f_i(h_i - 1) + \sum_{j \neq i} f_j h_j$, donc $v_i(f - f_i) \geq \min_j\{v_i(f_j)\} + r$ peut être rendu arbitrairement grand en prenant r assez grand (précisément, plus grand que $r_i - \min_j\{v_i(f_j)\}$ pour chaque i). Ceci montre l'affirmation principale du théorème.

Sexto, si on souhaite obtenir $v_i(f - f_i) = r_i$ exactement, on choisit z_i tel que $v_i(z_i) = r_i$ exactement, puis on utilise le point précédent pour trouver g tel que $v_i(g - f_i) > r_i$ pour chaque i, et une nouvelle fois pour trouver z tel que $v_i(z - z_i) > r_i$ pour chaque i : alors $f := g + z$ vérifie $v_i(f - f_i) = v_i((g - f_i) + (z - z_i) + z_i)$, or $v_i(z_i) = r_i$ et $v_i(g - f_i) > r_i$ et $v_i(z - z_i) > r_i$, si bien que $v_i(f - f_i) = r_i$ comme souhaité. ☺

Corollaire 3.5.3. L'ensemble $\mathscr{V}_{K/k}$ des places d'un corps K de fonctions de courbe sur k est infini.

Démonstration. On a vu en 3.3.2 que tous les éléments de $\mathscr{V}_{K/k}$ sont des valuations *discrètes*. Si cet ensemble était fini, disons $\mathscr{V}_{K/k} = \{v_1, \ldots, v_n\}$, d'après le résultat 3.5.2 qu'on vient de montrer, il existerait $f \in K$ tel que

$v_i(f) = 1$ pour tout i, c'est-à-dire $v(f) = 1$ pour toute place $v \in \mathscr{V}_{K/k}$. Un tel f contredit l'équivalence en 3.3.5 (une fonction qui n'a aucun pôle doit être constante, mais une fonction constante est soit identiquement nulle soit n'a pas de zéro non plus). ☺

3.6 L'identité du degré

Lemme 3.6.1. Soit K un corps de fonctions de courbe sur k, soient $v_1, \ldots, v_n$ des places de K sur k deux à deux distinctes, et soient $r_1, \ldots, r_n \in \mathbb{N}$. Si v est une place de K, posons $r_v = r_i$ si $v = v_i$ et $r_v = 0$ si v n'est pas l'une des v_i. On considère le k-espace vectoriel

$$L := \{f \in K : (\forall v)\, v(f) \geq -r_v\}$$

des fonctions $f \in K$ qui ont en v_i un pôle de multiplicité au plus r_i et aucun pôle ailleurs qu'en $v_1, \ldots, v_n$.

Alors la dimension de L est $\leq [\tilde{k} : k] + \sum_{i=1}^n r_i \deg(v_i)$ où on rappelle que $\deg(v_i)$ (degré de la place v_i, cf. 3.3.3) est $\dim_k(\varkappa_i)$ avec $\varkappa_i := \mathcal{O}_i/\mathfrak{m}_i$ le corps résiduel de v_i, et où $\tilde{k}$ est le corps des constantes (fermeture algébrique de k dans K, cf. 3.3.5).

Plus exactement, la dimension de L est $[\tilde{k} : k]$ lorsque tous les r_i sont nuls, et augmente d'au plus $\deg(v_i)$ lorsque r_i est augmenté de 1.

En particulier, cette dimension est *finie*.

Démonstration. On procède par récurrence sur $\sum_{i=1}^n r_i$. Si les r_i sont tous nuls, $L = \{f \in K : (\forall v)\, v(f) \geq 0\}$ est précisément $\tilde{k}$ (cf. 3.2.14), donc la formule est vérifiée dans ce cas.

Supposons l'inégalité vérifiée pour certains r_j et montrons qu'elle l'est encore quand on remplace l'un d'entre eux, disons r_i, par $r_i' := r_i + 1$, avec $r_j' = r_j$ si $j \neq i$. Soit L' l'espace correspondant (défini de la même façon que L mais avec les r_j') ; il est trivial que $L \subseteq L'$. Soit $z \in K$ tel que $v_i(z) = r_i' = r_i + 1$ (on n'impose pas de contrainte aux autres places). Alors pour $f \in L'$ on a $v_i(fz) \geq 0$, c'est-à-dire $fz \in \mathcal{O}_i$, et de plus $fz \in \mathfrak{m}_i$ se produit exactement lorsque $v_i(fz) \geq 1$ c'est-à-dire que $f \in L$. On a donc défini une application k-linéaire $L' \to \varkappa_i$ envoyant f sur la classe de $fz \in \mathcal{O}_i$ modulo $\mathfrak{m}_i$, dont le noyau est L. En particulier, $\dim_k(L') \leq \dim_k(\varkappa_i) + \dim_k(L) \leq [\tilde{k} : k] + \sum_{i=1}^n r_i' \deg(v_i)$, ce qui conclut la récurrence ; et on a bien montré l'affirmation commençant par « plus exactement ». ☺

Théorème 3.6.2 (« identité du degré »)**.** Soit K un corps de fonctions de courbe sur k, soit $x \in K$ non constant (cf. 3.3.5) : alors l'ensemble des places où x a un

zéro (c'est-à-dire $v(x) > 0$) est fini, et si on les note $v_1, \ldots, v_n$, on a :

$$\sum_{i=1}^{n} v_i(x)\ \deg(v_i) = [K : k(x)]$$

(Rappelons que $[K : k(x)]$ est fini, cf. 3.3.1(A).)

Démonstration. Les deux inégalités se démontrent indépendamment. Dans l'inégalité $\leq$, on n'utilisera pas le fait que $v_1, \ldots, v_n$ soient *toutes* les places où x a un zéro, ce qui prouvera, en particulier, qu'il y en a bien un nombre fini (majoré par $[K : k(x)]$).

Montrons d'abord l'inégalité $\leq$.

Pour chaque i, soit $d_i := \deg(v_i)$ et $r_i := v_i(x)$, et soient $z_{i,1}, \ldots, z_{i,d_i} \in \mathcal{O}_i$ dont les classes modulo $\mathfrak{m}_i$ forment une base de $\varkappa_i$ comme k-espace vectoriel (notamment $v_i(z_{i,u}) = 0$). Quitte à utiliser le théorème 3.5.2 on peut, sans changer cette propriété des $z_{i,u}$, assurer de surcroît que $v_j(z_{i,u}) \geq r_j$ pour tout $j \neq i$. On choisit enfin t_i tel que $v_i(t_i) = 1$ et $v_j(t_i) = 0$ si $j \neq i$ (de nouveau en utilisant 3.5.2). On va montrer que les $z_{i,u}t_i^s$ pour $1 \leq i \leq n$ et $1 \leq u \leq d_i$ et $0 \leq s < r_i$ sont linéairement indépendants sur $k(x)$, ce qui, comme leur nombre est $\sum_{i=1}^{n} r_i d_i$, donnera bien l'inégalité $\leq$.

Supposons donc qu'on ait une relation linéaire non-triviale

$$\sum_{j=1}^{n} \sum_{u=1}^{d_j} \sum_{s=0}^{r_j-1} f_{j,u,s} z_{j,u} t_j^s = 0$$

avec $f_{j,u,s} \in k(x)$. On sait que x est transcendant sur k, c'est-à-dire que les $f_{j,u,s}$ sont des fractions rationnelles en x. Quitte à chasser les dénominateurs, on peut supposer $f_{j,u,s} \in k[x]$ et que x ne les divise pas tous. Soit e le plus petit s tel que l'un des $f_{j,u,e}$ ne soit pas divisible par x (i.e., non nul en 0) et soit i correspondant (i.e., un indice tel que l'un des $f_{i,u,e}$ ne soit pas divisible par x).

On a $\sum_{j=1}^{n} \sum_{u=1}^{d_j} \sum_{s=0}^{r_j-1} f_{j,u,s} z_{j,u} t_j^s t_i^{-e} = 0$. Considérons la valuation v_i du terme $f_{j,u,s} z_{j,u} t_j^s t_i^{-e}$, qui vaut $v_i(f_{j,u,s}) + v_i(z_{j,u}) + s\, v_i(t_j) - e$. Remarquons que $v_i(f_{j,u,s}) \geq 0$ puisque $f_{j,u,s} \in k[x]$. On considère plusieurs cas :

- si $j \neq i$, on a $v_i(z_{j,u}) \geq r_i$ et $v_i(t_j) = 0$ donc la valuation considérée est au moins $0 + r_i + 0 - e > 0$;
- lorsque $j = i$ (si bien que $v_i(z_{i,u}) = 0$) et $s < e$, on a $f_{j,u,s} = x g_{j,u,s}$ pour un certain $g \in k[x]$, la valuation considérée vaut au moins $r_i + 0 + s - e > 0$ car $e < r_i$;
- lorsque $j = i$ et $s > e$, la valuation considérée vaut au moins $0 + 0 + s - e > 0$

— reste les termes où $j = i$ et $s = e$, où la valuation considérée vaut au moins $0 + 0 + s - e = 0$.

Bref, tous les termes de la somme sont dans $\mathcal{O}_i$ et tous ceux où $j \neq i$ ou bien $s \neq e$ sont dans $\mathfrak{m}_i$. En réduisant modulo $\mathfrak{m}_i$, on obtient donc

$$\sum_{u=1}^{d_i} f_{i,u,e}(0)\, z_{i,u}(v_i) = 0 \in \varkappa_i$$

(où $z_{i,u}(v_i)$ est la réduction de $z_{i,u}$ modulo $\mathfrak{m}_i$) et au moins un des $f_{i,u,e}(0)$ est non nul. Mais ceci contredit l'indépendance linéaire sur k des $z_{i,u}(v_i) \in \varkappa_i$.

Montrons maintenant l'inégalité $\geq$.

Soit $m := [K : k(x)]$ et soit $z_1, \ldots, z_m$ une base de K comme $k(x)$-espace vectoriel. Ajoutons aux v_i toutes les places où l'un des z_j a un pôle, et posons $r_i = \max(v_i(x), 0)$ (c'est-à-dire $r_i = v_i(x)$ pour les v_i de départ et $r_i = 0$ pour les nouveaux), et aussi $s_i = \max(\max_j\{v_i(z_j)\}, 0)$. Soit enfin L_N l'espace vectoriel $\{f \in K : (\forall i)\, v_i(f_i) \geq -(s_i + Nr_i)\}$: on a alors $x^{-\ell} z_j \in L_N$ pour tout j et tout $0 \leq \ell \leq N$, et les $x^{-\ell} z_j$ sont linéairement indépendants sur k (puisque x est transcendant d'après 3.3.5 et que les z_j sont linéairement indépendants sur $k(x)$). D'après le lemme 3.6.1, on en déduit $N \sum_i r_i \deg(v_i) + C \geq (N+1)m$ où C est une constante (à savoir $\sum_i s_i \deg(v_i) + [\tilde{k} : k]$). Or ceci n'est possible, pour N grand, que si $\sum_i r_i \deg(v_i) \geq m$, ce qui montre l'inégalité annoncée. ☺

Corollaire 3.6.3. Soit K un corps de fonctions de courbe sur k, soit $x \in K$ non nul. Alors l'ensemble des places où x a un zéro ou un pôle est fini.

Démonstration. Si x est constante (cf. 3.3.5), le résultat est trivial (l'ensemble des pôles est vide, et l'ensemble des zéros est vide si $x \neq 0$). Si x n'est pas constant, le théorème 3.6.2 montre que l'ensemble des zéros a pour cardinal au plus $[K : k(x)]$, qui est fini ; et pour ce qui est des pôles, il suffit de remplacer x par x^{-1}. ☺

3.6.4. L'identité du degré généralise le fait qu'un polynôme de degré d a au plus d zéros, et même exactement d si on compte les zéros avec multiplicité dans une clôture algébrique. Pour voir le rapport, considérons $h \in k[t]$ de degré $d > 0$: alors h (vu comme un élément de $k(t)$) est transcendant sur k d'après 3.3.1(A), mieux, l'extension $k(h) \subseteq k(t)$ est algébrique de degré d. En effet, t est racine du polynôme $h(u) - h \in k(h)[u]$ de degré d en l'indéterminée u ; et pour montrer que $1, \ldots, t^{d-1}$ sont linéairement indépendants sur $k(h)$, supposons que $z_0 + z_1 t + \cdots + z_{d-1} t^{d-1} = 0$ avec $z_i \in k(h)$, disons $z_i = f_i \circ h$ où $f_i \in k(u)$, quitte à chasser les dénominateurs on peut supposer $f_i \in k[u]$ non tous multiples de u et quitte à écrire $f_i = c_i + u g_i$ où $c_i = f_i(0) \in k$ non tous nuls et $g_i \in k[u]$, c'est-à-dire $z_i = c_i + h \cdot g_i \circ h$, et on a $c_0 + c_1 t + \cdots + c_{d-1} t^{d-1} \in k[t]/(h)$,

ce qui est impossible. Bref, $[k(t) : k(h)] = \deg h$ dans ce cas, et l'énoncé du théorème 3.6.2 est que $\sum_{i=1}^{n} v_i(h) \deg(v_i) = \deg h$ où les v_i sont les places où h a un zéro ; d'après la section 3.4, les $v_i(h)$ sont les multiplicités des facteurs irréductibles h_i divisant h (i.e., « où h a un zéro »), et les $\deg(v_i)$ sont les degrés des facteurs h_i en question.

Si $h \in k(t)$ est une fraction rationnelle, la même formule permet de voir que $[k(t) : k(h)]$ est égal à la somme des $v_i(h) \deg(v_i)$ comme précédemment, c'est-à-dire le degré du numérateur, plus éventuellement la contribution de la place ∞ (si $v_\infty(h) \geq 0$), pour laquelle $\deg(v_\infty) = 1$ et $v_\infty(h)$ est le degré du dénominateur moins celui du numérateur. Autrement dit, le terme de gauche de l'égalité du théorème 3.6.2 est le *maximum* du degré du numérateur et du degré du dénominateur : il est raisonnable de définir ainsi le degré d'une fraction rationnelle.

En s'inspirant de ces cas particuliers, on fait la définition générale suivante :

Définition 3.6.5. Soit K un corps de fonctions de courbe sur k et soit $h \in K$: alors on pose $\deg(h) = [K : k(h)]$ si h est non constant, et $\deg(h) = 0$ si h est constante (**degré** de x). Ainsi, le théorème 3.6.2 se réécrit :

$$\sum_{i=1}^{n} v_i(h) \deg(v_i) = \deg(h)$$

dès que $h \neq 0$, où $v_1, \ldots, v_n$ sont les places où h a un zéro.

On a vu ci-dessus que si h est un polynôme, $\deg h$ est bien le degré au sens usuel, et si h est une fraction rationnelle, $\deg h$ est le maximum du degré du numérateur et du dénominateur.

3.7 Diviseurs sur les courbes

Définition 3.7.1. Soit $K = k(C)$ un corps de fonctions de courbe sur k. Un **diviseur** sur la courbe C est une combinaison linéaire formelle à coefficients entiers de k-places de K : autrement dit, le groupe $\mathrm{Div}(C)$ des diviseurs est défini comme le groupe abélien libre $\bigoplus_{P \in \mathscr{V}_{K/k}} \mathbb{Z}$ de base l'ensemble $\mathscr{V}_{K/k}$ des places de C. On notera $\sum_P n_P(P)$ une telle combinaison (où P parcourt les places de C et les n_P sont des entiers relatifs tous nuls sauf un nombre fini).

Le **degré** d'un diviseur $D = \sum_P n_P \cdot (P)$ est défini comme $\deg(D) := \sum_P n_P \deg(P)$ où $\deg(P)$ est le degré de la place P (cf. 3.3.3). On notera $\mathrm{Div}^0(C)$ le sous-groupe des diviseurs de degré zéro (i.e., le noyau de $\deg$).

Un diviseur D est dit **effectif** (ou abusivement : « positif ») lorsque tous les coefficients n_P sont positifs. On note $D \geq 0$ pour cette affirmation.

Définition 3.7.2. Si $K = k(C)$ est un corps de fonctions de courbe sur k, et si $f \in K$ est non nulle, on appelle respectivement **diviseur des zéros**, **diviseur des pôles** et **diviseur principal** associés à la fonction f les diviseurs

$$f^*((0)) := \sum_{P\,:\,\mathrm{ord}_P(f)>0} \mathrm{ord}_P(f)\cdot(P)$$
$$f^*((\infty)) := \sum_{P\,:\,\mathrm{ord}_P(f)<0} -\mathrm{ord}_P(f)\cdot(P)$$
$$\mathrm{div}(f) := f^*((0)-(\infty)) = \sum_P \mathrm{ord}_P(f)\cdot(P)$$

où ord_P (aussi noté v_P) est la valuation correspondant[7] à la place P (i.e., l'ordre [du zéro] en P de f).

3.7.3. Le théorème 3.6.2 affirme que le degré du diviseur des zéros $f^*((0))$ ou du diviseur des pôles $f^*((\infty))$ de f est égal au degré de l'extension $k(f) \subseteq K$, qu'on peut appeler simplement « degré » de f. Le degré du diviseur principal $\mathrm{div}(f)$, qui est égal au degré du diviseur des zéros moins le diviseur des pôles, est donc nul : $\mathrm{div}(f) \in \mathrm{Div}(C)^0$.

Il faut souligner que $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ d'après la propriété 3.2.3(i) des valuations : div définit donc un morphisme $K^\times \to \mathrm{Div}(C)$ (dont le noyau est le groupe $\tilde{k}^\times$ des constantes non nulles).

Si $D = \sum_P n_P \cdot (P)$ est un diviseur, certains appellent « valuation » ou « ordre » ou « multiplicité » de D en P l'entier n_P (ce qui fait donc que la valuation de $\mathrm{div}(f)$ en P est par définition exactement la valuation $\mathrm{ord}_P(f)$ de f en P). On évitera d'abuser de cette terminologie.

Définition 3.7.4. Si $K = k(C)$ est un corps de fonctions de courbe sur k, on appelle **diviseur principal** un diviseur sur C (forcément de degré zéro, comme on l'a vu) de la forme $\mathrm{div}(f) := \sum_P \mathrm{ord}_P(f)\cdot(P)$ pour une certaine fonction $f \in k(C)$ non nulle. Les diviseurs principaux forment un sous-groupe du groupe des diviseurs, et même des diviseurs de degré zéro : on dit que deux diviseurs D et D' sont **linéairement équivalents**, et on note $D \sim D'$, lorsque leur différence $D' - D$ est un diviseur principal. Le groupe des diviseurs (resp. diviseurs de degré 0) modulo les diviseurs principaux (=modulo équivalence linéaire) s'appelle **groupe de Picard** (resp. groupe de Picard de degré zéro) de la courbe C, et est noté $\mathrm{Pic}(C)$ (resp. $\mathrm{Pic}^0(C)$).

7. Formellement, avec la présentation utilisée ici, $\mathrm{ord}_P = v_P$ et P sont *égaux*. Il est cependant utile de les distinguer (pour la clarté des notations ou pour la vision géométrique des choses), et d'appeler P une « place » de la courbe (voire, un « point fermé »), et ord_P la « valuation en la place P » ou « valuation correspondant à la place P ».

3.7.5. À titre d'exemple, calculons le groupe de Picard de la droite projective $\mathbb{P}^1_k$ sur un corps k. On a vu en 3.4 que les places de $\mathbb{P}^1_k$ sont en correspondance avec les polynômes unitaires irréductibles de $k[t]$, plus une place « à l'infini » ∞. Disons qu'on note P_h la place correspondant à la valuation v_h, pour h unitaire irréductible, qui vérifie $\deg P_h = \deg h$; pour h de degré un, c'est-à-dire de la forme $t - x$, on peut noter simplement x la place en question (i.e., $v_x(f) = \mathrm{ord}_x(f)$ est l'ordre du zéro, ou l'opposé de l'ordre du pôle, d'une fonction rationnelle f en x).

Si $D = n_\infty(\infty) + \sum_h n_h \cdot (P_h) \in \mathrm{Div}(\mathbb{P}^1_k)$ est un diviseur sur $\mathbb{P}^1_k$ (où n_∞ et les n_h sont des entiers, et tous les n_h sont nuls sauf un nombre fini), on peut définir une fonction $f := \prod_h h^{n_h}$ qui vérifie $v_h(f) = n_h$ par construction, donc $\mathrm{div}(f) = n'_\infty(\infty) + \sum_h n_h \cdot (P_h)$ où $n'_\infty = -\sum_h n_h \deg(h)$ est la valuation $v_\infty(f)$ puisque $v_\infty(h) = -\deg(h)$. Les diviseurs D et $\mathrm{div}(f)$ ne diffèrent donc que par $(n_\infty - n'_\infty) \cdot (\infty)$, et ce diviseur est nul si en fait $D \in \mathrm{Div}^0(\mathbb{P}^1_k)$ (c'est-à-dire que le degré $n_\infty + \sum_h n_h \deg(h) = n_\infty - n'_\infty$ de D est nul). Ceci prouve que tout diviseur est linéairement équivalent à un multiple de (∞) et que les diviseurs de degré zéro sur $\mathbb{P}^1_k$ sont exactement les diviseurs principaux. Autrement dit, $\mathrm{Pic}(\mathbb{P}^1_k) = \mathbb{Z}$ (l'isomorphisme étant donné par le degré) et $\mathrm{Pic}^0(\mathbb{P}^1_k) = 0$.

3.8 Espaces de Riemann-Roch

Définition 3.8.1. Soit $K = k(C)$ un corps de fonctions de courbe sur k, et soit $D = \sum_P n_P \cdot (P)$ un diviseur sur C (c'est-à-dire la donnée d'un entier n_P pour chaque place de P, tous nuls sauf un nombre fini). On appelle **espace de Riemann-Roch** associé au diviseur D le k-espace vectoriel

$$\begin{aligned}\mathscr{L}(D) &:= \{f \in K : (\forall P)\ \mathrm{ord}_P(f) \geq -n_P\} \\ &= \{f \in K^\times : \mathrm{div}(f) + D \geq 0\} \cup \{0\}\end{aligned}$$

des fonctions rationnelles sur C qui ont en chaque place P un pôle d'ordre au plus n_P (ou un zéro d'ordre au moins n_P dans le cas où n_P est strictement négatif ; et pas de pôle si n_P est nul). Ici, $\mathrm{ord}_P(f)$ désigne la valuation de f correspondant [8] à la place P, c'est-à-dire le coefficient de P dans $\mathrm{div}(f)$.

On note $\ell(D)$ la dimension de $\mathscr{L}(D)$ comme k-espace vectoriel (on va rappeler qu'elle est toujours finie).

Proposition 3.8.2. En notant D et D' des diviseurs sur une même courbe :

(o) Si $\mathscr{L}(D) \neq 0$ alors il existe D' linéairement équivalent à D (cf. 3.7.4) et effectif.

(i.a) En notant 0 le diviseur nul, on a $\mathscr{L}(0) = \tilde{k}$. (i.b) Si $D < 0$ (au sens où $-D$ est effectif et non nul), on a $\mathscr{L}(D) = 0$.

8. Voir note 7 page 77.

(ii) Si D et D' sont linéairement équivalents ($D \sim D'$), c'est-à-dire si $D' - D = \mathrm{div}(f)$ pour une certaine fonction f alors on a un isomorphisme $\mathscr{L}(D') \xrightarrow{\sim} \mathscr{L}(D)$ donné par $g \mapsto fg$. En particulier, $\mathscr{L}(D')$ et $\mathscr{L}(D)$ ont même dimension $\ell(D') = \ell(D)$.

(iii) Si $D \leq D'$ (au sens où $D' - D$ est effectif) alors $\mathscr{L}(D) \subseteq \mathscr{L}(D')$ et la dimension du k-espace vectoriel $\mathscr{L}(D')/\mathscr{L}(D)$ est au plus $\deg D' - \deg D$.

(iv) Le k-espace vectoriel $\mathscr{L}(D)$ est de dimension finie : plus précisément, si $D = D_+ - D_-$ avec D_+ et D_- effectifs, alors $\ell(D) \leq [\tilde{k} : k] + \deg D_+$.

Démonstration. (o) Si $f \in \mathscr{L}(D)$ alors $D' := \mathrm{div}(f) + D$ est effectif (par définition de $\mathscr{L}(D)$) et linéairement équivalent à D (par définition de l'équivalence linéaire).

(i) découle de 3.3.5 (une fonction sans pôle, c'est-à-dire un élément de $\mathscr{L}(0)$, est constante, et elle n'a pas non plus de zéro, c'est-à-dire n'appartient pas à $\mathscr{L}(D)$ pour $D < 0$, sauf si elle est nulle).

(ii) Il suffit de constater que si $D' = D + \mathrm{div}(f)$ alors $\mathrm{div}(g) + D' \geq 0$ équivaut à $\mathrm{div}(fg) + D \geq 0$ puisque les membres de gauche sont égaux (vu que $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$).

(iii) (sauf l'affirmation $\mathscr{L}(D) \subseteq \mathscr{L}(D')$, qui est triviale), et (iv) pour $D_- = 0$, sont une reformulation de 3.6.1. Le cas général de (iv) s'en déduit trivialement (augmenter D_- ne peut que faire diminuer $\ell(D)$). ☺

Proposition 3.8.3. En notant D un diviseur sur une courbe :
— Si $\deg D < 0$ alors $\ell(D) = 0$.
— Si $\deg D = 0$ et $\ell(D) \neq 0$ alors $\ell(D) = [\tilde{k} : k]$ et $D \sim 0$.

Démonstration. Dire que $\ell(D) \neq 0$ signifie que pour un certain f on a $D' := \mathrm{div}(f) + D \geq 0$. Or le degré de $\mathrm{div}(f)$ est nul (et le degré d'un diviseur effectif D' est évidemment positif), donc le degré de D est ≥ 0. De plus, si le degré de D (donc de D') est nul, cela signifie que $\mathrm{div}(f) + D = 0$, c'est-à-dire $D \sim 0$, qui entraîne $\ell(D) = 1$. ☺

3.9 Différentielles de Kähler

Définition 3.9.1. Soit k un corps (ou même un anneau) et A une k-algèbre. On appelle espace des **différentielles de Kähler** de A sur k, et on note $\Omega^1_{A/k}$, le A-module engendré par des symboles formels dx (ou $d_A x$ si on veut être plus précis) pour chaque $x \in A$, sujets aux relations :

(i) $d(x + x') = dx + dx'$ si $x, x' \in A$, et $d(cx) = c\,dx$ si $c \in k$ et $x \in A$ (i.e., $d\colon A \to \Omega^1_{A/k}$ est k-linéaire), et

(ii) $d(xy) = x\,dy + y\,dx$ si $x, y \in A$

(autrement dit, $\Omega^1_{A/k}$ est le quotient du A-module libre de base $\{dx : x \in A\}$ par le sous-module engendré par les relations qu'on vient de dire, autrement dit les $d(x+x') - dx - dx'$ pour $x, x' \in A$, les $d(cx) - c\,dx$ pour $c \in k$ et $x \in A$ et les $d(xy) - x\,dy - y\,dx$ pour $x, y \in A$).

3.9.2. Cette définition n'est pas très élégante. Une définition plus satisfaisante serait de dire que $d\colon A \to \Omega^1_{A/k}$ a la propriété « universelle » que toute autre application $\delta\colon A \to M$ (où M est un A-module) k-linéaire vérifiant $\delta(xy) = x\,\delta(y) + y\,\delta(x)$ (on dit que δ est une **dérivation** de A à valeurs dans M) se factorise de façon unique par d (i.e., il existe une application A-linéaire $u\colon \Omega^1_{A/k} \to M$ unique tel que $\delta(x) = u(dx)$). Il est purement formel de vérifier que cette propriété caractérise complètement $\Omega^1_{A/k}$, et est bien vérifiée de l'objet construit en 3.9.1.

Pour une extension de corps $k \subseteq K$, le K-module $\Omega^1_{K/k}$ est facile à décrire, à condition de faire une hypothèse de séparabilité que nous énonçons maintenant.

Proposition 3.9.3. Soit $k \subseteq K$ une extension de corps 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 (cf. 1.4.1 ; lire : les extensions $k^p \subseteq K^p$ et $k^p \subseteq k$, tous deux contenues dans K, sont linéairement disjointes),

— il existe une base de transcendance $(t_1, \ldots, t_n)$ pour laquelle K est (algébrique) *séparable* sur $k(t_1, \ldots, t_n)$ (cf. 1.7.9).

(Plus généralement, si on ne suppose plus $k \subseteq K$ de type fini, la première condition est équivalente à la seconde affirmée pour toutes les sous-extensions de type fini $k \subseteq K_0$ de K.)

Références. [Matsumura 1989, théorèmes 26.1 et 26.2] ☺

3.9.4. Lorsque ces deux conditions équivalentes sont satisfaites, on dit que l'extension $k \subseteq K$ (non nécessairement algébrique !) est **séparable**. (Il va de soi, en vertu de la seconde condition, que pour une extension algébrique, on retrouve la définition de « séparable » donnée en 1.7.9 ; comparer aussi avec 1.7.8 pour la première condition ci-dessus dans le cas d'une extension algébrique.) Dans les conditions de la seconde condition, on dit aussi que $(t_1, \ldots, t_n)$ est une base de transcendance **séparante**.

3.9.5. Toute extension de corps en caractéristique 0 est séparable (la première condition de 3.9.3 doit se lire comme trivialement vraie en caractéristique 0). Plus généralement, lorsque k est *parfait* (cf. 1.8.1 ; par exemple, un corps fini), *toute* extension $k \subseteq K$, algébrique ou non, est séparable d'après 1.8.7 (qui généralise donc la remarque 1.8.3).

Une autre condition suffisante pour que $k \subseteq K$ soit séparable est que K et k^{alg} soient linéairement disjoints au-dessus de k dans K^{alg} (on parle d'extension

régulière dans ce contexte ; il est facile de voir, en utilisant le fait que le Frobenius est un automorphisme de K^{alg}, que ceci implique la première condition de 3.9.3). Ceci s'applique lorsque K est le corps de fonctions d'un fermé de Zariski *géométriquement* irréductible (cf. 2.4.12, et 3.1.10).

On retiendra donc surtout ceci : 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 géométriquement irréductible (par exemple, C est défini dans le plan par l'annulation d'un polynôme P géométriquement irréductible, c'est-à-dire irréductible sur k^{alg}, cf. 3.1.9, ou plus généralement par un fermé de Zariski géométriquement irréductible, cf. 3.1.10),

alors l'extension $k \subseteq K$ est séparable. On fera cette hypothèse à chaque fois qu'il sera question de différentielles sur une courbe.

Beaucoup d'auteurs limitent la notion de « corps de fonctions de courbe » à ceux qui sont séparables sur le corps de base, voire, les corps de fonctions de courbes géométriquement irréductibles : on pourrait donc en faire de même.


L'hypothèse « k parfait » simplifie beaucoup de choses, mais elle ne trivialise pas pour autant *toutes* les questions de séparabilité : notamment, même si k est parfait, il n'est pas vrai que toute base de transcendance de K sur k soit automatiquement une base de transcendance séparante (contre-exemple : en caractéristique $p > 0$, si $k(t)$ désigne le corps des fractions rationnelles, t^p est une base de transcendance de $k(t)$ sur k, et pourtant elle n'est pas séparante, car l'extension $k(t^p) \subseteq k(t)$ n'est pas séparable).

Proposition 3.9.6. Soit $k \subseteq K$ une extension de corps de type fini et séparable. Si $(t_1, \ldots, t_n)$ une base de transcendance séparante (i.e., telle que K est algébrique séparable sur $k(t_1, \ldots, t_n)$, cf. 3.9.4), alors $\Omega^1_{K/k}$ est un K-espace vectoriel de base $dt_1, \ldots, dt_n$. Réciproquement, si $t_1, \ldots, t_n \in K$ sont tels que $dt_1, \ldots, dt_n$ soient linéairement indépendants sur K, alors ils sont une base de transcendance séparante.

Références. [Matsumura 1989, théorèmes 26.6 et 26.8], [Fried & Jarden 2008, lemme 2.8.3] ☺

3.9.7. En particulier, si $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), alors $\Omega^1_{K/k}$ *est un* K*-espace vectoriel de dimension* 1, et une base (c'est-à-dire, un élément non nul) en est donnée par dt pour n'importe quel $t \in K$ qui soit une base de transcendance séparante, autrement t non constant et $k(t) \subseteq K$ (algébrique) séparable.

Si t est un tel élément, c'est-à-dire que tout élément ω de $\Omega^1_{K/k}$ est multiple de dt par un coefficient uniquement défini, on peut noter $\frac{\omega}{dt} \in K$ ce coefficient, et

notamment, il y a un sens à écrire $\frac{df}{dt}$ lorsque $f \in K$.

3.9.8. À titre d'exemple, $\Omega^1_{k(t)/k}$ est le $k(t)$-espace vectoriel de dimension 1 et de base le symbole formel dt. Pour toute autre fraction rationnelle $f \in k(t)$, on a bien sûr $df = f'(t)\,dt$ (en appliquant les règles usuelles de différentiation), donc $df/dt = f'$ est bien la dérivée au sens usuel d'une fraction rationnelle.

(Ceci montre au passage que l'hypothèse de séparation n'est pas anodine dans 3.9.6 : en caractéristique $p > 0$, on a $d(t^p) = 0$, et pourtant t^p est bien une base de transcendance de $k(t)$ sur k — mais ce n'est pas, c'est là le point à remarquer, une base de transcendance *séparante*, c'est-à-dire que $k(t)$ n'est pas séparable sur $k(t^p)$.)


Il ne faut pas s'imaginer que tous les éléments de $\Omega^1_{K/k}$ soient des df pour certaines fonctions f. Par exemple, il est bien connu que $\frac{dt}{t} \in \Omega^1_{k(t)/k}$ n'est pas de la forme df (il faudrait prendre $f = \log t$, mais ce n'est pas une fraction rationnelle).

3.9.9. La question de savoir quand $dt \neq 0$ est facile en caractéristique 0 (si t n'est pas constant, il est transcendant sur k, cf. 3.3.5, donc est une base de transcendance, automatiquement séparante en caractéristique 0, et 3.9.6 donne $dt \neq 0$) ; elle l'est moins en caractéristique positive, surtout si k n'est pas parfait. On va essayer de l'éclaircir :

Proposition 3.9.10. Soit $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), soit $P \in \mathscr{V}_{K/k}$ une place et soit $R = \mathcal{O}_P$ l'anneau de valuation correspondant[9] ($\{f \in K : \mathrm{ord}_P(f) \geq 0\}$). Alors le R-module $\Omega^1_{R/k}$ s'identifie au sous-R-module de $\Omega^1_{K/k}$ engendré par les df pour $f \in R$ (autrement dit, $d_R f \mapsto d_K f$ définit une application R-linéaire injective, ce qui permet d'identifier $\Omega^1_{R/k}$ à l'image de celle-ci). De plus, $\Omega^1_{R/k}$ est *libre* de rang 1 comme R-module : autrement dit, si on a fixé $t \in R$ une uniformisante (c'est-à-dire $\mathrm{ord}_P(t) = 1$), il existe $\alpha \in \Omega^1_{R/k}$ tel que tout élément $\omega \in \Omega^1_{K/k}$ s'écrive de façon unique $\omega = ut^i\alpha$ pour $u \in R^\times$ et $i \in \mathbb{Z}$, et qu'on ait $i \geq 0$ si et seulement si $\omega \in \Omega^1_{R/k}$ (cf. 3.2.15(b)).

Références. [Hartshorne 1977, théorème II.8.8 et lemme II.8.9] ☺

Définition 3.9.11. Si $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), alors pour une place P de C et une différentielle de Kähler $\omega \in \Omega^1_{K/k}$, on appelle $\mathrm{ord}_P(\omega)$ l'entier i de la proposition 3.9.10, c'est-à-dire le plus grand i tel qu'on ait $\omega/t^i \in \Omega^1_{\mathcal{O}_P/k}$ où t est une uniformisante en P (concrètement, il s'agit donc du plus grand i tel qu'on puisse écrire $\omega = g_1\,df_1 + \cdots + g_N\,df_N$ avec $\mathrm{ord}_P(g_j) \geq i$ et $\mathrm{ord}_P(f_j) \geq 0$).

9. Voir note 7 page 77.

Cet entier l'appelle ordre du zéro, ou opposé de l'ordre du pôle, de ω en P ; lorsque $\mathrm{ord}_P(\omega) \geq 0$, on dit que ω est **holomorphe** en P, lorsque $\mathrm{ord}_P(\omega) > 0$, on dit qu'elle a un zéro en P, lorsque $\mathrm{ord}_P(\omega) < 0$, on dit qu'elle a un pôle en P.

3.9.12. Si $\omega \in \Omega^1_{K/k}$ et $g \in K$, il est clair que $\mathrm{ord}_P(g\omega) = \mathrm{ord}_P(g) + \mathrm{ord}_P(\omega)$ (d'après la même propriété pour deux fonctions, i.e., d'après 3.2.3(i)). On notera aussi que $\mathrm{ord}_P(df) \geq 0$ dès que $\mathrm{ord}_P(f) \geq 0$ (puisque les df pour $f \in \mathcal{O}_P$ appartiennent à $\Omega^1_{\mathcal{O}_P/k}$ d'après 3.9.10). Il n'est pas difficile de se convaincre que ord_P est la plus petite fonction qui possède les deux propriétés qu'on vient de signaler.

La définition de $\mathrm{ord}_P(\omega)$ assez complexe. Heureusement, on va pouvoir la simplifier sous des hypothèses peu contraignantes (notamment si k est parfait).

Proposition 3.9.13. Soit $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), soit $P \in \mathscr{V}_{K/k}$ une place *elle-même séparable*, c'est-à-dire que son corps résiduel $\varkappa_P$ est une extension séparable de k, et soit enfin t une uniformisante en P (c'est-à-dire $\mathrm{ord}_P(t) = 1$) : alors dt est une base du R-module $\Omega^1_{R/k}$ (qui est libre de rang 1 d'après la proposition précédente) ; en particulier, dt est une base du K-espace vectoriel $\Omega^1_{K/k}$ (ou si on préfère, t est une base de transcendance séparante de K sur k).

Références. [Goldschmidt 2003, théorème 2.5.7], [Silverman 1986, propositions II.1.4 et II.4.3] ☺

Corollaire 3.9.14. Dans les conditions de la proposition 3.9.13, on a donc : $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(\omega/dt)$ pour tout $\omega \in \Omega^1_{K/k}$ (ceci ne dépend pas du choix de l'uniformisante t).

Démonstration. On vient de voir en 3.9.13 que dt est une base de $\Omega^1_{R/k}$, c'est-à-dire que $\mathrm{ord}_P(dt) = 0$. On a alors $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(\omega/dt) + \mathrm{ord}_P(dt)$ comme on l'a signalé. ☺

Proposition 3.9.15. Si $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), et $P \in \mathscr{V}_{K/k}$ une place elle-même séparable (i.e., $\varkappa_P$ séparable sur k) ; alors pour tout $f \in K$ on a :

- $\mathrm{ord}_P(df) = \mathrm{ord}_P(f) - 1$ si $\mathrm{ord}_P(f) \neq 0$ dans k (i.e., si $\mathrm{ord}_P(f)$ n'est pas multiple de la caractéristique), et
- $\mathrm{ord}_P(df) \geq 0$ si $\mathrm{ord}_P(f) \geq 0$, et plus généralement $\mathrm{ord}_P(df) \geq \mathrm{ord}_P(f)$ si $\mathrm{ord}_P(f)$ est multiple de la caractéristique de k.

Démonstration. Soit $R := \mathcal{O}_P$ et soit t une uniformisante en P (i.e., $\mathrm{ord}_P(t) = 1$).

La seconde propriété que $\mathrm{ord}_P(df) \geq 0$ si $\mathrm{ord}_P(f) \geq 0$ a déjà été signalée (elle affirme que les df pour $f \in R$ appartiennent $\Omega^1_{R/k}$). On va l'utiliser pour montrer les autres.

D'après 3.9.14, on sait que $\mathrm{ord}_P(df) = \mathrm{ord}_P(df/dt)$. Écrivons $f = ut^i$ où $i = \mathrm{ord}_P(f)$ et $u \in R^\times$ (en utilisant 3.2.15). On a alors $df = i\,u\,t^{i-1}\,dt + t^i\,du$, soit $\frac{df}{dt} = i\,u\,t^{i-1} + t^i\,\frac{du}{dt}$. Si $i \neq 0$ dans k, le premier terme a valuation exactement $i-1$ et le second a valuation $\geq i$ (car $du/dt \in R$ comme on vient de le voir au paragraphe précédent), donc la valuation de la somme est $i-1$ (on utilise 3.2.3(ii.b)). Si $i = 0$ dans k, le premier terme s'annule et le second a toujours valuation $\geq i$. ☺

Proposition 3.9.16. Si $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), et soit $\omega \in \Omega^1_{K/k}$ non nulle. Alors l'ensemble des places P de K telles que $\mathrm{ord}_P(\omega) \neq 0$ est fini.

Références. [Goldschmidt 2003, lemme 2.5.1], [Silverman 1986, proposition II.4.3(e)] ☺

Définition 3.9.17. Si $K = k(C)$ est un corps de fonctions de courbe sur k, séparable (cf. 3.9.5), et si $\omega \in \Omega^1_{K/k}$ est non nulle, on appelle **diviseur canonique** associé à la différentielle ω le diviseur

$$\mathrm{div}(\omega) := \sum_P \mathrm{ord}_P(\omega) \cdot (P)$$

dont le coefficient devant chaque place P est l'ordre de ω en cette place (cf. 3.9.11).

3.9.18. À titre d'exemple, calculons $\mathrm{div}(dt)$ sur $\mathbb{P}^1_k$ où t est l'indéterminée du corps $k(t)$ des fractions rationnelles, lorsque k est un corps parfait. En 0, on a $\mathrm{ord}_0(t) = 1$ donc $\mathrm{ord}_0(dt) = 0$. En ∞, on a $\mathrm{ord}_\infty(t) = -1$ donc $\mathrm{ord}_\infty(dt) = -2$. Reste à traiter le cas des autres places, pour lesquelles la proposition 3.9.15 donne *a priori* seulement $\mathrm{ord}_P(dt) \geq 0$. Mais on a vu que toute telle place a une uniformisante $h \in k[t]$ (le point essentiel est que h est un *polynôme* en t) : de $\mathrm{ord}_P(h) = 1$ on tire $\mathrm{ord}_P(dh) = 0$, or $dh = h'\,dt$ (où h' est la dérivée usuelle du polynôme h) donc $0 = \mathrm{ord}_P(dh) = \mathrm{ord}_P(h') + \mathrm{ord}_P(dt)$, et comme $\mathrm{ord}_P(h') \geq 0$ puisque $h' \in k[t]$ et que $\mathrm{ord}_P(dt) \geq 0$, la seule possibilité est que les deux termes sont nuls, donc en fait $\mathrm{ord}_P(dt) = 0$ pour chaque place P autre que ∞. Bref, on a montré que $\mathrm{ord}_P(dt) = -2(\infty)$.

3.9.19. Si ω et ω' sont deux différentielles non nulles sur une même courbe C, en appelant $h \in K^\times$ l'unique élément tel que $\omega' = h\omega$ (vu que $\Omega^1_{K/k}$ est de dimension 1), on a $\mathrm{div}(\omega') = \mathrm{div}(h) + \mathrm{div}(\omega)$, c'est-à-dire que les diviseurs

canoniques associés à ω et ω' diffèrent par un diviseur principal, autrement dit, sont linéairement équivalents (cf. 3.7.4).

On peut donc appeler **classe canonique** la classe [10] $W \in \mathrm{Pic}(C)$ de n'importe quel diviseur canonique.

3.9.20. Si $D = \sum_P n_P \cdot (P)$ est un diviseur et W un diviseur canonique, on pourra remarquer que

$$\mathscr{L}(W - D) \cong \{\omega \in \Omega^1_{K/k} : (\forall P)\ \mathrm{ord}_P(\omega) \geq n_P\}$$

(où $\cong$ désigne un isomorphisme de k-espace vectoriels, c'est-à-dire l'égalité des dimensions) : précisément, si $W = \mathrm{div}(\omega_0)$, alors $\mathscr{L}(W - D) = \{f \in K^\times : \mathrm{div}(f) + \mathrm{div}(\omega_0) - D \geq 0\} \cup \{0\} = \{f \in K^\times : \mathrm{div}(f\omega_0) - D \geq 0\} \cup \{0\}$ est isomorphe via $f \mapsto f\omega_0$ à $\{\omega \in \Omega^1_{K/k} \setminus \{0\} : \mathrm{div}(\omega) - D \geq 0\} \cup \{0\}$, c'est-à-dire ce qu'on a écrit ci-dessus.

3.10 Le théorème de Riemann-Roch

3.10.1. Dans toute cette section, on va à chaque fois supposer la courbe C *géométriquement* irréductible (cf. 2.4.12, et 3.1.10). Ceci implique notamment $\tilde{k} = k$ (on remplace donc par 1 toutes les occurrences de la quantité $[\tilde{k} : k]$).

Théorème 3.10.2 (Riemann-Roch)**.** Soit C une courbe géométriquement irréductible sur un corps k. Il existe un entier $g \geq 0$, appelé **genre** de C tel que pour tout diviseur D on ait, en notant W un diviseur canonique :

$$\ell(D) - \ell(W - D) = \deg D + 1 - g$$

Références. [Goldschmidt 2003, corollaire 2.5.11], [Silverman 1986, théorème II.5.4], [Hartshorne 1977, théorème IV.1.3], [Fried & Jarden 2008, théorème 3.2.1] ☺

Corollaire 3.10.3. (A) Pour W un diviseur canonique sur une courbe C géométriquement irréductible sur un corps k, on a :

$$\ell(W) = g$$
$$\deg(W) = 2g - 2$$

(B) Si D est un diviseur avec $\deg D > 2g - 2$, alors $\ell(D) = \deg D + 1 - g$.

10. Normalement la classe canonique est plutôt notée par la lettre K, mais ici nous utilisons systématiquement K pour le corps des fonctions.

Démonstration. Pour la première affirmation, appliquer 3.10.2 à $D = 0$ donne $1-\ell(W) = 0+1-g$, d'où $\ell(W) = g$; puis à $D = W$ donne $g-1 = \deg W+1-g$ d'où $\deg W = 2g-2$. Pour la seconde affirmation, on utilise 3.8.3 pour conclure que $\ell(W-D) = 0$. ☺

3.10.4. S'agissant de la droite projective $\mathbb{P}^1$, il résulte du calcul fait en 3.9.18 que sa classe canonique est celle de $-2(\infty)$ (on peut tout simplement dire que c'est -2 vu qu'on a vu en 3.7.5 que son groupe de Picard s'identifie à $\mathbb{Z}$ via le degré des diviseurs). Ce degré -2 nous permet de calculer $g_{\mathbb{P}^1}$ par $2g_{\mathbb{P}^1} - 2 = -2$ soit $g_{\mathbb{P}^1} = 0$. Voici une forme de réciproque :

Proposition 3.10.5. Soit C une courbe géométriquement irréductible de genre 0 et ayant une place rationnelle (cf. 3.3.3). Alors C est isomorphe à $\mathbb{P}^1$ (c'est-à-dire que $k(C)$ est $k(t)$: la courbe est *rationnelle*).

Démonstration. Soit P une place rationnelle. En appliquant 3.10.3(B) à (P), on trouve $\ell((P)) = 2$. Il existe donc une fonction f non-constante, admettant au plus un pôle simple, en P ; comme elle est non-constante, d'après 3.3.5, elle doit aussi avoir un pôle, donc $\mathrm{div}(f)$, qui doit être de degré 0, est de la forme $(Q) - (P)$. D'après 3.6.2, on voit que $\deg f := [k(C) : k(f)] = 1$, c'est-à-dire $k(C) = k(f)$, et comme f est transcendante parce que non constante, on a bien montré que $k(C)$ est le corps des fractions rationnelles en une indéterminée. ☺

3.10.6. Pour montrer que l'hypothèse d'existence d'une place rationnelle n'est pas inutile, reprenons l'exemple de la « conique sans point » évoquée en 3.1.5 : on a vu que (sur un corps k de caractéristique $\neq 2$ dans lequel -1 n'est pas somme de deux carrés, par exemple le corps des réels) la courbe d'équation $x^2 + y^2 = -1$ n'est pas rationnelle. Elle est pourtant de genre 0 comme il résulte d'une application de 3.12.8 ci-dessous à l'extension de corps $k \subseteq k(\sqrt{-1})$ et de l'observation que la courbe $x^2 + y^2 = -1$ sur $k(\sqrt{-1})$ est la même que $x'^2 + y'^2 = 1$ (quitte à faire le changement de variable linéaire $x' = \sqrt{-1}\,x$ et $y' = \sqrt{-1}\,y$) donc rationnelle (cf. 3.1.4) donc de genre 0.

3.11 Points et places

3.11.1. On a défini en 3.1.1 un « corps de fonctions de courbe » $K = k(C)$ sur k comme une extension de corps de k qui soit de type fini et de degré de transcendance 1 sur k. La « courbe » elle-même n'a pas été définie et est considérée comme un objet purement formel dont on peut parler essentiellement à travers ses fonctions (i.e., les éléments de K) et ses places (i.e., les valuations — forcément discrètes — non-triviales de K au-dessus de k).

Cependant, si $Z(I)$ est un fermé de Zariski irréductible défini par un idéal I premier de $k[t_1, \ldots, t_n]$ tel que que le corps des fractions K de l'anneau $A := k[t_1, \ldots, t_n]/I$ (des fonctions régulières sur $Z(I)$) soit de degré de transcendance 1 sur k (*par exemple* $I = (h) \subseteq k[x, y]$ avec h irréductible comme en 3.1.3), on a envie de faire un lien entre les « points » (rationnels, fermés ou géométriques, cf. 2.4.8) de $Z(I)$ et les places de la courbe C définie par K. Un tel rapport existe, même s'il n'est pas parfait.

3.11.2. Cherchons dans un premier temps à associer un point (rationnel, fermé ou géométrique) de $Z(I)$ à une place de C. Il faudra faire une hypothèse (ci-dessous) assurant que la place n'est pas « à l'infini » par rapport aux coordonnées $t_1, \ldots, t_n$ choisies.

On peut considérer les classes de $t_1, \ldots, t_n$ modulo I comme des fonctions régulières (cf. 2.4.9) sur $Z(I)$, donc des éléments de $K = \mathrm{Frac}(A)$, i.e., des fonctions « sur C », qu'on notera $\bar{t}_1, \ldots, \bar{t}_n$. Précisément, si P est une place de C (c'est-à-dire de K), on peut considérer l'évaluation en P de $\bar{t}_i$ (cf. 3.3.4), c'est-à-dire soit la classe de $\bar{t}_i \in \mathcal{O}_P$ modulo $\mathfrak{m}_P$, si $\mathrm{ord}_P(\bar{t}_i) \geq 0$, soit le symbole ∞.

Faisons l'hypothèse qu'aucun des $\bar{t}_i$ n'a de pôle en P, ce qui peut se traduire par $\mathrm{ord}_P(\bar{t}_i) \geq 0$ pour chaque i, ou encore $A \subseteq \mathcal{O}_P$ (vu que A est le sous-anneau $k[\bar{t}_1, \ldots, \bar{t}_n]$ de K engendré par k et les $\bar{t}_i$). Nous résumerons cette hypothèse en « P n'est pas à l'infini pour les t_i ».

Expliquons d'abord comment on peut obtenir des points *géométriques* de $Z(I)$ (c'est-à-dire des points dans la clôture algébrique k^{alg}). Pour cela, plongeons $\varkappa_P$ (qui est algébrique sur k, cf. 3.3.3) dans k^{alg}. Les évaluations en P des $\bar{t}_i$, vues comme des éléments de k^{alg}, définissent un point dans $(k^{\mathrm{alg}})^n$: ce point est solution des équations h_j définissant I (disons $I = (h_1, \ldots, h_m)$) car $h_j(\bar{t}_1, \ldots, \bar{t}_n) = 0$ pour chaque j, ce qui donne la même propriété sur leurs classes modulo $\mathfrak{m}_P$. On a donc associé à chaque place P de C telle que $A \subseteq \mathcal{O}_P$ un point géométrique de $Z(I)$, mais il faut souligner que le point en question dépend du plongement de $\varkappa_P$ dans k^{alg}. (Pour mieux faire les choses, il faudrait considérer tous les différents plongements de $\varkappa_P$ dans k^{alg}, ce qui, si k est parfait, peut être décrit comme une orbite sous Galois : on associe donc à la place P une orbite sous Galois de points géométriques de $Z(I)$.)

Expliquons maintenant comment on peut obtenir un point *fermé* de $Z(I)$ (c'est-à-dire par définition un $Z(\mathfrak{n})$ avec $\mathfrak{n}$ idéal maximal de $k[t_1, \ldots, t_n]$ contenant I), toujours sous l'hypothèse que P n'est pas à l'infini pour les t_i, c'est-à-dire $A \subseteq \mathcal{O}_P$. L'intersection $\mathfrak{p} := A \cap \mathfrak{m}_P$ de A avec l'idéal maximal $\mathfrak{m}_P = \{x \in K : \mathrm{ord}_P(x) > 0\}$ est encore un idéal *maximal* : le fait qu'il s'agisse d'un idéal est clair (l'intersection d'un idéal de $\mathcal{O}_P$ avec un sous-anneau de celui-ci est certainement un idéal), et il est maximal car l'image $A/\mathfrak{p}$ de A dans $\varkappa_P = \mathcal{O}_P/\mathfrak{m}_P$ est un sous-anneau de $\varkappa_P$ contenant k, c'est-à-dire une k-algèbre

de dimension finie intègre, donc un corps d'après 1.1.13. L'idéal $\hat{\mathfrak{p}} := I + \mathfrak{p}$ de $k[t_1, \ldots, t_n]$ (abus de notation pour les polynômes dont la classe modulo I tombe dans $\mathfrak{p}$) a le même quotient et il est donc lui aussi maximal. Autrement dit, ceci définit ce qu'on a appelé un « point fermé » $Z(\hat{\mathfrak{p}})$ de $Z(I)$. Comme on l'a prouvé au passage, le corps résiduel $k[t_1, \ldots, t_n]/\hat{\mathfrak{p}}$ de ce point fermé est inclus dans le corps résiduel $\varkappa_P = \mathcal{O}_P/\mathfrak{m}_P$ de la place P.

Enfin, si dans la situation du paragraphe précédent, P est une place rationnelle, i.e., $\varkappa_P = k$, alors $A/\mathfrak{p}$ est aussi égal à k, c'est-à-dire que $\hat{\mathfrak{p}}$ est un idéal de la forme $(t_1 - x_1, \ldots, t_n - x_n)$ (où $x_i \in k$ est la classe de t_i modulo $I + \mathfrak{p}$, c'est-à-dire celle de $\bar{t_i}$ modulo $\mathfrak{p}$ ou de façon équivalente de modulo $\mathfrak{m}_P$, i.e., l'évaluation de $\bar{t_i}$ en P). On obtient donc bien (le singleton d')un point rationnel de $Z(I)$ dans cette situation, qui coïncide avec le point géométrique construit à l'avant-dernier paragraphe. (C'est notamment le cas si k est algébriquement clos ; et si k est parfait, on voit donc que le point fermé défini au paragraphe précédent est l'orbite sous Galois des points géométriques définis à l'avant-dernier paragraphe.)

Bref, on a prouvé :

Proposition 3.11.3. Soit I un idéal premier de $k[t_1, \ldots, t_n]$ tel que le corps des fonctions rationnelles $K := \mathrm{Frac}(k[t_1, \ldots, t_n]/I)$ du fermé de Zariski $Z(I)$ soit de degré de transcendance 1 sur k, et donc définisse une courbe C sur k. Alors à toute place P de C qui soit « n'est pas à l'infini pour les t_i » au sens où aucun des t_i n'a de pôle en cette place on peut associer un point fermé de $Z(I)$ par évaluation des $\bar{t_i}$ en P ; et si la place P est rationnelle, le point fermé est lui aussi rationnel.

Notamment, si k est algébriquement clos, les places de C qui ne sont pas à l'infini pour les t_i définissent des points (rationnels=géométriques) de $Z(I)$ par évaluation des $\bar{t_i}$.

3.11.4. Il ne faut pas s'attendre à ce que la correspondance entre places de C non situées à l'infini et points de $Z(I)$ définie aux paragraphes précédents soit bijective : dans l'exemple de la cubique nodale décrite en 3.1.6, la courbe est rationnelle, c'est-à-dire que c'est $\mathbb{P}^1$, et les deux places ± 1 de $\mathbb{P}^1$ correspondent au seul point $(0, 0)$ de $Z(I)$.

Néanmoins, elle est *surjective* : c'est le contenu du théorème 3.2.12 qui affirme que pour tout idéal maximal $\mathfrak{p}$ de $A = k[t_1, \ldots, t_n]/I$ il existe une valuation v sur $K = \mathrm{Frac}(A)$ telle que $A \subseteq \mathcal{O}_v$ et que $A \cap \mathfrak{m}_v = \mathfrak{p}$. (Notons que v est forcément non-triviale puisque $\mathfrak{p} \neq 0$ puisque A n'est pas un corps : car s'il l'était on aurait $K = A$ et d'après 2.2.5 il serait une extension finie de k, ce qui contredit l'hypothèse $\deg. \mathrm{tr}_k K = 1$.)

3.11.5. Il existe cependant des conditions sous lesquelles on peut dire qu'il y a une unique place de C qui détermine un point de $Z(I)$.

Pour donner un exemple simple mais important, considérons $h \in k[x, y]$ irréductible tel que $h(0, 0) = 0$ et que $h'_y(0, 0) \neq 0$ en notant h'_y la dérivée de

h par rapport à sa seconde variable ; quitte à faire un changement de variable linéaire sur x et y, on peut supposer $h'_x(0,0) = 0$ et $h'_y(0,0) = 1$: c'est-à-dire que h est la somme de y et de termes de degré total au moins 2.

Soit $K := k(\bar{x}, \bar{y} : h = 0) = \mathrm{Frac}(k[x,y]/(h))$ (on note $\bar{x}, \bar{y}$ les classes de x, y dans K pour les distinguer des indéterminées elles-mêmes).

Si on cherche une valuation v de qui détermine le point $(0,0)$, c'est-à-dire l'idéal $\mathfrak{p}$ engendré par $\bar{x}$ et $\bar{y}$, elle doit vérifier $a := v(\bar{x}) > 0$ et $b := v(\bar{y}) > 0$; et la donnée de a et b détermine complètement la valuation des monômes en $\bar{x}$ et $\bar{y}$: à savoir, $v(\bar{x}^i \bar{y}^j) = ai + bj$. On veut montrer que v est unique. (La difficulté est que la valuation d'une somme n'est pas uniquement déterminée par les valuations des termes, donc on ne peut pas simplement conclure que la valuation des polynômes en $\bar{x}, \bar{y}$ est connue à partir du fait que celle des monômes l'est.)

Comme h est irréductible, il n'est pas multiple de y (sauf si $h = y$, mais alors connaît déjà les valuations sur $k[x,y]/(y)$, cf. 3.4, et il y en a bien une seule pour laquelle $v(\bar{x}) > 0$, donc on peut exclure ce cas). Il existe donc des monômes x^i qui apparaissent dans h. Soit e l'exposant du plus petit tel monôme (i.e., la valuation usuelle en 0 de $h(x,0)$). On a $e \geq 2$ puisque $h'_x(0,0) = 0$. Tout monôme dans h est alors divisible soit par y (plus petite puissance de y) soit par x^e (plus petite puissance de x) ; par conséquent, les monômes de h qui (réduits modulo h) sont susceptibles d'avoir la plus petite v-valuation sont y et x^e, qui ont $v(y) = b$ et $v(x^e) = ae$; comme $\bar{h}$ s'annule dans K, 3.2.5 montre que $b = ae$ (et la valuation de $\bar{x}^i \bar{y}^j$ est donc $a(i + ej)$). À présent, cherchons à montrer que la donnée de a et e détermine complètement la valuation (et qu'on a forcément $a = 1$).

Pour cela, écrivons $h = y + cx^e + \rho$ où chaque monôme de ρ est de la forme $x^i y^j$ avec $i + ej > e$, c'est-à-dire, de v-valuation strictement supérieure à ae. Observons que dans un polynôme f quelconque en x, y, si on travaille modulo h, on peut remplacer n'importe quelle occurrence de y par $-cx^e - \rho$. Si f est un polynôme en x, y ayant plusieurs monômes $x^i y^j$ de plus petite v-valuation $a(i + ej)$, en effectuant l'opération qu'on vient de dire sur ces monômes, on peut tous les réécrire comme $c' x^{i+ej}$ plus des termes de v-valuation strictement supérieure. Si le coefficient du terme en x^{i+ej} ainsi obtenu ne s'annule pas, la valuation de $\bar{f} := f \mod h$ est donc $a(i + ej)$. S'il s'annule, on recommence la procédure avec le nouveau polynôme, dont les monômes sont maintenant tous de v-valuation strictement supérieure à $a(i + ej)$. Puisque la v-valuation de $\bar{f}$ est finie (sauf si f est un multiple exact de h), la procédure termine [11]. On a donc expliqué comment calculer la v-valuation de $\bar{f} := f \mod h$ sans jamais utiliser d'autre information sur v que a et e. Du coup, v est uniquement déterminé par

11. Une autre façon de voir la procédure ici décrite est d'utiliser l'ordre sur les monômes $x^i y^j$ consistant à comparer d'abord $i + ej$ puis, en cas d'égalité, i : on cherche à réécrire f modulo h pour rendre aussi grand que possible le plus petit monôme dans f.

ces données sur $k[x,y]/(h)$, donc sur K (cf. 3.2.6). Et comme on sait déjà qu'elle existe, il y a bien existence et unicité.

Enfin, comme on a obtenu que la valuation de tout élément de K est un multiple de a, on a forcément $a = 1$.

On a montré un cas particulier du résultat suivant :

Proposition 3.11.6. Si $h \in k[x,y]$ est un polynôme irréductible tel que h'_x et h'_y ne soient pas tous deux nuls en un certain point fermé de $Z(h)$ (la valeur d'un polynôme en un point fermé $Z(\mathfrak{m})$ doit se comprendre comme la classe de ce polynôme modulo $\mathfrak{m}$, vue comme un élément du corps résiduel $k[x,y]/\mathfrak{m}$ du point fermé ; on dit qu'un tel point n'est pas **singulier**, ou qu'il est **régulier**). Alors ce point fermé correspond à une *unique* place de la courbe de corps des fractions $k(x,y : h = 0) = \mathrm{Frac}(k[x,y]/(h))$, et ils ont même corps résiduel.

Notamment, tout point rationnel de $Z(h)$ en lequel h'_x et h'_y ne s'annulent pas simultanément correspond à une unique place de la courbe.

Démonstration omise. ☺

3.12 Revêtements de courbes

3.12.1. Soit $K = k(C)$ est un corps de fonctions de courbe sur k, et $K \subseteq L$ une extension *finie*. Alors L est lui-même un corps de fonctions de courbe sur k (le degré de transcendance sur k est toujours 1 car $K \subseteq L$ est algébrique ; et L est de type fini sur k car de type fini sur K qui est lui-même de type fini sur k). Appelons C' la courbe correspondante. On dit dans ces conditions qu'on a affaire à un **revêtement** de courbes sur k, noté symboliquement $C' \to C$ (on va voir prochainement comment associer une place de C à une place de C'). Le **degré** du revêtement est défini comme le degré $[L : K]$ de l'extension.

Plus exactement, un revêtement $\varphi\colon C' \to C$ de courbes est défini comme un morphisme $\varphi^*\colon k(C) \to k(C')$ d'anneaux, c'est-à-dire un plongement du corps $k(C)$ des fonctions de C dans le corps $k(C')$ des fonctions de C' (on note φ^* le morphisme d'anneaux pour le distinguer du revêtement lui-même), qui fait de $k(C')$ une extension *finie* de $k(C)$. Le degré du revêtement est $\deg\varphi = [k(C') : k(C)]$.

Par exemple, n'importe quel élément non constant $x \in K$ définit un revêtement $C \to \mathbb{P}^1$ donné par l'extension $k(x) \subseteq K$ (qui est finie car algébrique de type fini), qu'on aura tendance à identifier à x, et dont le degré a déjà été noté $\deg(x)$ (cf. 3.6.5).

3.12.2. Si $\varphi\colon C' \to C$ est un revêtement de courbes sur k, et si w est une place de C' (c'est-à-dire une valuation non-triviale sur $L := k(C')$), on peut considérer la restriction $w|_K = w \circ \varphi^*$ de w à $K := k(C)$. Il est évident qu'elle satisfait

les conditions (o), (i) et (ii) de 3.2.3 (puisqu'elle les satisfait déjà sur L) : elle définit donc une valuation sur K, mais on prendra garde au fait que cette valuation n'est pas forcément surjective — on pourrait même imaginer *a priori* qu'elle soit triviale.

En fait, $w|_K$ n'est pas triviale, car si $y \in L$ est tel que $w(y) = -1$, en considérant l'équation minimale $y^n + c_1 y^{n-1} + \cdots + c_n = 0$ de y sur K, avec $c_i \in K$, il n'est pas possible d'avoir $w(c_i) = 0$ pour chaque i sinon la somme ne s'annulerait pas (puisque la valuation du terme y^n serait strictement inférieure aux autres, cf. 3.2.5).

Le groupe des valeurs $w(K^\times)$ est donc un sous-groupe non trivial de $w(L^\times) = \mathbb{Z}$, qu'on peut noter $e\mathbb{Z}$, où $e \geq 1$ est la plus petite valeur strictement positive possible de w sur un élément de K. On définit alors une valuation discrète v sur C par $v(x) = \frac{1}{e} w(x)$ (de manière à ce que v prenne les valeurs $\mathbb{Z} \cup \{\infty\}$ et pas seulement les multiples de e). Cette place v est appelée l'**image** de w par le revêtement φ, et notée $\varphi(w)$. L'entier e est, pour sa part, appelé l'**indice de ramification** de φ en la place w. Lorsque e est égal à 1, on dit que la place w est **non ramifiée** pour le revêtement φ ; lorsque c'est le cas pour toute place w, on dit que φ est [partout] non ramifié.

Enfin, le degré $[\varkappa_w : \varkappa_v]$ de l'extension des corps résiduels (définie par le fait que pour $x \in K$ on a $v(x) \geq 0$ ssi $w(x) \geq 0$ et $v(x) > 0$ ssi $v(x) > 0$, si bien que tout élément de $\varkappa_v = \{x \in K : v(x) \geq 0\}/\{x \in K : v(x) > 0\}$ peut se voir comme un élément de $\varkappa_w = \{x \in L : w(x) \geq 0\}/\{x \in L : w(x) > 0\}$) est appelé le **degré résiduel** de φ en la place w.

3.12.3. On retiendra la définition de l'indice de ramification sous la forme suivante : si $\varphi\colon C' \to C$ est un revêtement de courbes, alors pour tout $f \in k(C)$ et toute place Q de C', on a

$$\mathrm{ord}_Q(\varphi^*(f)) = e_{\varphi,Q}\ \mathrm{ord}_{\varphi(Q)}(f)$$

où $\varphi(Q)$ est la place image de Q par f et où $e_{\varphi,Q}$ est l'indice de ramification de φ en Q (défini par cette égalité).

Quant au degré résiduel, on peut utiliser la composition des degrés $\deg(Q) = [\varkappa_Q : k] = [\varkappa_Q : \varkappa_P] \cdot [\varkappa_P : k] = f \deg(P)$ (avec $P := \varphi(Q)$) pour l'exprimer dans la formule analogue

$$\deg(Q) = f_{\varphi,Q}\ \deg(\varphi(Q))$$

Par ailleurs, il est utile de noter que si $x \in k(C)$ est non constant, en se rappelant qu'on a noté $\deg(x) := [k(C) : k(x)]$, on a $[k(C') : k(x)] = [k(C') : k(C)] \cdot [k(C) : k(x)]$, c'est-à-dire

$$\deg(\varphi^*(x)) = \deg(\varphi)\ \deg(x)$$

Proposition 3.12.4. Soit $K = k(C)$ un corps de fonctions de courbe sur k, et $f \in K$ un élément non constant identifié au revêtement $C \to \mathbb{P}^1_k$ donné par l'extension $k(f) \subseteq K$. Alors pour toute place P de C, la place image $f(P)$ de $\mathbb{P}^1$ définie ci-dessus (par restriction de $w := \mathrm{ord}_P$ à $k(f)$) coïncide bien avec ce qu'on a appelé évaluation de f en P en 3.3.4 (quitte à identifier un élément de $\varkappa_P$ à la place de $\mathbb{P}^1$ définie par son polynôme minimal sur k, cf. 3.4.4). De plus, l'indice de ramification de f en P vaut :

— l'ordre $\mathrm{ord}_P(f)$ du zéro de f en P si $f(P) = 0$ (i.e., $\mathrm{ord}_P(f) > 0$),

— l'ordre $-\mathrm{ord}_P(f)$ du pole de f en P si $f(P) = \infty$ (i.e., $\mathrm{ord}_P(f) < 0$).

Démonstration. Soit $w = \mathrm{ord}_P$ la valuation correspondant à la place P. Pour g une fraction rationnelle en une indéterminée t, on considère $w|_{k(t)}(g) = \mathrm{ord}_P(g \circ f)$ (on identifie $k(t)$ à $k(f) \subseteq K$ par la composition à droite par f puisque f est transcendant, cf. 1.3.1) : le but est de comprendre la valuation ainsi définie (après division par un entier à déterminer).

Tout d'abord, dans le cas où $\mathrm{ord}_P(f) < 0$, on a $\mathrm{ord}_P(g \circ f) = \deg(g)\ \mathrm{ord}_P(f)$ si $g \in k[t]$ comme on le calcule facilement en écrivant explicitement g et en utilisant 3.2.3 (i) et (ii.b), et par conséquent (cf. 3.2.6), on a $w|_{k(t)}(g) = -v_\infty(g)\ \mathrm{ord}_P(f)$ quel que soit $g \in k(t)$. Ceci montre bien que la place image est ∞ et que l'indice de ramification est $-\mathrm{ord}_P(f)$.

Le cas où $\mathrm{ord}_P(f) > 0$ s'en déduit par composition de g par $\frac{1}{t}$ (avant de composer par f) : dans ce cas, on a $w|_{k(t)}(g) = v_0(g)\ \mathrm{ord}_P(f)$ quel que soit $g \in k(t)$, c'est-à-dire que la place image est 0 et que l'indice de ramification est $\mathrm{ord}_P(f)$.

Dans le cas où $\mathrm{ord}_P(f) = 0$, soit comme d'habitude $\mathcal{O}_P = \{x \in K : \mathrm{ord}_P(x) \geq 0\}$ l'anneau de valuation en P, et $\mathfrak{m}_P = \{x \in K : \mathrm{ord}_P(x) > 0\}$ son idéal maximal et $\varkappa_P = \mathcal{O}_P/\mathfrak{m}_P$ le corps résiduel, et soit $h \in k[t]$ le polynôme minimal sur k de la classe $\bar{f}$ de f modulo $\mathfrak{m}_P$ (i.e., de ce qu'on a appelé évaluation de f en P en 3.3.4). Le fait que $h(\bar{f}) = 0 \in \varkappa_P$ signifie exactement $h \circ f \in \mathfrak{m}_P$, c'est-à-dire $\mathrm{ord}_P(h \circ f) > 0$, autrement dit $w|_{k(t)}(h) > 0$. Comme h est unitaire irréductible sur k, il y a (cf. 3.4.4) une unique valuation v sur $k(t)$ au-dessus de k donnant la valeur 1 à h : on en déduit que $w|_{k(t)}(g) = e\, v(g)$ où $e = \mathrm{ord}_P(h \circ f)$. et on a bien montré comme annoncé que la place v image de $w = \mathrm{ord}_P$ par f est celle associée au polynôme minimal h de $\bar{f} = f(P)$. ☺

Théorème 3.12.5. Soit $\varphi\colon C' \to C$ un revêtement de courbes sur k, soit P une place quelconque de C et $Q_1, \ldots, Q_n$ les places de C' dont l'image par φ est P. Notons e_i l'indice ce ramification de φ en Q_i et $f_i = [\varkappa_{Q_i} : \varkappa_P]$ le degré résiduel. Alors on a

$$\sum_{i=1}^{n} e_i\, f_i = \deg(\varphi)$$

Démonstration. L'idée est de se ramener au théorème 3.6.2 dont celui-ci est une généralisation.

Soit $x \in K := k(C)$ dont le seul zéro est en la place P : un tel élément existe car $\ell(n \cdot (P)) > 0$ pour n suffisamment grand d'après 3.10.3(B), si bien qu'il existe une fonction n'ayant aucun pôle ailleurs qu'en P, et en l'inversant on obtient une fonction n'ayant aucun zéro ailleurs qu'en P. Disons $\mathrm{ord}_P(x) =: r$.

Les zéros de $\varphi^*(x)$ sont exactement les places de C' dont l'image par φ est P (puisque $\mathrm{ord}_Q(\varphi^*(x)) = e_{\varphi,Q}\ \mathrm{ord}_{\varphi(Q)}(x)$ est strictement positif si et seulement si $\mathrm{ord}_{\varphi(Q)}(x)$ l'est, ce qui signifie bien que x a un zéro en $\varphi(Q)$, autrement dit que $\varphi(Q) = P$ puisque x n'a de zéro qu'en P).

Le théorème 3.6.2 donne $\sum_{i=1}^n \mathrm{ord}_{Q_i}(\varphi^*(x))\ \deg(Q_i) = \deg(\varphi^*(x))$. Mais comme on l'a expliqué en 3.12.3, on a d'une part $\mathrm{ord}_{Q_i}(\varphi^*(x)) = e_i r$, d'autre part $\deg(Q_i) = f_i \deg(P)$, et enfin $\deg(\varphi^*(x)) = \deg(\varphi)\deg(x)$. Bref, $\sum_{i=1}^n e_i f_i r \deg(P) = \deg(\varphi)\deg(x)$. Comme on a aussi $r\deg(P) = \deg(x)$ par une nouvelle application de 3.6.2, on en déduit la formule annoncée. ☺

3.12.6. Soit C une courbe sur un corps k, et soit k' une extension algébrique de k. On peut chercher à considérer une courbe, qu'on notera $C_{k'}$, qui soit définie par les mêmes équations que C mais sur k'. C'est légitime à condition que les extensions $K := k(C)$ et k' de k soient linéairement disjointes (à l'intérieur de K^{alg}), typiquement si C était définie (cf. 2.4.9) par un fermé de Zariski *géométriquement irréductible* sur k (ou en tout cas, qui reste irréductible sur k') : cf. 2.5.9. Sous cette hypothèse, on peut définir $C_{k'}$ comme la courbe dont le corps des fonctions est le composé $K.k'$ (le composé étant pris dans K^{alg}). On dira que $C_{k'}$ « est définie » pour résumer cette situation, et on appellera $C_{k'}$ la courbe obtenue par **extension des scalaires** de C de k à k'.

Si k' est une extension *finie* de k, alors $K.k' = k'(C_{k'})$ est une extension de K de même degré fini (cf. 1.4.8), et on peut considérer qu'on a affaire à un revêtement $C_{k'} \to C$ donné par l'inclusion $K \subseteq K.k'$.

Proposition 3.12.7. Soit $k \subseteq k'$ une extension de corps *finie et séparable*, et soit C une courbe sur un corps k dont le corps des fonctions $K := k(C)$ est linéairement disjoint de k' sur k (par exemple si C est géométriquement intègre, cf. 3.12.6). Alors $K \subseteq K.k'$ est séparable, et le revêtement $C_{k'} \to C$ de courbes sur k défini par l'extension $K \subseteq K.k'$ est partout non ramifié.

Références. [Goldschmidt 2003, théorème 3.2.3], [Fried & Jarden 2008, théorème 3.4.2(c)] ☺

Proposition 3.12.8. Soit C une courbe géométriquement irréductible sur un corps k, et soit k' une extension algébrique *séparable* de k. Soit $C_{k'}$ la courbe k' qui est définie par la même équation, c'est-à-dire, dont le corps des fonctions

est le composé $K.k'$ (où $K := k(C)$, le composé étant pris dans K^{alg} ; cf. 2.5.9). Alors $C_{k'}$ a le même genre que C.

Références. [Goldschmidt 2003, théorème 3.4.4], [Fried & Jarden 2008, théorème 3.4.2(b)] ☺

4 Exercices

Exercice 4.1.

Soit K un corps de fonctions sur un corps k (c'est-à-dire, une extension de type fini de k de degré de transcendance 1), soit P une place de K au-dessus de k (dont on pourra noter v ou ord_P la valuation), et soit z une uniformizante en P (autrement dit, $v(z) = 1$). Soit enfin $d \geq 2$ un entier naturel.

En raisonnant sur la valuation des x_i, montrer qu'il n'existe pas de solution autre que $(0, \ldots, 0)$ à l'équation $x_0^d + z x_1^d + z^2 x_2^d + \cdots + z^{d-1} x_{d-1}^d = 0$ (algébrique homogène de degré d en d inconnues $(x_0, \ldots, x_{d-1})$) dans K.

Corrigé. On remarque que si $x \in K^\times$, alors $v(x^d) = d\, v(x)$ est un multiple de d. Par conséquent, $v(z^i x^d) = i + d\, v(x)$ est congru à i modulo d. Par conséquent, dans la somme $x_0^d + z x_1^d + z^2 x_2^d + \cdots + z^{d-1} x_{d-1}^d$, il est impossible que deux termes aient la même valuation (puisqu'elles sont congrues à des valeurs différentes modulo d) sauf si cette valuation est ∞, c'est-à-dire que les termes sont nuls. Donc dès lors que tous les termes ne sont pas nuls, il y en a un qui a une valuation *strictement* plus petite que tous les autres. D'après 3.2.5, la somme ne peut pas être nulle, ce qui prouve le résultat voulu. ✓

Exercice 4.2.

Soit k un corps *algébriquement clos*. On considère $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ des polynômes *homogènes* de degrés totaux respectifs $d_1, \ldots, d_m > 0$ en les indéterminées $t_1, \ldots, t_n$. Le but de l'exercice est de montrer que si $n > m$ alors il existe dans k^n un zéro commun non-trivial à $f_1, \ldots, f_m$ (c'est-à-dire une solution de $f_1 = \cdots = f_m = 0$ dans k^n, différente de $(0, \ldots, 0)$). On suppose donc par l'absurde que l'ensemble $Z(f_1, \ldots, f_m)$ des zéros communs à $f_1, \ldots, f_m$ est réduit à $\{(0, \ldots, 0)\}$ et on va montrer $n \leq m$.

(1) Montrer qu'il existe $r \in \mathbb{N}$ tel que tout monôme de degré total $\geq r$ en $t_1, \ldots, t_n$ appartienne à l'idéal I engendré par $f_1, \ldots, f_m$ dans $k[t_1, \ldots, t_n]$. On pourra pour cela observer que chaque t_i s'annule sur $Z(f_1, \ldots, f_m)$ et chercher à en conclure qu'une puissance de t_i appartient à I.

Corrigé. L'hypothèse faite est que le fermé de Zariski $Z(I)$ défini par $f_1 = \ldots = f_m = 0$ est le même que celui défini par $t_1 = \ldots = t_n = 0$, notamment,

chaque t_i s'annule sur $Z(I)$ (soit $t_i \in \mathfrak{I}(Z(I))$). Le Nullstellensatz fort (2.3.3) permet de conclure que pour chaque i il existe r_i tel que $t_i^{r_i}$ appartienne à l'idéal I engendré par $f_1, \ldots, f_m$ dans $k[t_1, \ldots, t_n]$. Si on appelle r la somme des r_i alors tout monôme de degré total au moins r comporte nécessairement un facteur $t_i^{r_i}$ pour un certain i, et appartient donc à I. ✓

(2) Déduire du (1) que tout monôme q de degré total $\geq r$ en $t_1, \ldots, t_n$ s'écrit sous la forme $q = h_1 f_1 + \cdots + h_m f_m$ où $h_1, \ldots, h_m$ sont eux-mêmes homogènes de degré total $\deg q - d_j$ (ou bien nuls, notamment lorsque $\deg q < d_j$). On pourra pour cela ne conserver que les monômes de bon degré total dans h_j.

Corrigé. La conclusion du (1) montre que pour tout monôme q de degré total $\geq r$ en les t_i il existe $h_1, \ldots, h_m \in k[t_1, \ldots, t_n]$ tels que $q = h_1 f_1 + \cdots + h_m f_m$. Observons à présent qu'en remplaçant h_j par sa composante homogène de degré total $\deg q - d_j$, c'est-à-dire la somme des monômes ayant ce degré total (ou zéro si $\deg q < d_j$), puisque f_j est homogène de degré total d_j et que q est également homogène (c'est un monôme !) de degré total $\deg q$, on a toujours l'égalité $q = h_1 f_1 + \cdots + h_m f_m$ (en effet, on n'a pas changé les monômes de degré total $\deg q$ dans cette égalité, et on a retiré tous ceux d'un autre degré). ✓

Soit $K = k(f_1, \ldots, f_m)$ le sous-corps de $k(t_1, \ldots, t_n)$ engendré par $f_1, \ldots, f_m$ au-dessus de k.

(3) Déduire du (2) que tout polynôme q de degré total $s \geq r$ en $t_1, \ldots, t_n$ s'écrit comme combinaison K-linéaire de monômes en $t_1, \ldots, t_n$ chacun de degré total $< s$. En déduire la même conclusion avec maintenant des monômes chacun de degré $< r$.

Corrigé. Soit q un monôme de degré total $\deg q \geq r$. En décomposant chaque h_j comme somme de monômes de degré total $\deg q - d_j$, l'égalité $q = h_1 f_1 + \cdots + h_m f_m$ obtenue en (2) signifie que le monôme q est combinaison linéaire à coefficients dans K des monômes de degré total $< \deg q$, i.e., strictement plus petit que lui.

Si maintenant q est un polynôme de degré total $s \geq r$, chacun de ses monômes est soit déjà de degré $< r$ (donc $< s$, et il n'y a rien à faire) soit, d'après ce qu'on vient d'expliquer, combinaison K-linéaire de monômes de degré total strictement plus petits que lui et, en particulier, strictement plus petits que s. En ajoutant toutes ces combinaisons, on voit que tout polynôme q de degré total $s \geq r$ est combinaison K-linéaire de monômes chacun de degré total $< s$.

En recommançant, c'est-à-dire en réécrivant de nouveau tous les monômes comme combinaisons K-linéaires de monômes de degré $< s$ où s est le degré total du plus grand monôme qui apparaît, et en itérant ce processus (qui termine vu que le plus grand degré total s d'un monôme qui apparaît dans la combinaison K-linéaire décroît strictement à chaque étape tant qu'il est au moins égal à r), on finit par arriver à une combinaison K-linéaire de monômes chacun de degré

total $< r$, soit la conclusion souhaitée. ✓

(4) Déduire de (3) que la sous-K-algèbre $K[t_1, \ldots, t_n]$ de $k(t_1, \ldots, t_n)$ engendrée par les t_i (i.e., l'ensemble des combinaisons K-linéaires des monômes en $t_1, \ldots, t_n$) est un K-espace vectoriel de dimension *finie*. Conclure que $K[t_1, \ldots, t_n]$ est un corps, qu'il coïncide avec $k(t_1, \ldots, t_n)$, donc que ce dernier est un K-espace vectoriel de dimension finie.

Corrigé. On vient de voir que tout monôme en les $t_1, \ldots, t_n$ s'écrit comme combinaison linéaire à coefficients dans K des monômes de degré $< r$. Comme il n'y a qu'un nombre fini de monômes de degré $< r$, le K-espace vectoriel $K[t_1, \ldots, t_n]$ engendré (dans $k(t_1, \ldots, t_n)$) par tous les monômes en les t_i est de dimension finie.

Or $K[t_1, \ldots, t_n]$ est également un anneau intègre (puisque c'est un sous-anneau du corps $k(t_1, \ldots, t_n)$) : et un anneau intègre de dimension finie sur un corps est lui-même un corps (1.1.13). Donc $K[t_1, \ldots, t_n]$ est un corps, et comme il contient k et $t_1, \ldots, t_n$, et est contenu dans $k(t_1, \ldots, t_n)$, il coïncide avec ce dernier.

On a donc prouvé que $K[t_1, \ldots, t_n] = k(t_1, \ldots, t_n)$ est un K-espace vectoriel de dimension finie. ✓

(5) En raisonnant sur le degré de transcendance, conclure que $n \leq m$.

Corrigé. L'extension de corps $K \subseteq k(t_1, \ldots, t_n)$ étant finie, elle est algébrique. On peut alors extraire de $f_1, \ldots, f_m$ une base de transcendance sur k de $K = k(f_1, \ldots, f_m)$ (1.5.4(1b)), et puisque $k(t_1, \ldots, t_n)$ est algébrique sur K, la base de transcendance trouvée est encore une base de transcendance sur k de $k(t_1, \ldots, t_n)$, bref $\deg. \operatorname{tr}_k k(t_1, \ldots, t_n) \leq m$. Or manifestement $t_1, \ldots, t_n$ est une base de transcendance de $k(t_1, \ldots, t_n)$ donc on a $\deg. \operatorname{tr}_k k(t_1, \ldots, t_n) = n$. On a bien prouvé $n \leq m$. ✓

Exercice 4.3.

Cet exercice utilise le résultat de l'exercice 4.2 : il *n'est pas nécessaire* d'avoir traité l'exercice en question, seulement d'avoir pris connaissance de sa conclusion, formulée dans le premier paragraphe de son énoncé.

Soit k un corps *algébriquement clos*, et soit K un corps de fonctions de courbe sur k (c'est-à-dire, une extension finie du corps $k(z)$ des fractions rationnelles en une indéterminée z).

On considère $f \in K[t_1, \ldots, t_n]$ un polynôme *homogène* en les indéterminées $t_1, \ldots, t_n$ dont le degré total d vérifie $0 < d < n$. Le but de l'exercice est de montrer qu'il existe dans K^n un zéro non-trivial à f (c'est-à-dire une solution de $f(x_1, \ldots, x_n) = 0$ différente de $(0, \ldots, 0)$).

(1) *Dans un premier temps,* on suppose que $K = k(z)$ est le corps des fractions rationnelles en une indéterminée z, et on suppose de plus que f, *a priori* dans

$k(z)[t_1, \ldots, t_n]$, est en fait dans $k[z, t_1, \ldots, t_n]$ (et toujours de degré $0 < d < n$ en $t_1, \ldots, t_n$). On cherche une solution $(x_1, \ldots, x_n)$ de $f(x_1, \ldots, x_n) = 0$, où les x_i soient dans $k[z]$ (et non tous nuls). On va écrire $x_i = \sum_{j=0}^{N} c_{i,j} z^j$ où les $c_{i,j} \in k$ sont des coefficients indéterminés et où N est un entier. Expliquer pourquoi la condition $f(x_1, \ldots, x_n) = 0$ recherchée se traduit sous la forme d'un système d'équations algébriques en les $c_{i,j}$, toutes homogènes. On ne demande pas d'écrire ce système, mais on précisera au moins clairement le nombre d'équations, leur degré, et le nombre de variables ; on pourra appeler δ le degré de f en la variable z, et considérer le degré en z et le degré total en les $c_{i,j}$ d'un terme $a_{r_1,\ldots,r_n} x_1^{r_1} \cdots x_n^{r_n}$ de $f(x_1, \ldots, x_n)$. En utilisant le résultat de l'exercice 4.2, montrer que ce système a, en effet, une solution en les $c_{i,j}$ si N est assez grand.

Corrigé. Disons qu'on ait

$$f(t_1, \ldots, t_n) = \sum_{r_1 + \cdots + r_n = d} a_{r_1,\ldots,r_n} t_1^{r_1} \cdots t_n^{r_n}$$

où on a fait l'hypothèse que les coefficients $a_{\underline{r}}$ sont dans $k[z]$. Soit δ le plus grand de leurs degrés, qui est donc le degré de f en la variable z. Comme suggéré par l'énoncé, on cherche un zéro non-trivial dans $(k[z])^n$ par la méthode des coefficients indéterminés, en écrivant chaque x_i (pour i allant de 1 à n) comme un polynôme de degré $\leq N$ en z, à savoir $x_i = \sum_{j=0}^{N} c_{i,j} z^j$.

Considérons une expression de la forme $x_1^{r_1} \cdots x_n^{r_n}$: si on la développe complètement, elle est un polynôme en z de degré au plus $N(r_1 + \cdots + r_n)$ (puisque chaque x_i est un polynôme en z de degré $\leq N$) ; et elle est homogène de degré total $r_1 + \cdots + r_n$ en les $c_{i,j}$ (puisqu'un produit de polynômes homogènes est un polynôme homogène de la somme des degrés totaux), au sens où le coefficient devant chaque puissance de z est homogène de degré total $r_1 + \cdots + r_n$ en les $c_{i,j}$. Concernant $a_{r_1,\ldots,r_n} x_1^{r_1} \cdots x_n^{r_n}$, si $r_1 + \cdots + r_n = d$, on en déduit qu'il est de degré $\leq Nd + \delta$ en z, et (que son coefficient de chaque puissance de z est) homogène de degré d en les $c_{i,j}$. Il en va donc de même de la somme $f(x_1, \ldots, x_n)$ des $a_{r_1,\ldots,r_n} x_1^{r_1} \cdots x_n^{r_n}$.

On en déduit que l'équation $f(x_1, \ldots, x_n) = 0$ se traduit, en exprimant la nullité du coefficient devant chaque z^j, comme un système d'équations homogènes de degré d en les $c_{i,j'}$. Le nombre d'équations est donné par le nombre de coefficients de z à écrire, soit 1 de plus que la borne trouvée sur le degré en z, bref $Nd + \delta + 1$. Enfin, le nombre de variables est le nombre de $c_{i,j}$, c'est-à-dire $n\,(N+1)$.

Si on tient absolument à écrire le système, ce qui n'était pas demandé, c'est :

$$(\forall j) \sum_{\substack{s_{1,0} + \cdots + s_{n,N} = d \\ s_{1,1} + \cdots + N s_{n,N} + \rho = j}} \frac{(\Sigma s_{1,\bullet})! \cdots (\Sigma s_{n,\bullet})!}{s_{1,0}! \cdots s_{n,N}!} a_{(\Sigma s_{1,\bullet}),\ldots,(\Sigma s_{n,\bullet});\rho} \, c_{1,0}^{s_{1,0}} \cdots c_{n,N}^{s_{n,N}} = 0$$

où $\Sigma s_{i,\bullet}$ désigne $s_{i,0} + \cdots + s_{i,N}$ et $a_{r_1,\ldots,r_n;\rho}$ est le coefficient de z^ρ dans le polynôme $a_{r_1,\ldots,r_n} \in k[z]$, et où j parcourt les entiers de 0 à $Nd + \delta$.

Bref, on a un système de $Nd + \delta + 1$ équations, chacune homogène de degré total d, en $n\,(N+1) = Nn+n$ variables. Puisque $d < n$, on a $Nd+\delta+1 < Nn+n$ lorsque N est assez grand. On conclut d'après le résultat de l'exercice 4.2 que le système a une solution avec les $c_{i,j}$ non tous nuls, c'est-à-dire les x_i non tous nuls. ✓

(2) On suppose toujours que $K = k(z)$. On a montré en (1) que si $f \in k[z, t_1, \ldots, t_n]$ alors $f(x_1, \ldots, x_n) = 0$ a une solution non-triviale (dans $(k[z])^n$, donc dans K^n). En déduire que si $f \in k(z)[t_1, \ldots, t_n]$ alors $f(x_1, \ldots, x_n) = 0$ a encore une solution non-triviale dans K^n.

Corrigé. Il suffit de chasser les dénominateurs. Plus précisément, si $f \in k(z)[t_1, \ldots, t_n]$, soit $q \in k[z]$ un dénominateur commun à tous les coefficients $a_{r_1,\ldots,r_n}$ de f (en les variables $t_1, \ldots, t_n$). Alors $q\,f \in k[z, t_1, \ldots, t_n]$, et comme on a vu en (1) que l'équation $q\,f(x_1, \ldots, x_n) = 0$ a une solution non-triviale, cette solution en est aussi une de l'équation $f(x_1, \ldots, x_n) = 0$. ✓

(3) Dans cette question (indépendante des précédentes), on suppose que $K_0 \subseteq K$ est une extension de corps de degré $\ell := [K : K_0]$ fini. Soit $e_1, \ldots, e_\ell$ une base de K comme K_0-espace vectoriel. Lorsque $w \in K$, on notera $\mathbf{M}(w)$ la matrice $\ell \times \ell$ à coefficients dans K_0 qui représente l'application $K \to K,\ y \mapsto w \cdot y$ de multiplication par w (vue comme une application K_0-linéaire du K_0-espace vectoriel K de dimension ℓ), sur la base $e_1, \ldots, e_\ell$, et on notera $\mathrm{N}(w) := \det(\mathbf{M}(w))$ son déterminant (c'est donc un élément de K_0).
(a) Expliquer pourquoi $\mathbf{M}(ww') = \mathbf{M}(w)\,\mathbf{M}(w')$ si $w, w' \in K$, pourquoi $\mathrm{N}(ww') = \mathrm{N}(w)\ \mathrm{N}(w')$, et pourquoi $\mathrm{N}(w) = 0$ si et seulement si $w = 0$.
(b) Expliquer pourquoi si $w = \sum_{j=1}^{\ell} w_j e_j$ avec $w_j \in K_0$, alors les coefficients de $\mathbf{M}(w)$ s'écrivent comme des combinaisons K_0-linéaires des w_j, et pourquoi $\mathrm{N}(w)$ s'écrit comme un polynôme homogène de degré ℓ en $w_1, \ldots, w_\ell$.

Corrigé. (a) On a $\mathbf{M}(ww') = \mathbf{M}(w)\,\mathbf{M}(w')$ car la multiplication par ww' est la composée, dans n'importe quel ordre, de celle par w et de celle par w'. L'identité $\mathrm{N}(ww') = \mathrm{N}(w)\ \mathrm{N}(w')$ s'en déduit par la multiplicativité du déterminant. On en déduit que $\mathrm{N}(w)\ \mathrm{N}(w') = 1$ si w' est l'inverse de w, et donc que $\mathrm{N}(w) \neq 0$ si $w \neq 0$ (l'autre implication est triviale).

(b) Si $w = \sum_{j=1}^{\ell} w_j e_j$ alors on a $\mathbf{M}(w) = \sum_{j=1}^{\ell} w_j E_j$, où on a noté $E_j := \mathbf{M}(e_j)$: comme E_j est une certaine matrice $\ell \times \ell$ à coefficients dans K_0, ceci montre bien que les coefficients de $\mathbf{M}(w)$ s'écrivent comme des combinaisons K_0-linéaires des w_j. Comme le déterminant d'une matrice $\ell \times \ell$ est un polynôme homogène de degré ℓ en les coefficients de la matrice, on en déduit que $\mathrm{N}(w)$ s'écrit comme un polynôme homogène de degré ℓ en $w_1, \ldots, w_\ell$. ✓

(4) On suppose maintenant que K est un corps de fonctions de courbe sur k,

disons de degré $\ell := [K : K_0]$ sur le corps des fractions rationnelles $K_0 := k(z)$. On reprend les notations $\mathbf{M}(w)$ et $\mathrm{N}(w)$ de la question (3), en appelant $e_1, \ldots, e_\ell$ une base de K comme K_0-espace vectoriel. Soit $f \in K[t_1, \ldots, t_n]$ (toujours de degré total $0 < d < n$ en $t_1, \ldots, t_n$). On va écrire $x_i = \sum_{j=1}^{\ell} x_{i,j} e_j$ où les $x_{i,j} \in K_0$ sont des coefficients indéterminés. Expliquer pourquoi la condition $\mathrm{N}(f(x_1, \ldots, x_n)) = 0$ se traduit sous la forme d'une équation algébrique homogène de degré $d\ell$ en $n\ell$ indéterminées. En déduire qu'elle a une solution non-triviale. Conclure.

Corrigé. Disons qu'on ait

$$f(t_1, \ldots, t_n) = \sum_{r_1 + \cdots + r_n = d} a_{r_1, \ldots, r_n} t_1^{r_1} \cdots t_n^{r_n}$$

les coefficients $a_{\underline{r}}$ sont dans K. Comme suggéré par l'énoncé, on cherche un zéro non-trivial dans K^n par la méthode des coefficients indéterminés, en écrivant chaque x_i (pour i allant de 1 à n) comme $x_i = \sum_{j=1}^{\ell} x_{i,j} e_j$.

Considérons une expression de la forme $\mathbf{M}(x_1^{r_1} \cdots x_n^{r_n}) = \mathbf{M}(x_1)^{r_1} \cdots \mathbf{M}(x_n)^{r_n}$: d'après la question (3)(b), les coefficients de chaque $\mathbf{M}(x_i)$ sont des combinaisons K_0-linéaires des $x_{i,j}$ (pour ce i), donc les coefficients du produits sont des polynômes homogènes de degré total $r_1 + \cdots + r_n$ en les $x_{i,j}$ (en utilisant le fait que le produit de matrices est bilinéaire). Concernant $\mathbf{M}(a_{r_1, \ldots, r_n} x_1^{r_1} \cdots x_n^{r_n})$, si $r_1 + \cdots + r_n = d$, on en déduit qu'il est homogène de degré total d en les $x_{i,j}$. Il en va donc de même de la somme $\mathbf{M}(f(x_1, \ldots, x_n))$ des $a_{r_1, \ldots, r_n} x_1^{r_1} \cdots x_n^{r_n}$. Par l'homogénéité du déterminant, $\mathrm{N}(f(x_1, \ldots, x_n))$ est un polynome homogène (à coefficients dans K_0) de degré total $d\ell$ en les indéterminées $x_{i,j}$ qui sont au nombre de $n\ell$.

D'après la question (2), si $d\ell < n\ell$, ce qui équivaut à $d < n$, il y a bien une solution non triviale à cette équation algébrique de degré $d\ell$ en $n\ell$ indéterminées dans $K_0 = k(z)$. Or d'après la question (3)(a), l'annulation de ce déterminant $\mathrm{N}(f(x_1, \ldots, x_n))$ équivaut à l'annulation de tous les x_i (i.e., de tous les $x_{i,j}$). On a donc bien montré que $f(x_1, \ldots, x_n) = 0$ a une solution non-triviale dans K. ✓

(5) Les questions précédentes ont montré que si K est le corps des fonctions d'une courbe sur un corps k algébriquement clos et si $f \in K[t_1, \ldots, t_n]$ est un polynôme homogène en les indéterminées $t_1, \ldots, t_n$ dont le degré total d vérifie $0 < d < n$, alors f a un zéro non-trivial dans K^n. On s'est limité à un seul polynôme f pour plus de simplicité dans les notations. Mais en fait, les mêmes arguments montrent que si $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ sont plusieurs polynômes homogènes de degrés totaux respectifs $d_1, \ldots, d_m > 0$ en les indéterminées $t_1, \ldots, t_n$, on peut conclure à l'existence d'un zéro commun non-trivial à $f_1, \ldots, f_m$ dans K^n sous une certaine hypothèse sur $d_1, \ldots, d_m$. Sans réécrire les démonstrations, indiquer quelle serait cette condition.

Corrigé. Si on reprend les questions précédentes avec maintenant m polynômes, dans la question (1), on obtiendra maintenant un système de $\sum_{j=1}^{m}(Nd_j + \delta + 1) = N(d_1 + \cdots + d_m) + m\delta + m$ équations en $n(N+1)$ variables, qui a donc une solution pour N grand lorsque $d_1 + \cdots + d_m < n$. Les arguments des questions (2) et (4) ne sont essentiellement pas modifiés, et on arrive à la conclusion que :

Si K est le corps des fonctions d'une courbe sur un corps k algébriquement clos et si $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ sont des polynômes homogènes de degrés totaux respectifs $d_1, \ldots, d_m > 0$ en les indéterminées $t_1, \ldots, t_n$, qui vérifient $d_1 + \cdots + d_m < n$, alors $f_1, \ldots, f_m$ ont un zéro commun non-trivial dans K^n.

(Ce résultat s'appelle le théorème de Tsen. On pourra remarquer que l'exercice 4.1 montre que l'inégalité est optimale sur n'importe quel corps de fonctions de courbe, puisqu'on y a trouvé un polynôme homogène de degré d en $n = d$ variables sans zéro non-trivial.) ✓

Exercice 4.4.

Soit k un corps parfait de caractéristique $\neq 2, 5$. On considère la courbe C plane sur k d'équation $y^2 = x^5 - 1$. On admettra sans vérification que le polynôme $h := y^2 - x^5 + 1 \in k[x, y]$ est géométriquement irréductible, et on posera $K := k(C) = k(x)[y]/(h)$.

(1) Si w est une valuation de K au-dessus de k, montrer qu'on a $w(x) < 0$ si et seulement si $w(y) < 0$. Exprimer le rapport entre $w(y)$ et $w(x)$ si c'est le cas.

Corrigé. Si $w(x) < 0$ alors $w(x^5 - 1) = 5w(x)$ (puisque $w(x^5) < w(1)$), autrement dit $w(y^2) = 5w(x)$, d'où on déduit $w(y) = \frac{5}{2}w(x) < 0$. Réciproquement, si $w(x) \geq 0$ alors $w(x^5 - 1) \geq 0$, autrement dit $w(y^2) \geq 0$, d'où on déduit $w(y) \geq 0$. On a bien montré l'équivalence entre $w(x) < 0$ et $w(y) < 0$ et, de plus, $w(y) = \frac{5}{2}w(x)$ lorsque ces propriétés sont vérifiées. ✓

(2) Rappeler pourquoi tout élément de K s'écrit de façon unique sous la forme $f_0 + f_1 y$ avec $f_0, f_1 \in k(x)$.

Corrigé. Le corps K est le corps de rupture de $h := y^2 - x^5 + 1$ sur le corps $k(x)$ des fractions rationnelles en l'indéterminée x. Tout élément de $K = k(x)[y]/(h)$ est donc représenté de façon unique sous la forme d'un polynôme de degré < 2 en y, à savoir le reste de la division euclidienne par h (dans $k(x)[y]$) de n'importe quel représentant, ce qui est bien la forme demandée. ✓

(3) En déduire qu'il existe une et une seule valuation w de K au-dessus de k telle que $w(x) < 0$ (on pourra considérer la restriction de w à $k(x)$ et montrer que c'est, à une constante près, la valuation v_∞ à l'infini ; puis déduire de (2) que w est complètement déterminé par la donnée de $w(x)$ et en conclure ce qu'elle vaut).

Corrigé. La restriction de w à $k(x)$ vérifie les propriétés (o), (i) et (ii) de 3.2.3 qui définissent une valuation : c'est donc *à multiplication près par un entier* $e \geq 1$

une valuation sur $k(x)$, au-dessus de k ; et puisque $w(x) < 0$, cette valuation est la valuation à l'infini. Autrement dit, en notant $w(x) = -e$, on a $w(f_0) = e\, v_\infty(f_0)$ pour tout $f_0 \in k(x)$. Mais on sait aussi que $w(y) = \frac{5}{2}w(x) = -\frac{5}{2}e$, donc dans une forme $f_0 + f_1 y$, le premier terme a une valuation multiple de e et le second en a une qui vaut $-\frac{5}{2}e$ plus un multiple de e, et notamment les deux termes sont forcément de valuations *différentes* : ainsi, $w(f_0 + f_1 y)$ est complètement déterminé par la donnée de e, à savoir $e\,\min(v_\infty(f_0), v_\infty(f_1) - \frac{5}{2})$. Mais puisque l'image de w doit être $\mathbb{Z} \cup \{\infty\}$ (condition de normalisation), on a forcément $e = 2$, c'est-à-dire $w(x) = -2$ et $w(y) = -5$, et en général $w(f_0 + f_1 y) = \min(2v_\infty(f_0), 2v_\infty(f_1) - 5)$.

Il existe forcément une telle valuation, car x n'est pas constant (il est transcendant sur k), donc il a un pôle, ce qui signifie exactement qu'il existe une place w comme on vient de le décrire. ✓

(4) On note M la place de C qui a été trouvée (c'est-à-dire que $w = \mathrm{ord}_M$ est l'unique valuation de K au-dessus de k pour laquelle $w(x) < 0$). Montrer que pour tout $r \geq 3$ entier, les fonctions $1, x, x^2, \ldots, x^r, y, xy, \ldots, x^{r-3}y$ sont dans l'espace de Riemann-Roch $\mathscr{L}(2r(M))$ et sont linéairement indépendants sur k. En déduire un minorant de $\ell(2r(M))$. En prenant r grand, en déduire un majorant sur le genre g de C.

Corrigé. On vient de voir que $\mathrm{ord}_M(x) = -2$ et $\mathrm{ord}_M(y) = -5$. Par conséquent, $\mathrm{ord}_M(x^i) = -2i$ et $\mathrm{ord}_M(x^i y) = -2i - 5$. Ces quantités sont $\geq -2r$ lorsque respectivement $i \leq r$ et $i \leq r - \frac{5}{2}$ (c'est-à-dire en fait $i \leq r-3$ puisque i, r sont entiers). En toute autre place P que M, on sait que $\mathrm{ord}_P(x) \geq 0$ et $\mathrm{ord}_P(y) \geq 0$ d'après la question (3). On a bien montré que $1, x, x^2, \ldots, x^r, y, xy, \ldots, x^{r-3}y$ sont dans $\mathscr{L}(2r(M))$. Ils sont linéairement indépendants sur k car d'une part les puissances de x, qui sont dans $k(x)$, sont linéairement indépendantes sur k, et d'autre part 1 et y sont linéairement indépendants sur $k(x)$ (cf. question (2)). Bref, on a trouvé $(r+1)+(r-2) = 2r-1$ éléments k-linéairement indépendants dans $\mathscr{L}(2r(M))$, donc $\ell(2r(M)) \geq 2r - 1$.

Or on sait par 3.10.3(B) que si r est assez grand (à savoir $2r > 2g - 2$ mais peu importe), on a $\ell(2r(M)) = 2r + 1 - g$. On en déduit $2r + 1 - g \geq 2r - 1$, c'est-à-dire $g \leq 2$. ✓

Références

[Fried & Jarden 2008] Michael D. Fried & Moshe Jarden, *Field Arithmetic*, Springer (3rd edition 2008), ISBN 978-3-540-77269-9.

[Goldschmidt 2003] David M. Goldschmidt, *Algebraic Functions and Projective Curves*, Springer (2003) Graduate Texts in Mathematics **215**, ISBN 978-1-4419-2995-2.

[Hartshorne 1977] Robin Hartshorne, *Algebraic Geometry*, Springer (1977) Graduate Texts in Mathematics **52**, ISBN 978-1-4419-2807-8.

[Matsumura 1989] Hideyuki Matsumura, *Commutative Ring Theory*, Cambridge University Press (paperback edition 1989), ISBN 978-0-521-36764-6.

[Silverman 1986] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (1986) Graduate Texts in Mathematics **106**, ISBN 978-1-4757-1922-2.

Index