# § 29. Fractions rationnelles

### 1. *Corps des fractions d'un anneau d'intégrité : préliminaires*

Il est clair que tout sous-anneau K d'un corps est un anneau d'intégrité. Inversement, peut-on considérer tout anneau d'intégrité comme un sous-anneau d'un corps? Nous allons montrer dans ce § que ce problème admet une réponse affirmative, dans le cas d'un anneau commutatif tout au moins.

Pour construire un corps contenant un anneau d'intégrité commutatif K donné, supposons d'abord le problème résolu; autrement dit, supposons construit un corps L dont K soit un sous-anneau. Alors tout élément non nul $a$ de K admet un inverse dans L; plus généralement, étant donnés deux éléments $a$, $b \in K$, avec $b \neq 0$, on peut considérer dans L la fraction

$$a/b = ab^{-1}.$$

*L'ensemble de ces fractions est un sous-corps commutatif de* L *contenant* K. Soit en effet L′ cet ensemble, et considérons deux éléments $x$, $y$ de L′; on peut donc écrire

$$x = ab^{-1}, \qquad y = cd^{-1}$$

avec des éléments $a$, $b$, $c$, $d$ de K, et $b \neq 0$, $d \neq 0$; un calcul trivial (compte tenu de la *commutativité* de K) montre alors qu'on a les relations

$$x + y = (ad + bc)/bd \tag{1}$$

$$yx = xy = ac/bd, \tag{2}$$

et comme évidemment on a

$$a/1 = a \tag{3}$$

pour tout $a \in K$, on voit déjà que L′ est un sous-anneau de L contenant K. Pour établir que L′ est un sous-corps de L, on remarque qu'un élément $x = a/b$ de L′ est non nul si et seulement si $a \neq 0$; on a alors

$$x^{-1} = (ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1} = b/a,$$

ce qui prouve évidemment que $x$ est inversible dans L′.



S'il est possible de « plonger » K dans un corps L, on peut donc supposer (au besoin en utilisant la construction ci-dessus pour remplacer L par L′), que *tout* élément de L peut s'écrire sous la forme

$$x = a/b \quad \text{avec} \quad a, b \in K, \qquad b \neq 0. \tag{4}$$

Désignons alors par F l'ensemble des couples

$$(a, b) \quad \text{tels que} \quad a, b \in K, \qquad b \neq 0;$$

l'application

$$\nu : F \to L$$

donnée par

$$\nu(a, b) = a/b = ab^{-1}$$

est donc *surjective*; désignons alors par R la relation d'équivalence sur l'ensemble F associée à l'application $\nu$ (§ 4, n° 1), autrement dit la relation

$$\nu(a, b) = \nu(c, d),$$

qui s'écrit encore $a/b = c/d$, i.e.

$$ad = bc;$$

alors $\nu$ est composée de l'application canonique de F sur F/R, et d'une application $\nu'$ de F/R sur L (§ 4, Théorème 2), et il est clair que $\nu'$ est *bijective*. Si l'on utilise $\nu'$ pour identifier les éléments de L aux éléments de F/R qui leur correspondent, on voit donc qu'on peut regarder F/R comme un *corps* dans lequel les opérations sont définies par les formules (1) et (2) — plus exactement : si des éléments $x$ et $y$ de F/R sont représentés dans F par des couples $(a, b)$ et $(c, d)$, alors $x + y$ sera l'élément de F/R représenté par le couple $(ad + bc, bd)$, et $xy$ l'élément représenté par $(ac, bd)$.

Ces considérations, qui supposaient le problème résolu, vont nous permettre, à partir de l'anneau K, de construire effectivement un corps L contenant K.

### 2. *Construction du corps des fractions*

Soit donc K un *anneau d'intégrité commutatif*. Nous désignerons par F l'ensemble des couples $(a, b)$ avec $a, b \in K$, $b \neq 0$. Étant donnés deux éléments $(a, b)$ et $(c, d)$ de F, on désignera par

$$(a, b) \equiv (c, d) \mod R$$

la relation

$$ad = bc.$$

Nous allons d'abord montrer que R est une *relation d'équivalence* sur F.

Tout d'abord, la relation

$$(a, b) \equiv (a, b) \mod R$$

est toujours vraie puisqu'elle s'écrit

$$ab = ba.$$

D'autre part, la relation

$$(a, b) \equiv (c, d) \mod \mathrm{R}$$

implique la relation

$$(c, d) \equiv (a, b) \mod \mathrm{R},$$

car la première s'écrit $ad = bc$, et la seconde $cb = da$.

Considérons enfin les relations

$$\begin{aligned}(a, b) &\equiv (c, d) \mod \mathrm{R},\\ (c, d) &\equiv (e, f) \mod \mathrm{R},\\ (a, b) &\equiv (e, f) \mod \mathrm{R};\end{aligned}$$

elles s'écrivent respectivement $ad = bc$, $cf = de$ et $af = be$; en multipliant la première par $f$ et la seconde par $b$ (de façon à faire apparaître le terme $bcf$ dans les deux relations considérées), on déduit des deux premières relations la relation $adf = bde$, ou encore $(af - be)d = 0$; *comme* $d \neq 0$ *et comme* K *est un anneau d'intégrité*, ceci implique $af - be = 0$, i.e. $af = be$, et par suite les deux premières relations considérées impliquent la troisième.

Nous avons donc montré que R est une relation d'équivalence sur F, ce qui permet de construire un ensemble quotient F/R; nous désignerons par $\theta$ l'application canonique de F sur F/R.

Montrons maintenant qu'*il existe sur l'ensemble* F/R *deux lois de compositions*

$$(x, y) \mapsto x + y \qquad \text{et} \qquad (x, y) \mapsto xy$$

*telles que l'on ait*

$$\theta(a, b) + \theta(c, d) = \theta(ad + bc, bd) \tag{5}$$

$$\theta(a, b) \,.\, \theta(c, d) = \theta(ac, bd) \tag{6}$$

*quels que soient* $(a, b)$, $(c, d) \in \mathrm{F}$.

Remarquons d'abord que les seconds membres des relations (5) et (6) ont un sens, autrement dit qu'on a $bd \neq 0$ : cela provient des inégalités $b \neq 0$, $d \neq 0$, et du fait que K est un *anneau d'intégrité*.

Pour prouver maintenant l'existence d'applications de $(\mathrm{F/R}) \times (\mathrm{F/R})$ dans F/R vérifiant les conditions (5) et (6), nous utiliserons le Théorème 3 du § 4, en prenant $\mathrm{X} = \mathrm{Y} = \mathrm{Z} = \mathrm{F}$, $\mathrm{R} = \mathrm{S} = \mathrm{T}$, et pour application

$$f : \mathrm{F} \times \mathrm{F} \to \mathrm{F}$$

soit l'application donnée par

$$f[(a, b), (c, d)] = (ad + bc, bd),$$

soit l'application donnée par

$$f[(a, b), (c, d)] = (ac, bd).$$



En vertu du Théorème en question, tout revient à établir le résultat suivant : *les relations*

$$(a', b') \equiv (a'', b'') \mod \mathrm{R}$$

*et*

$$(c', d') \equiv (c'', d'') \mod \mathrm{R}$$

*impliquent les relations*

$$(a'd' + b'c', b'd') \equiv (a''d'' + b''c'', b''d'') \mod \mathrm{R} \tag{7}$$

*et*

$$(a'c', b'd') \equiv (a''c'', b''d'') \mod \mathrm{R} \tag{8}$$

Prouvons d'abord la relation (8); celle-ci s'écrit

$$a'c'b''d'' = b'd'a''c'';$$

comme on a par hypothèse

$$a'b'' = b'a'' \qquad \text{et} \qquad c'd'' = d'c'', \tag{9}$$

la relation cherchée s'obtient en multipliant membre à membre les deux relations qu'on vient d'écrire. Quant à la relation (7), qui s'écrit encore

$$(a'd' + b'c')b''d'' = (a''d'' + b''c'')b'd',$$

elle est visiblement équivalente à

$$(a'b'' - a''b')d'd'' + (c'd'' - c''d')b'b'' = 0,$$

et résulte évidemment de (9).

Nous sommes donc bien dans les conditions d'application du Théorème 3 du § 4, et il existe donc sur l'ensemble quotient F/R deux lois de composition vérifiant les conditions (5) et (6), qui du reste déterminent sans ambiguïté les lois de composition en question comme le montre le même Théorème.

*Remarque* 1. Le lecteur évitera de croire qu'on pourrait simplifier ces raisonnements dans le cas « élémentaire » où il s'agit de construire les nombres rationnels à partir des nombres entiers. Un nombre rationnel peut s'écrire d'une infinité de façons différentes sous la forme d'une fraction, et on ne peut pas définir la somme (par exemple) de deux nombres rationnels en se bornant à poser

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd};$$

pour que cette formule définisse la somme de deux *nombres rationnels* (et non pas seulement de deux *fractions*, notion totalement dépourvue d'intérêt en soi), on doit montrer que, si l'on remplace les fractions $a/b$ et $c/d$ par des fractions équivalentes (i.e. définissant les mêmes nombres rationnels), le second membre est de même remplacé par une fraction équivalente — par exemple, on

doit démontrer que les fractions

$$1/2 + 4/6 = 14/12$$

et

$$4/8 + 2/3 = 28/24$$

sont équivalentes. Le fait qu'on ne se donne généralement pas la peine, dans l'enseignement élémentaire, de faire ces démonstrations ôte toute espèce de valeur mathématique aux définitions (sic) ainsi obtenues de la somme et du produit de deux nombres rationnels, et constitue une escroquerie majeure, destinée à masquer à des enfants innocents et sans défense la difficulté réelle du problème.

En fait, et quelle que soit la méthode adoptée, on est obligé d'utiliser les raisonnements du § 4, Théorème 3, ainsi que les calculs, d'ailleurs fort simples, qui démontrent (7) et (8); une construction qui parviendrait à s'en passer serait immanquablement erronée.

### 3. *Vérification des axiomes des corps*

Dans ce n° on va montrer que l'ensemble F/R, muni des deux lois de composition définies au n° précédent, *est un corps commutatif.*

Montrons d'abord que l'addition est commutative; il suffit, compte tenu de (5), de remarquer que l'élément $(ad + bc, bd)$ de F ne change pas si l'on permute $(a, b)$ et $(c, d)$, autrement dit si l'on remplace $a, b, c, d$ par $c, d, a, b$ respectivement.

Montrons maintenant que l'addition est associative. Soient

$$x = \theta(a, b), \qquad y = \theta(c, d), \qquad z = \theta(e, f)$$

des éléments de F/R; on a

$$(x + y) + z = \theta(ad + bc, bd) + \theta(e, f) = \theta[(ad + bc)f + bde, bdf]$$
$$x + (y + z) = \theta(a, b) + \theta(cf + de, df) = \theta[adf + b(cf + de), bdf];$$

il suffit donc d'établir que

$$(ad + bc)f + bde = adf + b(cf + de),$$

ce qui est facile...

L'addition admet un élément neutre, à savoir

$$0 = \theta(0, 1);$$

on a en effet d'après (5).

$$\theta(0, 1) + \theta(a, b) = \theta(0.b + 1.a, 1.a) = \theta(a, b).$$

Tout élément

$$x = \theta(a, b)$$

de F/R admet enfin un opposé, à savoir

$$-x = \theta(-a, b).$$



En effet on a

$$\theta(a, b) + \theta(-a, b) = \theta(0, b^2)$$

en sorte qu'il suffit de montrer que

$$\theta(0, b) = \theta(0, 1) \quad \text{pour tout } b \in \mathrm{K},\ b \neq 0;$$

or cette relation s'écrit $0.1 = b.0$, et est donc trivialement vraie.

Ainsi, nous avons déjà établi que F/R, muni de l'addition, est un groupe commutatif.

Montrons maintenant que dans F/R la multiplication est commutative, associative, et admet un élément neutre. La commutativité est évidente sur la formule (6). L'associativité s'obtient en observant que

$$[\theta(a, b)\theta(c, d)]\theta(e, f) = \theta(ac, bd)\theta(e, f) = \theta[(ac)e, (bd)f]$$

tandis que

$$\theta(a, b)[\theta(c, d)\theta(e, f)] = \theta(a, b)\theta(ce, df) = \theta[a(ce), b(df)];$$

enfin, l'élément

$$1 = \theta(1, 1)$$

de F/R est élément neutre pour la multiplication, comme le montre un calcul trivial.

Pour achever la démonstration du fait que F/R est un corps, il resterait d'une part à vérifier l'identité de distributivité $(x + y)z = xz + yz$ dans F/R, d'autre part à montrer que tout élément non nul de F/R est inversible. On laisse au lecteur le soin d'établir le premier point à titre d'exercice. Quant au second, remarquons d'abord que la relation

$$\theta(a, b) = 0$$

équivaut à $a = 0$, car étant donné que $0 = \theta(0, 1)$, la relation en question s'écrit encore $a.1 = b.0$. Ceci dit soit $x$ un élément non nul de F/R; on a donc

$$x = \theta(a, b) \qquad \text{avec} \qquad a \neq 0, b \neq 0;$$

on a alors le droit de considérer l'élément

$$x^{-1} = \theta(b, a)$$

de F/R, et celui-ci est effectivement inverse de $x$; on a en effet

$$x.x^{-1} = \theta(ab, ab)$$

de sorte que tout revient à montrer que

$$\theta(e, e) = 1 = \theta(1, 1)$$

pour tout $e \neq 0$; mais c'est clair, puisque la relation considérée s'écrit $e.1 = 1.e$.

### 4. *Immersion de l'anneau* K *dans son corps des fractions*

Il nous reste, pour résoudre entièrement le problème posé au n° 1, à montrer comment on peut considérer K comme un sous-anneau du corps F/R; ici comme en beaucoup d'autres circonstances, nous ne montrerons pas que K est à proprement parler un sous-anneau (ni même un sous-ensemble) de F/R, mais nous construirons un isomorphisme « canonique » de K sur un sous-anneau de F/R (le lecteur aura intérêt à se souvenir de la façon dont on identifie les nombres réels à des nombres complexes ou les éléments d'un anneau commutatif à des polynômes à coefficients dans cet anneau, etc...).

Pour cela, considérons l'application

$$j : \mathrm{K} \to \mathrm{F/R}$$

donnée par

$$j(a) = \theta(a, 1)$$

pour tout $a \in \mathrm{K}$. Elle est *injective*, car la relation $\theta(a', 1) = \theta(a'', 1)$ s'écrit $a' \cdot 1 = 1 \cdot a''$. C'est de plus un *homomorphisme d'anneaux*. On a en effet

$$\begin{aligned} j(a') + j(a'') &= \theta(a', 1) + \theta(a'', 1) = \theta(a' \cdot 1 + 1 \cdot a'', 1 \cdot 1) \\ &= \theta(a' + a'', 1) = j(a' + a''), \\ j(a') \cdot j(a'') &= \theta(a', 1)\theta(a'', 1) = \theta(a'a'', 1 \cdot 1) = \theta(a'a'', 1) = j(a'a''), \\ j(1) &= \theta(1, 1) = 1. \end{aligned}$$

L'application $j$ est donc bien un isomorphisme de K sur un sous-anneau de F/R, à savoir le sous-anneau formé des éléments de la forme $\theta(a, b)$ avec $b = 1$. Dorénavant nous ne ferons aucune différence entre un élément $a$ de K et l'élément $\theta(a, 1)$ de F/R; autrement dit, nous écrirons

$$\theta(a, 1) = a, \tag{10}$$

pour tout $a \in \mathrm{K}$.

On a alors le résultat suivant : *tout élément de* F/R *est un quotient de deux éléments de* K; de façon précise, on a

$$\theta(a, b) = ab^{-1}, \tag{11}$$

ou, si l'on préfère,

$$\theta(a, b) = \theta(a, 1) \cdot \theta(b, 1)^{-1} \tag{12}$$

On notera que $\theta(b, 1)$ n'est pas nul puisque $b \neq 0$, donc est inversible dans F/R d'après le n° précédent.

Pour prouver (12), il suffit de montrer que

$$\theta(a, b) \cdot \theta(b, 1) = \theta(a, 1),$$

ce, que

$$\theta(ab, b) = \theta(a, 1);$$

mais cette relation s'écrit $ab1 = ba$, et est donc évidente.



Le corps F/R que nous avons construit dans ce qui précède s'appelle le **corps des fractions de l'anneau d'intégrité commutatif** K; le lecteur pourra par la suite oublier la façon dont nous l'avons obtenu; il suffit, pour toutes les applications, d'en connaître les propriétés suivantes : K *est un sous-anneau de son corps des fractions, et tout élément de celui-ci est quotient de deux éléments de* K. En particulier, nous n'utiliserons plus jamais la notation $\theta(a, b)$ pour désigner les éléments du corps des fractions de K; nous les désignerons par la notation $a/b$ ou $\frac{a}{b}$ ou $ab^{-1}$. Mais bien entendu le lecteur devra se garder de commettre l'erreur grossière qui consisterait à croire que, pour que deux fractions $a/b$ et $c/d$ soient égales, il faut que $a = c$ et $b = d$; une fraction *n'est pas* un couple $(a, b)$ d'éléments de K, avec $b \neq 0$; c'est une classe de tels couples.

En partant de $\mathrm{K} = \mathbf{Z}$, anneau des entiers rationnels, il est clair que les considérations précédentes conduiraient au corps $\mathbf{Q}$ des nombres rationnels. D'ailleurs, si l'on connaît de nombreuses méthodes « simples » ou « géométriques » pour définir les nombres rationnels à partir des nombres entiers, on n'en connaît qu'une seule qui soit mathématiquement correcte — à savoir celle que nous venons d'exposer; l'hypothèse que $\mathrm{K} = \mathbf{Z}$ ne permet pas de la simplifier si peu que ce soit; voir la *Remarque* 1 ci-dessus.

### 5. *Fractions rationnelles à coefficients dans un corps*

Soit K un corps commutatif; on a vu (§ 27, Théorème 1) que pour tout entier $n \geq 1$ l'anneau $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ des polynômes à $n$ indéterminées à coefficients dans K est intègre. On peut donc lui appliquer les considérations des n° précédents. Le corps des fractions de l'anneau $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ se désigne par la notation

$$\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$$

et s'appelle le **corps des fractions rationnelles à** $n$ **variables** sur le corps K. Les éléments de $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ s'appellent eux-mêmes des **fractions rationnelles à** $n$ **variables à coefficients dans** K.

Pour manipuler pratiquement des fractions rationnelles, il est inutile, encore une fois, d'avoir recours aux considérations du n° 2 : celles-ci servent uniquement à prouver l'*existence* du corps $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$; mais ce qui compte dans la pratique, ce sont les *propriétés* de ce corps. Autrement dit, le lecteur devra retenir les assertions suivantes, *et rien d'autre :*

(FR 1) : *les fractions rationnelles à n variables à coefficients dans* K *sont les éléments d'un corps commutatif noté* $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$;

(FR 2) : *parmi les fractions rationnelles à n variables à coefficients dans* K *figurent les polynômes à n indéterminées à coefficients dans* K; plus précisément, l'anneau $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ des polynômes à $n$ indéterminées à coefficients dans K est un sous-anneau du corps $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$;

(FR 3) : *pour toute fraction rationnelle* $f \in \mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$, *il existe deux polynômes*

$p, q \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, *avec* $q \neq 0$, *tels que l'on ait*

$$f = pq^{-1} = p/q.$$

Bien entendu, il existe plusieurs façons d'écrire $f$ comme quotient de deux polynômes, et pour que deux fractions rationnelles $p'/q'$ et $p''/q''$ soient égales, il faut et il suffit que $p'q'' = p''q'$.

*Exemple* 1. Une fraction rationnelle à une variable à coefficients dans un corps K est une expression de la forme

$$f = \frac{p(\mathrm{X})}{q(\mathrm{X})},$$

où $p$ et $q$ sont des polynômes à une indéterminée X, à coefficients dans K, avec $q \neq 0$. Exemple :

$$\frac{\mathrm{X}^3 + \mathrm{X}^2 - 1}{\mathrm{X}^2 - 1}.$$

On notera que la condition $q \neq 0$ *n'exclut pas* la possibilité que l'on ait $q(x) = 0$ pour certains $x \in \mathrm{K}$; elle signifie simplement que $q$ n'est pas l'élément 0 de l'anneau K[X], i.e. que ses *coefficients* ne sont pas tous nuls.

*Exemple* 2. L'expression

$$f = \frac{\mathrm{X} + \mathrm{Y}}{\mathrm{X} - \mathrm{Y}}$$

est une fraction rationnelle à deux variables X et Y, à coefficients dans **Q**.

### 6. *Valeurs d'une fraction rationnelle*

Soient L un corps commutatif, K un sous-corps de L, et $f$ une fraction rationnelle à $n$ variables à coefficients dans K. Soit

$$u = (u_1, \ldots, u_n)$$

un élément de $\mathrm{L}^n$. On dit que $f$ **est définie en** $u$, ou que $u_1, \ldots, u_n$ **sont substituables dans** $f$, s'il existe des polynômes $p$ et $q$ vérifiant

$$f = p/q, \qquad q(u_1, \ldots, u_n) \neq 0;$$

cela ne veut pas dire que, *quels que soient* les polynômes $p$ et $q$ (avec $q \neq 0$) tels que $f = p/q$, on aura nécessairement $q(u_1, \ldots, u_n) \neq 0$.

*Exemple* 3. $u = 0$ est substituable dans la fraction rationnelle

$$\frac{\mathrm{X}^2}{\mathrm{X}^3 + \mathrm{X}},$$



car celle-ci s'écrit aussi

$$\frac{\mathrm{X}}{\mathrm{X} + 1}$$

et sous cette forme on voit que le dénominateur ne s'annulle pas pour $u = 0$.

Supposons $f$ définie en $u = (u_1, \ldots, u_n)$; on peut alors définir la **valeur de** $f$ **en** $u$, de la façon suivante. Écrivons

$$f = p/q \qquad \text{avec} \qquad q(u) \neq 0;$$

l'élément $p(u)/q(u)$ de L ne dépend alors que de $f$, et non du choix de $p$ et $q$; en effet, si l'on a une autre représentation de $f$, soit

$$f = p'/q' \qquad \text{avec} \qquad q'(u) \neq 0,$$

il vient

$$pq' = p'q,$$

donc (§ 28, formule (6))

$$p(u)q'(u) = p'(u)q(u),$$

et par suite

$$p(u)/q(u) = p'(u)/q'(u),$$

ce qui établit notre assertion. Cela dit, c'est l'élément $p(u)/q(u)$ de L qu'on appelle valeur de $f$ en $u$; et on le désigne par la notation

$$f(u) \qquad \text{ou} \qquad f(u_1, \ldots, u_n);$$

on a donc

$$f(u) = p(u)/q(u) \qquad \text{si} \qquad f = p/q \qquad \text{avec} \qquad q(u) \neq 0.$$

Il est clair que, si $f$ est un polynôme, alors $f$ est définie en $u$ quel que soit $u$, et que la valeur $f(u)$ qui résulte de la définition précédente coïncide avec celle qu'on a définie au § 28, n° 1 : il suffit pour le voir d'écrire $f = f/1$.

Montrons que *l'ensemble des fractions rationnelles qui sont définies en un point donné* $u \in \mathrm{L}^n$ *est un sous-anneau de* $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. Supposons en effet $f'$ et $f''$ définies en $u$; on peut alors écrire

$$\begin{aligned} f' &= p'/q' \qquad \text{avec} \qquad q'(u) \neq 0, \\ f'' &= p''/q'' \qquad \text{avec} \qquad q''(u) \neq 0, \end{aligned}$$

d'où

$$f' + f'' = \frac{p'q'' + p''q'}{q'q''}, \qquad f'f'' = \frac{p'p''}{q'q''},$$

et comme on a $q'(u)q''(u) \neq 0$ on voit que $f' + f''$ et $f'f''$ sont définies en $u$; comme les polynômes (et en particulier — 1) sont définis en $u$, il s'ensuit bien que les fractions rationnelles définies en $u$ forment un sous-anneau de $\mathrm{K}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$.

*Supposons* $f'$ *et* $f''$ *définies en* $u \in \mathrm{L}^n$; *alors les valeurs en* $u$ *des fractions* $f' + f''$ *et* $f'f''$ *sont égales respectivement à* $f'(u) + f''(u)$ *et* $f'(u)f''(u)$. Conservons en effet les

notations utilisées ci-dessus, et soit $g = f' + f''$; on a donc

$$g = p/q \qquad \text{avec} \qquad p = p'q'' + p''q', \qquad q = q'q'';$$

donc

$$g(u) = p(u)/q(u) = \frac{p'(u)q''(u) + p''(u)q'(u)}{q'(u)q''(u)} = \frac{p'(u)}{q'(u)} + \frac{p''(u)}{q''(u)},$$

ce qui prouve le premier résultat annoncé; le second se démontre de même.

*Supposons $f$ définie en $u$; pour que $f^{-1}$ soit définie en $u$, il faut et il suffit que $f(u) \neq 0$; on a alors*

$$f^{-1}(u) = f(u)^{-1}.$$

En effet supposons $f$ et $f^{-1}$ définies en $u$; on a $1 = f \cdot f^{-1}$, d'où, en prenant les valeurs en $u$,

$$1 = f(u) \cdot f^{-1}(u),$$

ce qui prouve que $f(u) \neq 0$ et que $f^{-1}(u) = f(u)^{-1}$. Inversement supposons $f$ définie en $u$ et $f(u) \neq 0$; on a $f = p/q$ avec $q(u) \neq 0$, et aussi $p(u) \neq 0$ puisque $f(u) \neq 0$; écrivant $f^{-1} = q/p$ on voit donc que la fraction rationnelle $f^{-1}$ est, elle aussi, définie en $u$.

*Exemple* 4. Prenons $n = 2$ et la fraction rationnelle

$$f = \frac{X + Y}{X - Y};$$

elle est définie en tout point $(u, v) \in L^2$ tel que $u \neq v$ (i.e. en dehors de la diagonale); il n'existe aucun autre point de $L^2$ où $f$ soit définie. En effet, soient $p$ et $q$ des polynômes à coefficients dans K tels que $f = p/q$; on a donc

$$(X + Y)q(X, Y) = (X - Y)p(X, Y);$$

posant $p = \sum p_n$, $q = \sum q_n$ où $p_n$ et $q_n$ sont homogènes de degré total $n$, on déduit immédiatement de la relation précédente que l'on a

$$(X + Y)q_n(X, Y) = (X - Y)p_n(X, Y);$$

on déduit de là (le lecteur le démontrera à titre d'exercice, en mettant en évidence les coefficients de $p_n$ et $q_n$, et en établissant des relations entre ces coefficients) que pour tout $n$ il existe un polynôme $r_n(X, Y)$ tel que

$$q_n(X, Y) = (X - Y)r_n(X, Y);$$

il s'ensuit évidemment que $q(u, v) = 0$ pour $u = v$, de sorte que $f$ n'est définie en aucun point de la diagonale de $L^2$, comme annoncé.

*Exemple* 5. K étant un corps commutatif arbitraire, prenons

$$L = K(X_1, \ldots, X_n),$$



et pour $u$ le point

$$u = (X_1, \ldots, X_n) \in L^n;$$

alors *toute* fraction rationnelle $f \in K(X_1, \ldots, X_n)$ est définie en $u$, car en écrivant $f = p/q$ avec $q \neq 0$, on a $q(X_1, \ldots, X_n) \neq 0$ pour la raison que

$$q(X_1, \ldots, X_n) = q$$

comme on l'a vu au § 28, *Remarque* 1. On peut donc définir $f(X_1, \ldots, X_n)$; cet élément de L est donné par

$$f(X_1, \ldots, X_n) = p(X_1, \ldots, X_n)/q(X_1, \ldots, X_n) = p/q = f.$$

Cela explique pourquoi, dans la pratique, on désigne souvent une fraction rationnelle par la notation $f(X_1, \ldots, X_n)$; mais les considérations développées ici permettent de *démontrer* que $f(X_1, \ldots, X_n) = f$, alors que dans les manuels classiques cette relation n'est considérée que comme une simple convention d'écriture.

Cet *Exemple* (et beaucoup d'autres) explique aussi pourquoi il est nécessaire de définir la valeur d'une fraction rationnelle à coefficients dans un corps K en un point dont les coordonnées appartiennent non à K, mais à un sur-corps arbitraire de K. Dans la pratique la plus élémentaire, il est évidemment indispensable de savoir attribuer une valeur à une fraction rationnelle à coefficients *réels* en un point à coordonnées *complexes*.

*Remarque* 2. Lorsqu'une fraction rationnelle $f \in K(X_1, \ldots, X_n)$ n'est pas définie en un point $u \in L^n$, où L est un surcorps commutatif de K, deux cas sont possibles : il peut arriver que l'inverse $1/f$ de $f$ soit définie en $u$ (on dit alors que $u$ est un **pôle de** $f$), et il peut arriver que $1/f$ ne soit pas non plus définie en $u$ (on dit alors que $u$ est un **point d'indétermination de** $f$). Le premier cas se produit si et seulement si l'on peut écrire

$$f = p/q \qquad \text{avec} \qquad p(u) \neq 0, \qquad q(u) = 0;$$

s'il en est ainsi, il est en effet clair que $f^{-1} = q/p$ est définie en $u$, et y a pour valeur 0, en sorte que $f$ ne peut être définie en $u$; inversement, si $u$ est un pôle de $f$, on peut écrire, puisque $f^{-1}$ est définie en $u$,

$$f^{-1} = q/p \qquad \text{avec} \qquad p(u) \neq 0;$$

si l'on avait $f^{-1}(u) \neq 0$, $f$ serait aussi définie en $u$ comme on l'a vu plus haut, ce qui par hypothèse n'est pas le cas; on a donc $f^{-1}(u) = 0$, i.e. $q(u) = 0$, et par suite

$$f = p/q \qquad \text{avec} \qquad p(u) \neq 0, \qquad q(u) = 0$$

comme annoncé.

Les considérations qui précèdent permettent d'autre part de caractériser les points d'indétermination de $f$: $u$ est un point d'indétermination de $f$ si, *quels que soient* les polynômes $p$ et $q$ tels que

$$f = p/q, \quad q \neq 0,$$

on a

$$p(u) = q(u) = 0.$$

Prenons par exemple $K = L = \mathbf{C}$ et la fraction rationnelle à deux indéterminées

$$f = \frac{X + Y}{X - Y};$$

elle est évidemment définie en tout point $(u, v) \in \mathbf{C}^2$ tel que $u \neq v$; les points de la diagonale $u = v$ autres que $(0, 0)$ sont évidemment des *pôles* de $f$; enfin, le point $(0, 0)$ est un *point d'indétermination* de $f$. Pour établir ce dernier résultat, il faut prouver que, si deux polynômes $p, q \in \mathbf{C}[X, Y]$ vérifient

$$\frac{p}{q} = \frac{X + Y}{X - Y},$$

alors on a nécessairement

$$p(0, 0) = q(0, 0) = 0.$$

Or posons

$$p = a + a'X + a''Y + \cdots$$
$$q = b + b'X + b''Y + \cdots,$$

les termes non écrits étant tous de degré deux au moins; on a par hypothèse

$$(X - Y)p = (X + Y)q$$

i.e.

$$(X - Y)\,(a + a'X + a''Y + \cdots) = (X + Y)\,(b + b'X + b''Y + \cdots)$$

et par suite

$$a(X - Y) = b(X + Y), \qquad \text{i.e. } a = b = -b,$$

d'où résulte évidemment $a = b = 0$; comme $p(0, 0) = a$ et $q(0, 0) = b$ notre assertion est établie.

L'étude détaillée des fractions rationnelles, et d'objets similaires (les « fonctions algébriques de plusieurs variables ») est l'un des principaux buts de la Géométrie Algébrique.

# § 30. Dérivations, formule de Taylor

Dans la théorie des fonctions d'une variable réelle, la dérivée $f'(t)$ d'une fonction $f(t)$ est définie à l'aide d'un « passage à la limite », i.e. à l'aide d'un processus aussi peu algébrique que possible. Cependant, lorsque $f$ est une fonction polynomiale, soit

$$f(t) = \sum a_r t^r,$$

on sait qu'il en est de même de la dérivée de $f$, et que celle-ci est

$$f'(t) = \sum r a_r t^{r-1}.$$

Il est clair que, si l'on se bornait à étudier des fonctions polynomiales, on pourrait *définir* la dérivée d'une telle fonction à l'aide des formules précédentes, dans lesquelles ne figure aucune opération de passage à la limite.

Ces remarques suggèrent la possibilité d'étendre la notion de dérivée aux polynômes à coefficients dans un anneau commutatif quelconque, et à démontrer dans ce cas, par des procédés purement algébriques, des propriétés qui, dans le cas classique, s'obtiennent par des raisonnements « analytiques » applicables à des fonctions beaucoup plus générales que les fonctions polynomiales. C'est ce qu'on va faire dans ce §. Les résultats ainsi obtenus ne sont pas de simples généralisations élégantes mais dénuées d'intérêt pratique de la théorie classique; on les utilisera effectivement plus loin pour distinguer les racines simples des racines multiples d'une équation algébrique, et on s'en sert aujourd'hui à propos d'autres problèmes importants (par exemple pour distinguer les « points simples » des « points multiples » d'une variété algébrique).

### *I. Dérivations dans un anneau*

Soit K un anneau; on appelle **dérivation de l'anneau** K toute application

$$D : K \to K$$

qui vérifie les relations

$$(1) \qquad D(x + y) = D(x) + D(y)$$
$$(2) \qquad D(xy) = D(x)\,y + xD(y)$$

quels que soient $x, y \in K$. Cette définition est évidemment inspirée par les règles de calcul classiques des dérivées; du reste :

*Exemple* 1. Prenons pour K l'anneau des fonctions polynomiales sur **R**; si

$$x(t) = \sum a_r t^r$$

est une telle fonction, définissons $D(x)$ comme étant la fonction

$$x'(t) = \sum r a_r t^{r-1};$$

les règles classiques de dérivation d'une somme et d'un produit montrent alors que l'application D ainsi définie est une dérivation de l'anneau K.

Les relations (1) et (2) montrent qu'on a

$$D(1) = 0 \tag{3}$$

car en faisant $y = 1$ dans (2) il vient $x.D(1) = 0$ pour tout $x$, en particulier pour $x = 1$. Plus généralement, on a, *si* K *est commutatif*,

$$D(x^n) = nx^{n-1}D(x) \tag{4}$$

pour tout $x \in K$ et tout entier $n \geqslant 0$; pour $n = 0$ ce résultat se réduit en effet à (3); et s'il est établi pour $n - 1$, alors (2) montre que

$$D(x^n) = D(x^{n-1}.x) = D(x^{n-1})x + x^{n-1}D(x) = (n-1)x^{n-2}D(x)x + x^{n-1}D(x) = nx^{n-1}D(x)$$

si K est commutatif.

## 2. *Dérivations d'un anneau de polynômes*

Nous allons démontrer le résultat suivant :

Théorème 1. *Soit* D *une dérivation d'un anneau commutatif* K. *Étant donné un polynôme* $u \in K[X]$, *il existe dans l'anneau* K[X] *une et une seule dérivation qui coïncide avec* D *sur* K *et qui applique le polynôme* X *sur le polynôme donné* $u$.

Supposons trouvée une telle dérivation D'; étant donné un polynôme

$$f = \sum a_r X^r \quad (a_r \in K),$$

les règles de calcul (1), (2), (4) donnent

$$D'(f) = \sum D'(a_r X^r) = \sum [D'(a_r)X^r + r a_r X^{r-1} D'(X)]$$

et vu les conditions imposées à D' il reste donc

$$D'(f) = \sum D(a_r)X^r + u(X)\sum r a_r X^{r-1}. \tag{5}$$

Pour exprimer le résultat, il est commode d'introduire d'une part le polynôme

$$f^D(X) = \sum D(a_r)X^r \tag{6}$$



obtenu en appliquant D aux coefficients de $f$, d'autre part le **polynôme dérivé**

$$f'(X) = \sum r a_r X^{r-1} \tag{7}$$

de $f$; ceci fait, la relation (5) s'écrit

$$D'(f) = f^D + u.f' \tag{8}$$

et prouve l'unicité de D'.

Il reste à montrer que l'application

$$D' : K[X] \to K[X]$$

donnée par la formule (8) est effectivement une dérivation satisfaisant aux conditions de l'énoncé. Les formules évidentes

$$(f+g)^D = f^D + g^D, \qquad (f+g)' = f' + g'$$

montrent déjà que D' vérifie (1). Pour établir (2), remarquons d'abord que si $D_1$ et $D_2$ sont des dérivations d'un anneau L, alors quels que soient $u_1, u_2 \in L$ l'application

$$x \mapsto u_1.D_1(x) + u_2.D_2(x)$$

de L dans L est encore une dérivation de L. Pour montrer que D' satisfait à (2), il suffit donc d'après (8) de prouver que, dans K[X], les deux applications

$$f \to f^D, \qquad f \mapsto f'$$

sont des dérivations, autrement dit qu'on a les formules

$$(fg)^D = f^D.g + f.g^D, \qquad (fg)' = f'g + fg'.$$

Supposons d'abord $f$ et $g$ réduits à des monômes,

$$f = aX^p, \qquad g = bX^q;$$

on a alors

$$(fg)^D = (abX^{p+q})^D = D(ab)X^{p+q} = D(a)X^p.bX^q + aX^p.D(b)X^q$$
$$(fg)' = (abX^{p+q})' = (p+q)abX^{p+q-1} = paX^{p-1}.bX^q + aX^p.qbX^{q-1},$$

ce qui établit évidemment les formules cherchées dans ce cas particulier. Dans le cas général, on décompose $f$ et $g$ en sommes de monômes, ce qui permet de se ramener facilement au cas particulier qu'on vient d'étudier.

Nous avons déjà établi que l'application (8) est bien une dérivation; il reste à vérifier d'une part qu'elle coïncide avec D sur K, autrement dit que

$$f = a \in K \quad \text{implique} \quad D'(f) = D(a),$$

ce qui est clair d'après (5); et d'autre part, que

$$D'(X) = u,$$

ce qui est aussi évident si l'on écrit $X = 1.X$ et si l'on remarque que $D(1) = 0$. Le Théorème 1 est donc entièrement démontré.

### 3. *Dérivées partielles*

Le Théorème 1 s'étend comme suit aux polynômes à plusieurs indéterminées :

THÉORÈME 2. *Soient* K *un anneau commutatif,* D *une dérivation de* K, *et* $u_1, \ldots, u_n$ *des polynômes à n indéterminées à coefficients dans* K. *Il existe alors une et une seule dérivation* D′ *de l'anneau* $K[X_1, \ldots, X_n]$ *qui se réduit à* D *sur* K *et qui vérifie*

$$D'(X_i) = u_i \quad \textit{pour} \quad 1 \leqslant i \leqslant n.$$

La démonstration est évidemment analogue à celle du Théorème 1, et nous nous bornerons à indiquer comment on calcule $D'(f)$ pour un polynôme

$$f = \sum a_{r_1 \ldots r_n} X_1^{r_1} \ldots X_n^{r_n}.$$

Comme D′ est une dérivation, on a

$$D'(f) = \sum D'(a_{r_1 \ldots r_n} X_1^{r_1} \ldots X_n^{r_n}) = \sum D'(a_{r_1 \ldots r_n}) X_1^{r_1} \ldots X_n^{r_n} + \sum a_{r_1 \ldots r_n} D'(X_1^{r_1}) X_2^{r_2} \ldots X_n^{r_n} + \cdots + \sum a_{r_1 \ldots r_n} X_1^{r_1} \ldots X_{n-1}^{r_{n-1}} D'(X_n^{r_n}),$$

et comme $D'(a) = D(a)$ pour $a \in K$, $D'(X_i) = u_i$, il vient

$$(9) \quad D'(f) = \sum D(a_{r_1 \ldots r_n}) X_1^{r_1} \ldots X_n^{r_n} + u_1 \sum r_1 a_{r_1 \ldots r_n} X_1^{r_1 - 1} X_2^{r_2} \ldots X_n^{r_n} + \cdots + u_n \sum r_n a_{r_1 \ldots r_n} X_1^{r_1} \ldots X_{n-1}^{r_{n-1}} X_n^{r_n - 1}.$$

On est ainsi conduit à introduire, comme au n° précédent, les notations suivantes. Tout d'abord on posera

$$f^D = \sum D(a_{r_1 \ldots r_n}) X_1^{r_1} \ldots X_n^{r_n};$$

c'est le polynôme obtenu en appliquant D aux coefficients de $f$. D'autre part, on appellera **dérivée partielle de $f$ par rapport à $X_i$** le polynôme

$$(10) \qquad f'_i = \sum r_i a_{r_1 \ldots r_n} X_1^{r_1} \ldots X_{i-1}^{r_{i-1}} X_i^{r_i - 1} X_{i+1}^{r_{i+1}} \ldots X_n^{r_n} :$$

si l'on regarde $f$ comme un polynôme en $X_i$, à coefficients dans l'anneau

$$K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n],$$

il est clair que $f'_i$ n'est autre que le polynôme dérivé de $f$ au sens du n° précédent (ce qui correspond bien à la notion classique de dérivée partielle d'une fonction de plusieurs variables : on dérive par rapport à une variable, en regardant les autres comme des « constantes »). Ceci dit, la relation (9) s'écrit encore

$$(11) \qquad D'(f) = f^D + \sum_{i=1}^{i=n} u_i . f'_i.$$



Dans la pratique, au lieu de la notation $f'_i$, on utilise souvent les notations

$$f'_{X_i}, \qquad \frac{\partial f}{\partial X_i}$$

qui sont d'usage courant en Analyse. Si l'on pose

$$D_i(f) = f'_i,$$

il est clair que l'application $D_i$ de l'anneau $K[X_1, \ldots, X_n]$ dans lui-même vérifie les conditions suivantes : c'est une *dérivation*, et on a

$$D_i(a) = 0 \quad \text{si} \quad a \in K$$
$$D_i(X_j) = \begin{cases} 0 & \text{si} \quad i \neq j \\ 1 & \text{si} \quad i = j. \end{cases}$$

Et, d'après le Théorème 2, ou d'après le Théorème 1 appliqué à l'anneau

$$K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$$

sur lequel $D_i$ est nulle, ces propriétés *caractérisent* l'application $D_i$.

### 4. *Dérivation des fonctions composées*

Le classique théorème de « dérivation des fonctions composées » est, lorsqu'il s'agit de polynômes, une conséquence du résultat suivant :

THÉORÈME 3. *Soient* L *un anneau commutatif,* K *un sous-anneau de* L, D *une dérivation de* L *nulle sur* K, *et f un polynôme à n indéterminées à coefficients dans* K. *On a alors*

$$D[f(u_1, \ldots, u_n)] = \sum_{i=1}^{i=n} f'_i(u_1, \ldots, u_n) . D(u_i)$$

*quels que soient* $u_1, \ldots, u_n \in L$.

Il suffit évidemment d'établir ce résultat lorsque $f$ est un monôme, soit

$$f = a X_1^{r_1} \ldots X_n^{r_n};$$

on a alors

$$D[f(u_1, \ldots, u_n)] = D(a . u_1^{r_1} \ldots u_n^{r_n})$$
$$= D(a) u_1^{r_1} \ldots u_n^{r_n} + \sum_{i=1}^{i=n} a . u_1^{r_1} \ldots u_i^{r_i - 1} D(u_i^{r_i}) u_{i+1}^{r_{i+1}} \ldots u_n^{r_n}$$
$$= D(a) u_1^{r_1} \ldots u_n^{r_n} + \sum_{i=1}^{i=n} D(u_i) . r_i a u_1^{r_1} \ldots u_i^{r_i - 1} u_i^{r_i - 1} u_{i+1}^{r_{i+1}} \ldots u_n^{r_n};$$

si $D = 0$ sur K, le premier terme disparaît, et il reste visiblement la formule cherchée.

COROLLAIRE. *Soient* K *un anneau commutatif, $f$ un polynôme à $n$ indéterminées à coefficients dans* K, *et*

$$u_1, \ldots, u_n \in \mathrm{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_p]$$

*des polynômes à $p$ indéterminées à coefficients dans* K. *Les dérivées partielles du polynôme*

$$g(\mathrm{Y}_1, \ldots, \mathrm{Y}_p) = f[u_1(\mathrm{Y}_1, \ldots, \mathrm{Y}_p), \ldots, u_n(\mathrm{Y}_1, \ldots, \mathrm{Y}_p)]$$

*sont données par les relations*

$$\frac{\partial g}{\partial \mathrm{Y}_j} = \sum_{i=1}^{i=n} f_i'(u_1, \ldots, u_p) \cdot \frac{\partial u_i}{\partial \mathrm{Y}_j} \quad (1 \leqslant j \leqslant p).$$

Il suffit pour le voir d'appliquer le Théorème 3 en prenant $\mathrm{L} = \mathrm{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_p]$ et pour D la dérivation partielle par rapport à $\mathrm{Y}_j$.

Le Corollaire précédent est à proprement parler le *théorème des fonctions composées pour les polynômes*.

On ne saurait en attendre des conséquences très profondes, étant donné qu'il résulte à peu près trivialement des *définitions* posées dans ce §.

### 5. *Formule de Taylor*

Soient K un anneau commutatif, $f$ un polynôme à *une* indéterminée et à coefficients dans K, et considérons le polynôme $\mathrm{X} + \mathrm{Y}$ à *deux* indéterminées X et Y et à coefficients dans K. En le substituant à la variable qui figure dans $f$, on obtient un polynôme

$$f(\mathrm{X} + \mathrm{Y}) \in \mathrm{K}[\mathrm{X}, \mathrm{Y}] = \mathrm{K}[\mathrm{X}]\,[\mathrm{Y}],$$

qu'on peut donc écrire comme polynôme en Y à coefficients dans l'anneau K[X], i.e. sous la forme

$$f(\mathrm{X} + \mathrm{Y}) = f_0(\mathrm{X}) + f_1(\mathrm{X})\mathrm{Y} + \cdots + f_n(\mathrm{X})\mathrm{Y}^n \tag{12}$$

si $f$ est de degré $n$. On se propose de calculer les polynômes $f_p(\mathrm{X})$ à l'aide des **dérivées successives** de $f$, à savoir les polynômes

$$f'' = (f')', \qquad f''' = (f'')', \ \ldots$$

Pour cela, dérivons par rapport à Y les deux membres de la relation (12); d'après le Corollaire du Théorème 3, le premier membre a pour dérivée $f'(\mathrm{X} + \mathrm{Y})$; il vient donc

$$f'(\mathrm{X} + \mathrm{Y}) = f_1(\mathrm{X}) + 2f_2(\mathrm{X})\mathrm{Y} + \cdots + nf_n(\mathrm{X})\mathrm{Y}^{n-1};$$

en dérivant à nouveau ce résultat par rapport à Y, on trouve

$$f''(\mathrm{X} + \mathrm{Y}) = 2f_2(\mathrm{X}) + 3 \cdot 2f_3(\mathrm{X})\mathrm{Y} + \cdots + n(n-1)f_n(\mathrm{X})\mathrm{Y}^{n-2},$$

et en poursuivant ainsi de suite on obtient évidemment

$$f^{(k)}(\mathrm{X} + \mathrm{Y}) = k!f_k(\mathrm{X}) + (k+1)k \ldots 2f_{k+1}(\mathrm{X})\mathrm{Y} + \ldots + n(n-1)\ldots(n-k+1)f_n(\mathrm{X})\mathrm{Y}^{n-k}.$$



Il est clair que la relation précédente, étant une égalité entre polynômes en X et Y à coefficients dans K, reste vraie si on y remplace X et Y par $u$ et $v$, où $u$ et $v$ sont des éléments arbitraires d'un sur-anneau commutatif L de K. En particulier, on peut remplacer X et Y par X et 0; il reste alors la relation

$$f^{(k)}(\mathrm{X}) = k!f_k(\mathrm{X}), \qquad 0 \leqslant k \leqslant n.$$

Donc :

THÉORÈME 4. *Soit $f$ un polynôme de degré $n$ à une indéterminée à coefficients dans un anneau commutatif* K, *et soient* X *et* Y *deux indéterminées sur* K. *On a alors*

$$f(\mathrm{X} + \mathrm{Y}) = f(\mathrm{X}) + f'(\mathrm{X})\mathrm{Y} + f_2(\mathrm{X})\mathrm{Y}^2 + \cdots + f_n(\mathrm{X})\mathrm{Y}^n \tag{12}$$

*avec*

$$k!f_k(\mathrm{X}) = f^{(k)}(\mathrm{X}) \quad \textit{pour} \quad 2 \leqslant k \leqslant n. \tag{13}$$

Ce résultat est connu sous le nom de **formule de Taylor** pour la raison suivante. Tout d'abord, comme c'est une égalité entre polynômes, on peut y remplacer les indéterminées X et Y par des éléments quelconques d'un sur-anneau commutatif arbitraire de K, en particulier par des éléments $x$ et $h$ de K; on a donc

$$f(x+h) = f(x) + f'(x)h + f_2(x)h^2 + \cdots + f_n(x)h^n \quad \text{avec} \quad k!f_k(x) = f^{(k)}(x),$$

quels que soient $x$, $h \in \mathrm{K}$. Supposons alors $\mathrm{K} = \mathbf{R}$, corps des nombres réels; il vient évidemment

$$f_k(x) = \frac{f^{(k)}(x)}{k!},$$

et le résultat obtenu s'écrit donc

$$f(x+h) = f(x) + h\frac{f'(x)}{1!} + h^2\frac{f''(x)}{2!} + \cdots + h^n\frac{f^{(n)}(x)}{n!},$$

ce qui est justement la formule de Taylor classique (celle-ci, dans le cas des fonctions *polynomiales*, est donc un résultat de nature purement algébrique).

EXEMPLE 2. Prenons $\mathrm{K} = \mathbf{Z}$ et

$$f(\mathrm{X}) = \mathrm{X}^n;$$

les formules (12) et (13) s'écrivent

$$(\mathrm{X} + \mathrm{Y})^n = \mathrm{X}^n + n\mathrm{X}^{n-1}\mathrm{Y} + f_2(\mathrm{X})\mathrm{Y}^2 + \cdots + f_n(\mathrm{X})\mathrm{Y}^n$$

avec

$$k!f_k(\mathrm{X}) = n(n-1)\ldots(n-k+1)\mathrm{X}^{n-k},$$

ou encore

$$k!\left[f_k(\mathrm{X}) - \binom{n}{k}\mathrm{X}^{n-k}\right] = 0;$$

puisque l'anneau $\mathbf{Z}$ est intègre, il s'ensuit que

$$f_k(X) = \binom{n}{k} X^{n-k};$$

ainsi, on obtient dans ce cas la relation

$$(X + Y)^n = \sum_{k=0}^{k=n} \binom{n}{k} X^{n-k} Y^k.$$

Pour en déduire la formule du binôme établie au § 8, n° 4, il suffit de remarquer que si deux polynômes $f(X, Y)$ et $g(X, Y)$ à coefficients *entiers rationnels* sont identiques, alors la relation

$$f(x, y) = g(x, y)$$

est vraie lorsque $x$ et $y$ sont des éléments *arbitraires* d'un anneau commutatif *arbitraire* L.

### 6. *Caractéristique d'un corps commutatif*

Revenons au Théorème 4. Pour que la formule (12) soit réellement intéressante, il est nécessaire qu'on puisse calculer complètement les polynômes $f_k$, et pour cela il s'impose d'essayer de les déduire de la formule (13). Autrement dit, nous avons à résoudre le problème suivant : étant donnés un entier rationnel $r \neq 0$ (en l'occurence, $k!$) et un élément $b$ de K [en l'occurence, l'un quelconque des coefficients du polynôme $f^{(k)}(X)$], trouver tous les $x \in K$ tels que

$$r.x = b.$$

Étant donné que

$$rx = (r.1)x$$

où 1 est l'élément unité de K, le problème aura une et une seule solution dès que $r.1$ est *inversible*. Si K est un *corps commutatif*, cela signifie que $r.1 \neq 0$.

Dans l'hypothèse où K est un corps commutatif, on est donc amené à considérer, dans l'anneau $\mathbf{Z}$ des entiers rationnels, l'ensemble I des entiers $r$ tels que

$$r.1 = 0;$$

I contient 0, et s'il contient deux entiers $r$ et $s$ il contient visiblement $r - s$ : c'est donc un sous-groupe du groupe additif $\mathbf{Z}$, et par suite (§ 7, *Exemple* 8) *il existe un entier* $p \geqslant 0$ *et un seul tel que* $I = p\mathbf{Z}$; on dit que $p$ est la **caractéristique** du corps K.

La caractéristique $p$ d'un corps commutatif K peut évidemment se définir comme suit : si la relation $r.1 = 0$ implique $r = 0$, alors $p = 0$; sinon, $p$ est le plus petit entier strictement positif tel que $p.1 = 0$. Dans tous les cas, la relation $r.1 = 0$ signifie que $r$ est multiple de $p$, ou encore : *pour que* $r.1 \neq 0$ *il faut et il suffit que* $r$ *ne soit pas divisible par la caractéristique de* K.

Il est important de noter que *la caractéristique d'un corps commutatif est toujours soit* 0, *soit un nombre premier*. Supposons en effet le corps K de caractéristique $p \neq 0$, et considérons deux entiers $r$ et $s$ tels que

$$p = rs;$$

on a alors

$$0 = p.1 = (r.1)\,(s.1);$$

comme un corps est un anneau d'intégrité, il en résulte soit $r.1 = 0$ (auquel cas $p$ divise $r$) soit $s.1 = 0$ (auquel cas $p$ divise $s$), ce qui établit notre assertion.

Si K est un *corps de caractéristique* 0, alors pour tout $b \in K$ et tout entier $r \neq 0$, l'équation

$$rx = b$$

possède dans K une et une seule solution, à savoir

$$x = (r.1)^{-1}b,$$

que l'on écrit plus simplement sous la forme

$$x = \frac{b}{r} \qquad \text{ou} \qquad b/r.$$

*Exemple* 3. Les corps $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ et plus généralement tout sur-corps commutatif de $\mathbf{Q}$, sont évidemment de caractéristique 0.

*Exemple* 4. Prenons $K = \mathbf{Z}/p\mathbf{Z}$ où $p$ est un nombre premier (§ 8, Théorème 1); pour tout entier rationnel $r$, la relation $r.1 = 0$ dans $\mathbf{Z}/p\mathbf{Z}$ signifie évidemment que $r$ est nul comme entier modulo $p$, autrement dit que $r$ est multiple de $p$; donc ici on a $I = p\mathbf{Z}$, autrement dit *le corps* $\mathbf{Z}/p\mathbf{Z}$, *pour* $p$ *premier, est de caractéristique* $p$.

*Remarque* 1. Soit K un corps de caractéristique 0; l'application

$$n \mapsto n.1$$

de $\mathbf{Z}$ dans K est donc injective, et par suite est un isomorphisme de $\mathbf{Z}$ sur un sous-anneau de K. En fait, cette application peut même se prolonger en un isomorphisme du corps $\mathbf{Q}$ sur un sous-corps de K; soit en effet $x \in \mathbf{Q}$ et écrivons $x = a/b$ avec $a, b \in \mathbf{Z}$, $b \neq 0$; alors l'élément

$$j(x) = (a.1)\,(b.1)^{-1}$$

de K ne dépend que de $x$, et non de la représentation de $x$ sous forme de fraction; en effet, la relation $a'/b' = a''/b''$ s'écrit $a'b'' = a''b'$, donc implique

$$(a'.1)\,(b''.1) = (a''.1)\,(b'.1),$$

donc

$$(a'.1)\,(b'.1)^{-1} = (a''.1)\,(b''.1)^{-1},$$

ce qui prouve notre assertion. Ceci dit, il est immédiat de vérifier que l'application $j$ de $\mathbf{Q}$ dans K ainsi obtenue est un isomorphisme de $\mathbf{Q}$ sur un sous-corps de K.

Dans la pratique, on identifie le plus souvent chaque nombre rationnel $x \in \mathbf{Q}$ à son image $j(x)$ dans K, de sorte que $\mathbf{Q}$ *est un sous-corps de tout corps de caractéristique* 0.

On peut également montrer (cf. *Exercice* 8) que tout corps K de caractéristique $p \neq 0$ contient un sous-corps isomorphe à $\mathbf{Z}/p\mathbf{Z}$, à savoir l'ensemble des multiples entiers $r.1$ ($r \in \mathbf{Z}$) de l'élément unité de K.

Si K est un *corps de caractéristique* 0, il est clair que la formule de Taylor du n° précédent prend la forme

$$f(X+Y) = \sum_{k=0}^{k=n} f^{(k)}(X) \cdot \frac{Y^k}{k!}. \tag{14}$$

Ce résultat est encore valable en caractéristique $p \neq 0$ pourvu que l'on ait $k!.1 \neq 0$ pour $k \leqslant n$, autrement dit pourvu que $p$ ne divise aucun entier inférieur à $n$, autrement dit pourvu que

$$n < p.$$

### 7. *Ordre de multiplicité des racines d'une équation*

Soient K un anneau commutatif, $f$ un polynôme à une indéterminée à coefficients dans K, et dans la formule de Taylor

$$f(X+Y) = f(X) + f'(X)Y + f_2(X)Y^2 + \cdots$$

remplaçons X et Y par $a$ et $T - a$ respectivement, où $a$ est un élément donné de K et où T est une indéterminée sur K; il vient

$$\begin{aligned} f(T) &= f(a) + f'(a).(T-a) + f_2(a).(T-a)^2 + \cdots \\ &= f(a) + (T-a)q(T) \end{aligned}$$

où $q \in K[T]$. Étant donnés des polynômes $g$, $h$ à coefficients dans K, disons que $h$ **est divisible par** $g$ s'il existe un troisième polynôme $q$, à coefficients dans K, tel que $h = gq$. Le résultat que nous venons d'obtenir conduit immédiatement à l'énoncé que voici (déjà établi au § 28, Lemme 1) :

THÉORÈME 5. *Soit $f$ un polynôme à une indéterminée à coefficients dans un anneau commutatif K; pour qu'un élément $a$ de K soit racine de $f$, il faut et il suffit que le polynôme $f(X)$ soit divisible par le polynôme $X - a$.*

En effet, si $a$ est racine de $f$, on a $f(a) = 0$, et la formule de Taylor montre donc que

$$f(T) = (T-a)q(T).$$

Inversement, de cette relation résulte

$$f(a) = (a-a)q(a) = 0,$$

d'où le Théorème.



Étant donnée une racine $a \in K$ du polynôme $f$, on appelle **ordre de multiplicité de** $a$ le plus grand entier $r$ tel que le polynôme $f(T)$ soit divisible par le polynôme

$$(T-a)^r.$$

Si $r = 1$, on dit que $a$ est une **racine simple;** si $r = 2$, que $a$ est une **racine double,** etc.

THÉORÈME 6. *Soit $f$ un polynôme à une indéterminée à coefficients dans un anneau commutatif quelconque* K; *pour qu'un élément $a \in K$ soit racine simple de $f$, il faut et il suffit que l'on ait*

$$f(a) = 0, \qquad f'(a) \neq 0.$$

En effet, si $a$ est racine, on a

$$f(T) = (T-a)q(T) \quad \text{avec} \quad q(T) = f'(a) + f_2(a).(T-a) + \cdots,$$

d'où

$$q(a) = f'(a).$$

Supposons $f'(a) = 0$; alors (Théorème 5) le polynôme $q(T)$ est divisible par $T - a$, donc $f$ est divisible par $(T-a)^2$, et $a$ n'est pas racine simple. Si inversement $a$ n'est pas racine simple, on a une relation

$$f(T) = (T-a)^2 g(T),$$

d'où

$$f'(T) = 2(T-a)g(T) + (T-a)^2 g'(T),$$

ce qui prouve évidemment que $f'(a) = 0$ et achève la démonstration.

THÉORÈME 7. *Soit $f$ un polynôme à une indéterminée à coefficients dans un corps commutatif* K *de caractéristique* 0. *Pour qu'un élément $a$ de* K *soit racine multiple d'ordre $r$ de $f$, il faut et il suffit qu'il vérifie les relations*

$$f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0, \qquad f^{(r)}(a) \neq 0. \tag{15}$$

Supposons que $a$ soit racine multiple d'ordre $r$; on a alors

$$f(T) = (T-a)^r g(T), \tag{16}$$

avec en outre $g(a) \neq 0$, sinon (Théorème 5) $g(T)$ serait divisible par $T - a$, et $f(T)$ par $(T-a)^{r+1}$. Or, en dérivant $k$ fois la relation (16) on trouve évidemment une relation de la forme

$$f^{(k)}(T) = r(r-1)\ldots(r-k+1)(T-a)^{r-k}g(T) + (T-a)^{r-k+1}q_k(T),$$

où $q_k$ est un polynôme dont la forme exacte importe peu; de cette relation on tire $f^{(k)}(a) = 0$ pour $k \leqslant r-1$, et en outre

$$f^{(r)}(a) = r!\,g(a);$$

comme $g(a) \neq 0$ et comme K est de caractéristique 0, on a bien $f^{(r)}(a) \neq 0$.

Inversement, supposons réalisées les conditions (15); comme K est de caractéristique 0, on peut écrire

$$f(\mathrm{T}) = \sum_{k=0}^{k=n} (\mathrm{T}-a)^k . \frac{f^{(k)}(a)}{k!} = (\mathrm{T}-a)^r \left[ \frac{f^{(r)}(a)}{r!} + (\mathrm{T}-a)\frac{f^{(r+1)}(a)}{(r+1)!} + \cdots \right];$$

autrement dit, on a une relation

$$f(\mathrm{T}) = (\mathrm{T}-a)^r g(\mathrm{T})$$

avec $g(a) \neq 0$; si $f$ était divisible par $(\mathrm{T}-a)^{r+1}$ il est clair, puisque K[T] est un anneau d'intégrité, que $g$ serait divisible par $\mathrm{T}-a$, ce qui est impossible puisque $g(a)$ n'est pas nul; par conséquent, $(\mathrm{T}-a)^r$ est la plus haute puissance de $\mathrm{T}-a$ qui divise $f$, et $a$ est donc racine multiple d'ordre $r$, ce qui achève la démonstration.

*Exemple* 5. K étant un corps de caractéristique 0, cherchons à quelle condition l'équation

$$x^3 + px + q = 0$$

à coefficients $p$, $q$ dans K admet une racine multiple $a$. Celle-ci doit annuler le premier membre *et* sa dérivée (Théorème 6) i.e. vérifier

$$\begin{aligned} a^3 + pa + q &= 0 \\ 3a^2 + p &= 0; \end{aligned}$$

multipliant la première relation par 3, la seconde par $a$, et retranchant membre à membre, on en déduit que $2pa + 3q = 0$, i.e. que

$$a = -3q/2p;$$

et en portant ce résultat dans la relation $3a^2 + p = 0$, on en conclut aussitôt que les coefficients $p$ et $q$ doivent vérifier

$$4p^3 + 27q^2 = 0.$$

Inversement, si cette relation est vérifiée, il est immédiat de voir que $-3q/2p$ est racine double de l'équation considérée.

Le lecteur pourra vérifier qu'en fait ces résultats supposent seulement que la caractéristique de K est différente de 2 et 3, et non pas que K est de caractéristique 0.

# EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

¶ **1.** On considère deux fractions rationnelles $f, g \in K(X_1, \ldots, X_n)$ où K est un anneau d'intégrité commutatif *infini*. On suppose qu'il existe dans l'ensemble $K^n$ un ouvert de Zariski (§§ 27, 28, *Exercice* 1) non vide A tel que $f$ et $g$ soient définies et aient la même valeur en tout point $x \in A$. Montrer qu'alors $f = g$. (Ce résultat, notamment dans le cas classique où $K = \mathbf{R}$ ou $\mathbf{C}$, explique pourquoi on a le droit d'identifier toute fraction rationnelle à coefficients dans K à la fonction qu'elle définit sur une partie de $K^n$.)

**2.** Une fonction rationnelle à *une* variable ne possède aucun point d'indétermination (si $f = p/q$ où $p$ et $q$ s'annulent simultanément en $a$, mettre en facteur dans $p$ et $q$ les plus hautes puissances possibles de $X - a$).

**3.** Soient K un corps commutatif, $a$ un élément de K, et A l'ensemble des fractions rationnelles $f \in K(X)$ qui sont définies en $a$. Montrer que A est un anneau de valuation du corps $K(X)$ (§ 8, *Exercice* 6) et que l'idéal des éléments non inversibles de A est formé des $f \in A$ telles que $f(a) = 0$.
Montrer que les $f \in K(X)$ qui peuvent s'écrire sous la forme $f = p/q$, où $p$ et $q$ sont des polynômes tels que

$$d^o(p) \leqslant d^o(q),$$

forment également un anneau de valuation de $K(X)$.

**4.** Soient L un corps commutatif, K un sous-corps de L, et $x_1, \ldots, x_n$ des éléments de L. On désigne par $K(x_1, \ldots, x_n)$ le plus petit sous-corps de L contenant K et les $x_i$ (sous-corps de L **engendré** par K et les $x_i$; un corps contenant K comme sous-corps et engendré par K et un nombre fini d'éléments s'appelle une **extension de type fini** de K, ou un **corps de fonctions algébriques** sur K). Montrer que c'est l'ensemble des éléments de L qui peuvent s'écrire sous la forme

$$f(x_1, \ldots, x_n)$$

où $f \in K(X_1, \ldots, X_n)$ est définie en $(x_1, \ldots, x_n)$. Montrer que $K(x_1, \ldots, x_n)$ est isomorphe à $K(X_1, \ldots, X_n)$ si les $x_i$ sont algébriquement indépendants sur K.

¶ **5.** Soit K un corps commutatif. Étant donnée une fraction rationnelle $f \in K(X)$ non dans K, montrer que l'élément X du corps $K(X)$ est algébrique sur le sous-corps $K(f)$ engendré par K et $f$. En déduire qu'il en est de même de tout $g \in K(X)$.
Montrer qu'*étant donnés deux polynômes $p, q \in K[X]$, il existe une relation algébrique non triviale, à coefficients dans K, entre $p$ et $q$.*



¶¶ **6.** Soient L un corps commutatif et K un sous-corps de L.

*a*) Soient $x_1, \ldots, x_r, y, z$ des éléments de L; on suppose que $z$ est algébrique sur le sous-corps $K(x_1, \ldots, x_r, y)$ mais non sur $K(x_1, \ldots, x_r)$; montrer qu'alors $y$ est algébrique sur

$$K(x_1, \ldots, x_r, z).$$

*b*) On suppose que L est de **degré de transcendance fini** sur K, autrement dit qu'il existe un entier $n$ tel que $n + 1$ éléments quelconques de L vérifient une relation algébrique non triviale à coefficients dans K. Montrer qu'on peut alors trouver des éléments $x_1, \ldots, x_r$ de L, en nombre fini, algébriquement indépendants sur K, et tels que tout élément de L soit algébrique sur le sous-corps $K(x_1, \ldots, x_r)$ (on dit alors que les $x_i$ forment une **base de transcendance** de L sur K).

*c*) Soient $x_1, \ldots, x_r$ et $y_1, \ldots, y_s$ deux bases de transcendance de L sur K. Montrer qu'il existe un indice $j$ tel que $y_j$ ne soit pas algébrique sur $K(x_1, \ldots, x_{r-1})$ (observer que dans le cas contraire tout élément de L serait algébrique sur ce sous-corps, et en particulier $x_r$). En déduire, à l'aide de la question *a*), que $x_1, \ldots, x_{r-1}, y_j$ forment une base de transcendance de L sur K.

*d*) Déduire de là que deux bases de transcendance quelconques de L sur K ont le même nombre d'éléments (qu'on appelle le **degré de transcendance** de L sur K). Montrer que ce nombre est le plus grand entier $n$ tel qu'on puisse trouver $n$ éléments de L algébriquement indépendants sur K.

*e*) Montrer que *si $f_1, \ldots, f_{n+1}$ sont $n + 1$ fractions rationnelles à $n$ indéterminées, à coefficients dans un corps commutatif* K, *il existe une relation algébrique non triviale, à coefficients dans* K, *entre $f_1, \ldots, f_{n+1}$.*

*f*) On suppose le corps commutatif K *infini*. Soit A un ouvert de Zariski (§§ 27, 28, *Exercice* 1) non vide dans $K^p$; on dit qu'une application $f$ de A dans $K^q$ est **rationnelle** s'il existe des fractions rationnelles

$$f_1, \ldots, f_q \in K(X_1, \ldots, X_p)$$

telles que $f_1, \ldots, f_q$ soient définies en tout $x \in A$ et que l'on ait

$$f(x) = (f_1(x), \ldots, f_q(x)) \quad \text{pour tout } x \in A$$

(Cette notion généralise celle d'application polynomiale des §§ 27, 28, *Exercice* 17.) Cela dit, montrer que si une application rationnelle de A dans $K^q$ est *surjective*, on a $p \geqslant q$. (Ce résultat montre que les phénomènes « pathologiques » du type de la courbe de Peano — existence d'une application *continue* d'une droite *sur* un plan, par exemple — ne peuvent pas se produire lorsqu'on se limite à des applications définies par des fonctions polynomiales ou rationnelles.)

[La notion de degré de transcendance exposée dans cet *Exercice* est à la base de la définition de la dimension d'une variété algébrique.
Soit V une **variété algébrique** dans $\mathbf{C}^n$, i.e. une partie de $\mathbf{C}^n$ définie par un nombre fini d'équations

$$f_1(x) = \cdots = f_r(x) = 0$$

où $f_1, \ldots, f_r$ sont des polynômes à $n$ variables à coefficients dans $\mathbf{C}$. On appelle *fonction polynomiale* sur V toute application de V dans $\mathbf{C}$ qui est la restriction à V d'une fonction polynomiale sur $\mathbf{C}^n$. Ces fonctions polynomiales sur V forment évidemment un anneau A contenant $\mathbf{C}$ (fonctions constantes), et d'ailleurs engendré sur $\mathbf{C}$ par $n$ éléments convenablement choisis (par exemple les restrictions à V des fonctions coordonnées de $\mathbf{C}^n$). On dit que V est **irréductible** si l'anneau A est intègre; il revient au même, comme on peut le démontrer, d'exiger que V

ne peut pas s'écrire comme réunion de deux autres variétés algébriques distinctes de V. Si V est irréductible, on peut former le corps L des fractions de A; en notant $f_1, \ldots, f_n$ les restrictions à V des fonctions coordonnées de $\mathbf{C}^n$, il est clair que

$$L = \mathbf{C}(f_1, \ldots, f_n).$$

On dit que L est le **corps des fonctions rationnelles de la variété** V. Cela fait, L est de degré de transcendance fini sur $\mathbf{C}$, et on appelle alors **dimension** de V le degré de transcendance de L sur $\mathbf{C}$. Une « courbe » est de dimension 1, une « surface » de dimension 2, etc...
On démontre que la dimension $p$ d'une variété algébrique irréductible V est aussi le plus grand entier tel que l'on puisse construire une chaîne croissante

$$V_0 \subset V_1 \subset \cdots \subset V_p = V$$

de variétés algébriques irréductibles non vides et deux à deux distinctes. Une « surface » contient une « courbe » qui contient un « point », ce qui explique (sic) pourquoi une « surface » est de dimension 2.
Les variétés algébriques dans $\mathbf{C}^n$ sont utilisées en Analyse, notamment pour étudier les systèmes d'équations aux dérivées partielles linéaires à coefficients constants. Considérons par exemple l'équation

$$\sum_{i_1, \ldots, i_n \geqslant 0} a_{i_1 \cdots i_n} \frac{\partial^{i_1 + \cdots + i_n} f}{\partial x_1^{i_1} \ldots \partial x_n^{i_n}} = 0$$

où $f$ est une fonction inconnue de $n$ variables réelles, et où les coefficients $a_{i_1 \cdots i_n}$ sont des constantes complexes presque toutes nulles. Si l'on cherche les solutions de la forme

$$f(x_1, \ldots, x_n) = e^{u_1 x_1 + \cdots + u_n x_n}$$

où $u_1, \ldots, u_n$ sont des constantes complexes, on est évidemment ramené à résoudre l'équation

$$\Sigma a_{i_1 \cdots i_n} \cdot u_1^{i_1} \ldots u_n^{i_n} = 0.$$

i.e. à étudier l'hypersurface algébrique de $\mathbf{C}^n$ définie par cette équation.]

**7.** Trouver les pôles et les points d'indétermination des fractions rationnelles suivantes :

$$\frac{X}{Y}; \quad \frac{X - Y}{XY}; \quad \frac{(X^2 - 1)(Y^2 - 1)}{X^2 + Y^2 - 1}; \quad \frac{X + Y + Z}{X - Y}; \quad \frac{X - Z}{Y - Z}$$

(on prendra $\mathbf{C}$ pour corps de base).

**8.** Soit K un corps commutatif; on considère (§§ 27, 28, *Exercice* **11**) l'anneau K[[X]] des séries formelles à une variable à coefficients dans K. Comme c'est un anneau d'intégrité on peut former son corps des fractions, qu'on note K((X)). Montrer que tout élément de celui-ci s'écrit d'une façon et d'une seule sous la forme du produit d'une puissance (éventuellement négative) de X par une série formelle dont le terme constant n'est pas nul, i.e. sous la forme d'une « série »

$$(*) \qquad \sum_{n=-\infty}^{n=+\infty} a_n X^n$$

à coefficients $a_n$ dans K, avec la condition que les entiers $n$ *négatifs* tels que $a_n \neq 0$ soient en nombre fini.
On notera que, comme K[X] est un sous-anneau de K[[X]], le corps K((X)) contient un



sous-corps isomorphe à K(X), en sorte que toute fraction rationnelle à une variable à coefficients dans K peut se représenter par une série de la forme (*). Trouver les séries formelles (*) représentant les fractions rationnelles suivantes :

$$\frac{1}{X - X^2}; \qquad \frac{X^2 + X + 1}{X^4 - X^2}.$$

Montrer que la série (*) représentant une fraction rationnelle $f$ ne comporte aucune puissance négative de X lorsque $f$ est définie en $x = 0$, et réciproquement (*).
Montrer que K[[X]] est un anneau de valuation (§ 8, *Exercice* 6) du corps K((X)).

**9.** Soient A un anneau commutatif et S une partie de A; on suppose que S contient 1 mais ne contient pas 0, et que l'on a $xy \in S$ quels que soient $x \in S$, $y \in S$ (si A est un anneau d'intégrité on peut prendre par exemple pour S l'ensemble des éléments non nuls de A; dans le cas général, un exemple important s'obtient en prenant pour S l'ensemble des $x \in A$ qui n'appartiennent pas à un idéal premier donné de A).

*a*) Soit F l'ensemble des couples $(x, s)$ avec $x \in A$, $s \in S$; étant donnés deux éléments $y' = (x', s')$ et $y'' = (x'', s'')$ de F, on désigne par $R\{y', y''\}$ la relation

$$\text{il existe un } s \in S \text{ tel que } \quad s(x's'' - x''s') = 0.$$

Montrer que R est une relation d'équivalence sur F. Que se passe-t-il lorsque A est intègre et qu'on prend pour S l'ensemble des éléments non nuls de A ?

*b*) Soient $A_S$ l'ensemble quotient F/R et $\theta$ l'application canonique de F sur F/R. Montrer qu'il existe sur $A_S$ une et une seule structure d'anneau commutatif telle que l'on ait les formules

$$\theta(x, s) + \theta(y, t) = \theta(xt + ys, st)$$
$$\theta(x, s) \cdot \theta(y, t) = \theta(xy, st).$$

*c*) Montrer que l'application $j$ de A dans $A_S$ donnée par

$$j(x) = \theta(x, 1)$$

est un homomorphisme d'anneaux, que $j(s)$ est inversible dans $A_S$ pour tout $s \in S$, et que tout élément de $A_S$ est quotient d'un élément $j(x)$, $x \in A$, par un élément $j(s)$, $s \in S$. Quel est le noyau de l'homomorphisme $j$? A quelle condition $j$ est-il injectif?

*d*) Soit $f$ un homomorphisme de A dans un anneau commutatif K. Pour que $f(s)$ soit inversible dans K quel que soit $s \in S$, il faut et il suffit que $f$ soit composé de l'homomorphisme $j$ de la question précédente et d'un homomorphisme de l'anneau $A_S$ dans l'anneau K.

*e*) Soient A un anneau d'intégrité commutatif, K son corps des fractions, et $\mathfrak{p}$ un idéal premier de A (i.e. tel que $\mathfrak{p} \neq A$ et que la relation $xy \in \mathfrak{p}$ implique $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$); on prend pour S le complémentaire de $\mathfrak{p}$ dans A. Montrer que l'anneau $A_S$ est isomorphe au sous-anneau $A_{\mathfrak{p}}$ de K formé des fractions qui peuvent se mettre sous la forme $x/y$ avec $x, y \in A$ et $y \notin \mathfrak{p}$.

(*) L'opération qui, étant donnés deux polynômes $f, g \in K[X]$, consiste à écrire sous la forme (*) la fraction rationnelle $f/g$ est connue dans les ouvrages anciens sous le nom de *division de $f$ par $g$ suivant les puissances croissantes de* X; elle consiste aussi, pour chaque entier $r \geqslant 0$ (et si le terme constant de $g$ n'est pas nul, cas auquel on peut toujours se ramener trivialement), à trouver un polynôme $q$ de degré $\leqslant r$, tel que $f(X) - q(X)g(X)$ soit multiple de $X^{r+1}$. Le polynôme $q$ s'obtient en supprimant les termes de degré $> r$ de la série formelle (*) qui représente $f/g$.
Dans la pratique, on doit effectuer ces opérations lorsqu'on veut développer en série entière ou de Laurent le quotient de deux polynômes ou séries entières, ou en trouver des développements limités.

*f*) Les hypothèses restant celles de *e*), on associe à chaque idéal $\mathfrak{a}$ de l'anneau $A_\mathfrak{p}$, distinct de $A_\mathfrak{p}$, l'idéal $A \cap \mathfrak{a}$ de l'anneau A. Montrer qu'on obtient de cette façon une bijection de l'ensemble des idéaux de $A_\mathfrak{p}$ distincts de $A_\mathfrak{p}$ sur l'ensemble des idéaux de A contenus dans $\mathfrak{p}$. Quelle est l'application réciproque?

*g*) Soient L un corps commutatif et $a_1, \ldots, a_n$ des éléments de L. On prend

$$A = L[X_1, \ldots, X_n]$$

et pour $\mathfrak{p}$ l'ensemble des polynômes $f \in A$ tels que $f(a_1, \ldots, a_n) = 0$. Montrer que $A_\mathfrak{p}$ est l'ensemble des fractions rationnelles $f(X_1, \ldots, X_n)$, à coefficients dans L, qui sont définies au point $(a_1, \ldots, a_n)$ de $K^n$.

*h*) Étendre les résultats de la question *f*) au cas d'un anneau de fractions $A_S$ quelconque.

**10.** Soient A un anneau d'intégrité commutatif et K son corps des fractions. Montrer que le corps des fractions de l'anneau de polynômes A[X] est canoniquement isomorphe au corps de fractions rationnelles K(X).

**11.** Soient A un anneau d'intégrité commutatif, M un A-module, et K le corps des fractions de A. On se propose de montrer que, *si* M *est sans torsion* (§ 10, *Exercice* 11; les résultats de cet Exercice ne seront pas utiliser ici), *on peut plonger* M *dans un espace vectoriel sur* K (exemple trivial : $A^n$ se plonge dans $K^n$).
On ne fait aucune hypothèse sur M jusqu'à nouvel ordre.

*a*) Soit F l'ensemble des couples $(m, s)$ avec $m \in M$, $s \in A$ et $s \neq 0$. Étant donnés deux éléments $x' = (m', s')$ et $x'' = (m'', s'')$ de F, on note $R\{x', x''\}$ la relation

$$\text{il existe un } s \in A \text{ tel que } s(s'm'' - s''m') = 0 \text{ et } s \neq 0.$$

Montrer que R est une relation d'équivalence sur l'ensemble F.

*b*) Soit V l'ensemble quotient F/R; on note $\theta$ l'application canonique de F sur V. Montrer qu'on peut définir la somme de deux éléments de V de telle sorte que l'on ait

$$\theta(m', s') + \theta(m'', s'') = \theta(s''m' + s'm'', s's'')$$

quels que soient $(m', s')$, $(m'', s'') \in F$, et que V, muni de cette loi de composition, est un groupe commutatif.

*c*) Montrer qu'il existe une application $(\lambda, x) \to \lambda x$ de $K \times V$ dans V qui vérifie la condition suivante : si $\lambda = u/s$ et si $x = \theta(m, t)$ (avec $u, s, t \in A$, $m \in M$, et $s, t$ non nuls), on a

$$\lambda x = \theta(um, st).$$

Montrer que le groupe commutatif V, muni de cette application, est un espace vectoriel sur K.

*d*) On définit une application « canonique » $j$ de M dans V par

$$j(m) = \theta(m, 1);$$

montrer que c'est un homomorphisme de A-modules (NB : comme V est un espace vectoriel sur K, on peut *a fortiori* regarder V comme un A-module), dont le noyau est le sous-module de torsion de M (i.e. l'ensemble des $m$ tels que l'on ait $sm = 0$ pour au moins un $s \in A$ *non nul*). En déduire que, si M est sans torsion, $j$ est un isomorphisme de M sur un sous-module de V. Exemple (en prenant $A = \mathbf{Z}$) : tout groupe commutatif sans torsion se plonge dans un espace vectoriel rationnel.

*e*) On suppose M sans torsion et de type fini. Montrer que V est de dimension finie sur K. Soit $n = \dim(V)$ (on dit que $n$ est le **rang de M**); montrer qu'il existe deux bases $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_i)_{1 \leqslant i \leqslant n}$ de V telles que, si l'on désigne par P et Q les sous-A-modules (isomorphes à $A^n$) de V engendrés par les $a_i$ et $b_i$ respectivement, on ait $P \subset M \subset Q$.



*f*) Déduire de là et du Théorème 3 du § 18 le résultat suivant : *si* A *est un anneau principal, tout* A*-module* M *sans torsion et de type fini est isomorphe à* $A^n$ *où* $n$ *est le rang de* M. Traduction lorsque $A = \mathbf{Z}$?

*g*) Soit M un module de type fini sur un anneau principal A. Soit T le sous-module de torsion de M. Montrer que M/T est libre de type fini. En déduire (à l'aide de l'*Exercice* 8 du § 17) que M est isomorphe au produit direct de T et d'un A-module libre de type fini. (Ce résultat ramène l'étude des modules de type fini à celle des modules *de torsion* de type fini, qui sera faite au § 31, *Exercices* 8, 9, 10.)

*h*) Soient M un module libre de type fini sur un anneau principal A et M′ un sous-module de M. Montrer que les propriétés suivantes sont équivalentes : *i*) M′ est facteur direct dans M *ii*) le module quotient M/M′ est sans torsion *iii*) quels que soient $a \in A$ et $x \in M$, la relation $ax \in M'$ implique $a = 0$ ou $x \in M'$. Retrouver à partir de là le résultat du § 18, *Exercice* 2.

*i*) Soit M′ un sous-groupe de $\mathbf{Z}^n$ défini par un système d'équations linéaires et homogènes à coefficients entiers. Montrer que toute base de M′ fait partie d'une base de $\mathbf{Z}^n$.

**12.** On trouve, dans un manuel d'Algèbre destiné aux élèves des Lycées et Collèges, la phrase suivante : « Sous réserve de ne pas donner aux variables des valeurs qui annulent le numérateur ou le dénominateur, l'ensemble des fractions rationnelles muni des lois d'addition et de multiplication présente une structure de corps. » Que pensez-vous de cet énoncé?

# § 30

**1.** Soit K un corps commutatif de caractéristique 0 (par exemple $K = \mathbf{C}$). Montrer que l'équation

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1 = 0$$

n'a aucune racine multiple dans K.

**2.** Soit K un corps commutatif. Trouver un polynôme $f \in K[X]$ de degré 7 tel que 1 soit racine multiple d'ordre 4 au moins de $f(X) + 1$, et $-1$ racine multiple d'ordre 4 au moins de $f(X) - 1$. Généraliser en remplaçant les entiers 4 et 7 par $n$ et $2n - 1$.

**3.** Chacun des polynômes suivants admet 1 pour racine; déterminer son ordre de multiplicité :

$$X^{2n} - nX^{n+1} + nX^{n-1} - 1; \qquad X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1;$$
$$X^{2n} - n^2X^{n+1} + 2(n^2-1)X^n - n^2X^{n-1} + 1.$$

**4.** Soit $f$ un polynôme à une variable à coefficients dans un corps commutatif K. On suppose $f' = 0$. Montrer que $f$ est constant si K est de caractéristique 0, et que $f$ est un polynôme en $X^p$ si K est de caractéristique $p \neq 0$. Réciproque?

¶ **5.** Soit K un corps commutatif de caractéristique 0. On se propose de trouver toutes les applications

$$t \mapsto U(t)$$

de K dans l'anneau $M_n(K)$ qui vérifient

$$U(x+y) = U(x)U(y) \quad \text{quels que soient } x, y \in K,$$
$$U(0) = 1_n$$

et qui sont de plus polynomiales, i.e. de la forme

$$U(t) = A_0 + A_1 t + \cdots + A_r t^r + \cdots$$

où les matrices $A_r \in M_n(K)$ sont presque toutes nulles.

*a*) Montrer que la dérivée $U'(t)$ de la fonction polynomiale $U(t)$ vérifie

$$U'(t) = A_1 . U(t).$$



*b*) Montrer que la matrice $A_1 = N$ est nilpotente et que

$$U(t) = \sum_{r \geq 0} N^r \frac{t^r}{r!} = \exp(tN)$$

(cf. § 8, *Exercice* 2).

*c*) Montrer inversement que, pour toute matrice nilpotente N, l'application

$$t \mapsto \exp(tN)$$

satisfait aux conditions requises.

*d*) Trouver la matrice N dans le cas de la fonction $U(t)$ du § 12, *Exercice* 11, et *vérifier* dans ce cas qu'on a bien $U(t) = \exp(tN)$.

**6.** Soit K un corps commutatif de caractéristique 0. Montrer qu'il n'existe aucun polynôme $f \in K[X]$ non nul tel que l'on ait

$$f(x+y) = f(x)f(y)$$

quels que soient $x, y \in K$. Même question pour la relation

$$f(xy) = f(x) + f(y).$$

Quels sont les polynômes tels que

$$f(x+y) = f(x) + f(y)?$$

¶ **7.** Soit K un corps de caractéristique $p \neq 0$.

*a*) Montrer qu'on a

$$(x+y)^p = x^p + y^p$$

quels que soient $x, y \in K$. En déduire plus généralement que

$$(x+y)^q = x^q + y^q$$

si $q$ est une puissance de $p$.

*b*) Montrer que l'application $x \to x^p$ est un isomorphisme de K sur un sous-corps de K (que l'on note $K^p$). Montrer que $K^p = K$ si K est fini.

*c*) Quels sont les polynômes $f \in K[X]$ vérifiant

$$f(x+y) = f(x) + f(y)$$

quels que soient $x, y \in K$?

¶ **8.** Soit K un corps de caractéristique $p \neq 0$. Montrer que, pour $n \in \mathbf{Z}$ et $x \in K$, l'élément $nx \in K$ ne dépend que de $x$ et de la classe de $n$ modulo $p$. En déduire qu'on peut considérer K comme un espace vectoriel sur le corps $\mathbf{Z}/p\mathbf{Z}$.
Montrer que *le nombre d'éléments d'un corps fini de caractéristique p est une puissance de p.*

**9.** Soit $p$ un nombre premier. Montrer que le coefficient binômial $\binom{p^n}{r}$ est divisible par $p$ pour tout $n \geq 1$ et tout $r$ tel que $1 \leq r \leq p^n - 1$. (Utiliser l'*Exercice* 7 pour le corps $K = \mathbf{Z}/p\mathbf{Z}$.) Démonstration élémentaire?

**10.** Soit $f(X_1, \ldots, X_n)$ un polynôme à $n$ variables à coefficients dans un anneau commutatif K. On suppose $f$ homogène de degré $r$. Montrer que

$$X_1 f'_1(X_1, \ldots, X_n) + \ldots + X_n f'_n(X_1, \ldots, X_n) = r.f(X_1, \ldots, X_n)$$

où $f'_i$ est la dérivée partielle de $f$ par rapport à $X_i$. Cette relation (connue sous le nom d'identité d'Euler) caractérise-t-elle les polynômes homogènes de degré $r$?

**11.** Soit

$$(*) \qquad a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

une équation algébrique à coefficients $a_i$ entiers rationnels; on suppose dans ce qui suit les $a_i$ premiers entre eux (cas auquel on peut évidemment toujours se ramener en divisant les $a_i$ par leur pgcd).
Soit $x = p/q$ une racine rationnelle de l'équation $(*)$; on suppose $p$ et $q$ premiers entre eux. Montrer que $p$ divise $a_0$ et que $q$ divise $a_n$.
Application : trouver les racines rationnelles des équations suivantes :

$$6x^4 - 11x^3 - x^2 - 4 = 0$$
$$2x^3 + 12x^2 + 13x + 15 = 0$$
$$6x^5 + 11x^4 - x^3 + 5x - 6 = 0$$
$$x^6 + 3x^5 + 4x^4 + 3x^3 - 15x^2 - 16x + 20 = 0$$
$$2x^6 + x^5 - 9x^4 - 6x^3 - 5x^2 - 7x + 6 = 0.$$

**12.** Soit K un anneau commutatif. On considère l'anneau $L = K[\varepsilon]$ engendré par K et un élément $\varepsilon$ tel que

$$\varepsilon^2 = 0$$

(faire $n = 1$ dans l'*Exercice* 23 du § 28). Pour que l'application

$$x \mapsto x + D(x)\varepsilon$$

de K dans L soit un homomorphisme, il faut et il suffit que D doit une dérivation de l'anneau K.

**13.** Dans quels corps a-t-on l'identité

$$x^4 - x^2 + 1 = (x^2 - 5x + 1)(x^2 + 5x + 1)?$$

**14.** Soit K un corps de caractéristique $p \neq 0$. Si un $x \in K$ vérifie $x^n = 1$ pour un entier $n$, il existe un entier $r$ *non divisible par* $p$ tel que

$$x^r = 1.$$

**15.** Soit K un anneau commutatif. On définit (par récurrence sur l'entier $n \geqslant 0$) les **opérateurs différentiels d'ordre $n$ au plus sur** K comme suit : ce sont des applications D de K dans K, vérifiant

$$D(x + y) = D(x) + D(y) \quad \text{quels que soient } x, y \in K,$$

et possédant en outre la propriété suivante : si $n = 0$, il existe un $a \in K$ tel que

$$D(x) = ax \quad \text{pour tout } x \in K;$$



si $n \geqslant 1$, il existe, pour tout $x \in K$, un opérateur différentiel $D_x$ d'ordre $n - 1$ au plus sur K tel que l'on ait

$$D(xy) = x.D(y) + D_x(y) \quad \text{pour tout } y \in K.$$

*a*) Déterminer tous les opérateurs différentiels d'ordre 1 au plus sur K.
*b*) Montrer que si D′ et D″ sont des opérateurs différentiels d'ordres $r$ et $s$ au plus, l'application composée

$$D'' \circ D'$$

est un opérateur différentiel d'ordre $r + s$ au plus, et le crochet de Jacobi

$$D'' \circ D' - D' \circ D''$$

un opérateur différentiel d'ordre $r + s - 1$ au plus.
*c*) Soit D un opérateur différentiel d'ordre $n$ au plus. On considère une famille $(x_i)_{i \in I}$ d'éléments de K, avec Card (I) $= n + 1$. Pour toute partie F de I, on pose

$$x_F = \prod_{i \in F} x_i \quad \text{et } x_\varnothing = 1.$$

Montrer qu'on a l'identité

$$\sum_{F \subset I} (-1)^{\mathrm{Card}(F)} x_F \, D(x_{I-F}) = 0.$$

Montrer réciproquement que toute application D de K dans K, possédant cette propriété et telle que $D(x + y) = D(x) + D(y)$, est un opérateur différentiel d'ordre $n$ au plus dans K.
*d*) Déduire de là une formule pour calculer les dérivées partielles d'ordre $p$ d'un produit de $n + 1$ polynômes, par récurrence sur $n$. Cas $p = 1$?
*e*) On prend

$$K = k[X_1, \ldots, X_n]$$

où $k$ est un anneau commutatif. Construire tous les opérateurs différentiels dans K qui sont nuls sur $k$.