Université Pierre et Marie Curie 2004-2005

Master de Sciences et Technologies
Mention : Mathématiques

M1 Algèbre commutative et théorie de Galois

Patrick Polo

Version du 14 octobre 2004

Introduction

Ce cours est constitué de deux parties. La première constitue une introduction à l'algèbre commutative. On y introduira les notions de base concernant les anneaux, les idéaux, la construction des anneaux quotients et des anneaux de fractions, les modules, le produit tensoriel, les anneaux et modules noethériens, les anneaux factoriels, les théorèmes de transfert, pour la noethérianité et la factorialité, aux anneaux de polynômes, et enfin les modules de type fini sur un anneau principal.

La deuxième partie constituera une introduction à la théorie de Galois. On y étudiera les extensions finies de corps, les notions d'extensions normales, séparables, de groupe de Galois, la construction des corps finis, et la théorie de Galois proprement dite, c'est-à-dire, la correspondance entre sous-groupes du groupe de Galois d'une extension galoisienne, et corps intermédiaires. On essaiera de présenter une application (parmi de nombreuses possibles), de cette théorie, par exemple le théorème d'Artin et Schreier décrivant les corps qui admettent une extension finie qui soit algébriquement close.

Des références bibliographiques possibles sont les suivantes. Si l'on souhaite se limiter aux ouvrages en langue française, on pourra consulter, par exemple, pour la 1ère partie du cours,

J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

P. Samuel, Théorie algébrique des nombres, Hermann, 1967,

et, pour la 2ème partie,

J.P. Escofier, Théorie de Galois, Dunod, 2000.

Si l'on peut lire des livres en anglais, on pourra consulter aussi, par exemple,

M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

S. Lang, Algebra, Addison-Wesley, 1965.

D'autres références, spécifiques à certaines parties du cours, sont données dans la bibliographie (provisoire) qui suit.

Table des matières

Bibliographie

[] Voici une bibliographie provisoire (elle aussi en évolution au fil du texte).

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[Bla] A. Blanchard, Les corps non commutatifs, P.U.F., 1972.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, tome 1/Algèbre, Cedic Fernand Nathan, 1977.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[Kri] J.-L. Krivine, Théorie des ensembles, Cassini, 1998.

[Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.

[La] S. Lang, Algebra, Addison-Wesley, 1965.

[Laf] J.-P. Lafon, Les formalismes fondamentaux de l'algèbre commutative, Hermann, 1974.

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[SD] H.P.F. Swinnerton-Dyer, A brief guide to algebraic number theory, C.U.P., 2001.

Chapitre 1

Anneaux, idéaux, localisation

Version du 14 octobre 2004

1.1 Anneaux et corps

On rappelle qu'un anneau A est un ensemble non vide muni de deux lois, $+$ et $\cdot$, telles que :

1) $(A, +)$ est un groupe abélien, c.-à-d., $+$ est associative et commutative, A possède un élément 0 tel que $0 + a = a$ pour tout a, et tout a admet un opposé noté $-a$, tel que $a + (-a) = 0$;

2) la loi $\cdot$ est associative et A admet un élément neutre 1 tel que $1 \cdot a = a = a \cdot 1$, pour tout a ;

3) la loi $\cdot$ est distributive (à gauche et à droite) sur l'addition, c.-à-d., pour tout $a, b, c \in A$:

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca.$$

(Ici, comme c'est l'usage, on a omis le signe $\cdot$ et écrit ab au lieu de $a \cdot b$, etc...).

On dit que l'anneau A est commutatif si, de plus, la loi $\cdot$ est commutative.

Rappelons aussi qu'il résulte de 1) et 3) que

$$a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0),$$

de sorte que $a \cdot 0 = 0$, et de même $0 \cdot a = 0$, pour tout a.

Remarque On n'exclut pas la possibilité que $1 = 0$. Si c'est le cas, alors $a = a \cdot 1 = a \cdot 0 = 0$ pour tout a, et donc A se réduit au singleton $\{0\}$,

appelé l'anneau nul. Ce cas ne présente aucun intérêt et pourrait être exclu en ajoutant la condition $1 \neq 0$; toutefois, une raison de s'autoriser l'anneau nul est de ne pas avoir à exclure le cas $I = A$ lorsqu'on définira l'anneau quotient A/I pour un idéal I de A (voir plus loin).

Définition 1.1.1 *On dit qu'un élément $a \in A \setminus \{0\}$ est inversible s'il existe $a' \in A$ tel que $aa' = a'a = 1$. Un tel a', s'il existe, est nécessairement unique et est alors noté a^{-1} ou $1/a$. On note $A^\times$ l'ensemble des éléments inversibles de A.*

Exercice 1.1.1 On suppose $A \neq 0$. Montrer que $A^\times$ est un groupe.

Définition 1.1.2 *Un corps est un anneau commutatif $k \neq 0$ tel que l'ensemble $k \setminus \{0\}$ forme un groupe pour la multiplication, c.-à-d., tel que $k^\times = k \setminus \{0\}$.*

Définition 1.1.3 *Soit $D \neq 0$ un anneau non-commutatif. Si tout élément non-nul de D est inversible, on dit que D est un corps non-commutatif, ou corps gauche, ou encore une algèbre à division (en anglais : non-commutative field, skew field, ou division algebra). C.-à-d., l'usage est de réserver le mot corps au cas d'un corps commutatif (field en anglais).*

Définition 1.1.4 *On dit que l'anneau A est intègre (en anglais : A is a domain, or integral domain) s'il est non nul et vérifie : $a, b \in A \setminus \{0\} \Rightarrow ab \neq 0$.*

Exercice 1.1.2 Tout corps est un anneau intègre. Réciproquement, soit A un anneau commutatif intègre. On suppose que A est un ensemble fini, ou bien que A est une k-algèbre de dimension finie (où k est un corps). Montrer, dans chaque cas, que A est un corps.

Définition 1.1.5 *Un morphisme d'anneaux est une application f d'un anneau A vers un anneau B qui respecte l'addition, la multiplication et l'élément unité, c.-à-d., tel que $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ et $f(1_A) = 1_B$.*

Un sous-anneau de B est un sous-groupe A de B qui est stable par multiplication et contient l'élément unité 1_B ; dans ce cas, l'inclusion $A \subseteq B$ est un morphisme d'anneaux. Réciproquement, si $f : A \to B$ est un morphisme injectif, alors on peut identifier A à son image $f(A)$, qui est un sous-anneau de B.

Remarque La condition $f(a+b) = f(a) + f(b)$ entraîne $f(0) = f(0)$ (car dans le groupe $(A, +)$ on peut simplifier par $f(0)$) et $f(-a) = -f(a)$. Par contre, la condition $f(ab) = f(a)f(b)$ n'entraîne pas la 3ème : si on pose $f(a) = 0$ pour tout a, les conditions 1) et 2) sont vérifiées mais la 3ème ne l'est pas si $B \neq \{0\}$.

Définition 1.1.6 *Suivant les règles générales, on dit qu'un morphisme d'anneaux $f : A \to B$ est un isomorphisme s'il existe un morphisme $g : B \to A$ tel que $gf = \mathrm{id}_A$ et $fg = \mathrm{id}_B$. Plus simplement, ceci équivaut à dire que l'application f est bijective, car on vérifie facilement que la bijection inverse $g : B \to A$ est alors un morphisme d'anneaux (le vérifier !).*

Convention Dans ce cours, tous les anneaux considérés seront supposés commutatifs, sauf peut-être dans un paragraphe consacré au produit tensoriel. On convient donc que dans la suite le mot anneau signifie anneau commutatif, sauf mention explicite du contraire.

1.2 Idéaux, idéaux premiers et maximaux

Soit A un anneau. Comme convenu plus haut, A est supposé commutatif. On rappelle qu'un idéal I de A est un sous-ensemble qui est un sous-groupe pour l'addition (c.-à-d., $0 \in I$ et $x, y \in I \Rightarrow x - y \in I$) et qui est stable par multiplication par tout élément de A, c.-à-d. :

$$\forall x \in I,\ \forall a \in A, \qquad ax \in I.$$

Deux exemples immédiats sont : l'idéal nul, noté (0), et l'anneau A tout entier, qu'on désignera parfois par (1), voir ci-dessous. Voici d'autres exemples.

Exemples 1.2.1 1) Soit $A = \mathbb{Z}$, et k un entier. On note $(k) = \{nk \mid n \in \mathbb{Z}\}$. C'est un idéal de $\mathbb{Z}$.

2) Soient $A = \mathbb{C}[X]$ et $\lambda \in \mathbb{C}$. On pose

$$(*) \qquad (X - \lambda) = \{P \in \mathbb{C}[X] \mid P(\lambda) = 0\}.$$

C'est un idéal de $\mathbb{C}[X]$.

Il résulte de la définition qu'une intersection arbitraire d'idéaux de A est un idéal de A. Ceci fournit le premier point de la proposition suivante.

Proposition 1.2.1 *Soit S une partie non-vide de A. Alors l'intersection de tous les idéaux de A contenant S est le plus petit idéal de A contenant S. On l'appelle* **l'idéal engendré par** *S et on le note (S). De plus, cet idéal (S) est égal à l'ensemble des sommes finies de la forme*

$$\sum_{i=1}^{n} a_i x_i, \quad \text{où } n \geq 1, x_i \in S, a_i \in A.$$

Démonstration. On a déjà vu la 1ère assertion, voyons la 2ème. Notons I l'ensemble des sommes ci-dessus. Il est clair que I est un sous-groupe de A, et aussi qu'il est stable par multiplication par tout $a \in A$. C'est donc un idéal de A, qui contient S. Réciproquement, tout idéal de A contenant S contient toutes les sommes ci-dessus, donc contient I. Ceci prouve que I est l'idéal engendré par S. □

Pour $S = \{0\}$, (0) est l'idéal nul, et pour $S = \{1\}$ on a $(1) = A$. Ceci justifie les notations introduites plus haut.

Exercice 1.2.1 Dans l'exemple 2) plus haut, montrer que l'idéal défini par le terme de droite de $(*)$ est bien égal à l'idéal engendré par le polynôme $X - \lambda$. (Utiliser la division euclidienne.)

Définition 1.2.1 *Soient I, J des idéaux de A. On désigne par $I + J$ l'idéal engendré par $I \cup J$ et par IJ l'idéal engendré par les produits xy, pour $x \in I$ et $y \in J$. Il résulte de la proposition ci-dessus que $I + J$ est l'ensemble des éléments $x + y$, avec $x \in I$ et $y \in J$, et que IJ est l'ensemble de toutes les sommes finies*

$$\sum_{i=1}^{n} x_i y_i,$$

pour $n \geq 1$, $x_i \in I$, $y_i \in J$.

Définition 1.2.2 *Soit I un idéal de A. On dit que I est <u>premier</u> si $I \neq A$ et si $ab \in I \Rightarrow a \in I$ ou $b \in I$. On dit que I est <u>maximal</u> si $I \neq A$ et s'il n'existe pas d'idéal $J \neq A$ contenant strictement I.*

On notera que, par définition, l'idéal A n'est ni maximal ni premier.

Exercice 1.2.2 Montrer que tout idéal maximal est premier.

Remarque (culturelle). Les idéaux premiers d'un anneau A jouent un rôle extrêmement important. En arithmétique, si A est un anneau de nombres, ses idéaux premiers généralisent la notion usuelle de nombre premier dans $\mathbb{Z}$. En

géométrie algébrique, disons sur $\mathbb{C}$, si I est un idéal de l'anneau $\mathbb{C}[X_1, \ldots, X_n]$ et si $V(I)$ désigne la variété des zéros de I, c.-à-d.,

$$V(I) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f(x_1, \ldots, x_n) = 0, \forall f \in I\},$$

les idéaux premiers de $A = \mathbb{C}[X_1, \ldots, X_n]/I$ correspondent aux sous-variétés irréductibles de $V(I)$. Les lecteurs intéressés pourront consulter, par exemple, [SD] pour le 1er aspect, et [Die] ou [Pe2] pour le second.

De façon plus immédiate, un intérêt des idéaux premiers est que l'anneau quotient associé (voir ci-dessous) est intègre.

1.3 Anneaux quotients

On rappelle que si A est un groupe abélien et H un sous-groupe de A, on peut former le groupe quotient A/H : ses éléments sont les classes d'équivalence pour la relation

$$a \sim b \Leftrightarrow a - b \in H.$$

La classe d'un élément a est désignée par $a + H$ et l'addition est définie par

$$(a + H) + (b + H) = a + b + H.$$

Bien sûr, il faut vérifier que la formule ci-dessus a bien un sens, c.-à-d., que si a' (resp. b') est un autre représentant de la classe $a + H$ (resp. $b + H$) alors la classe de $a' + b'$ est la même que celle de $a + b$. C'est bien le cas, car si $a' = a + h$ et $b' = b + h'$, alors

$$a' + b' = a + h + b + h' = a + b + h + h'.$$

On notera que le fait que $(A, +)$ soit abélien joue un rôle essentiel. L'application de A dans A/H qui à tout $a \in A$ associe sa classe dans A/H s'appelle la projection canonique de A sur A/H ; c'est un morphisme de groupes abéliens.

Proposition 1.3.1 1) *Soit A un anneau commutatif et I un idéal de A. Alors la multiplication de A induit une structure d'anneau sur A/I. De façon plus précise, il existe sur A/I une unique structure d'anneau telle que la projection canonique $\pi : A \to A/I$ soit un morphisme d'anneaux.*

2) *De plus, pour tout idéal K de A/I, son image inverse $\pi^{-1}(K) = \{a \in A \mid \pi(a) \in K\}$ est un idéal de A, et l'application $K \mapsto \pi^{-1}(K)$ est une bijection de l'ensemble des idéaux de A/I sur l'ensemble des idéaux J de A contenant I ; la bijection réciproque est $J \mapsto J/I$.*

Démonstration. Pour que π soit un morphisme d'anneaux, la multiplication dans A/I doit nécessairement être définie par la formule

$$(a+I)(b+I) = ab+I, \tag{1}$$

pour tout $a, b \in A$. Pour vérifier que cette formule fait sens, il faut, à nouveau, vérifier que si a' (resp. b') est un autre représentant de la classe de $a+I$ (resp. $b+I$), alors la classe de $a'b'$ est la même que celle de ab. C'est bien le cas car si $a' = a+h$ et $b' = b+h'$, avec $h, h' \in I$, alors

$$a'b' = (a+h)(b+h') = ab+ah'+hb+hh', \tag{2}$$

et chacun des trois produits ah', $hb = bh$, et hh' appartient à I. Ceci montre que la formule (1) a bien un sens (c.-à-d., le terme de droite est bien défini). On vérifie alors aussitôt, en utilisant cette formule, que la multiplication est associative, commutative et distributive sur l'addition, que la classe $1+I$ est l'élément unité, et que π est un morphisme d'anneaux. Ceci prouve la 1ère partie de la proposition. La 2ème est laissée au lecteur. □

Il ne faut pas être rebuté par l'aspect formel de cette définition. Dans la pratique, on ne pense jamais à A/I comme à un ensemble de classes d'équivalence ; on voit plutôt les éléments de A/I comme "des éléments de A", avec lesquels on calcule "modulo I". L'exemple de base est celui des anneaux $\mathbb{Z}/n\mathbb{Z}$.

De plus, cette façon de "négliger" (c.-à-d., de rendre nuls) les éléments de I permet dans bien des cas de travailler avec un anneau A/I plus simple que A , et d'en déduire des résultats pour A lui même. Un exemple frappant est le théorème de l'invariance du rang d'un A-module libre de type fini (voir plus loin).

On peut aussi obtenir des résultats négatifs sur A, c.-à-d., montrer que A n'a pas telle ou telle propriété, en montrant que cette propriété entraîne une contradiction facile à détecter dans un certain anneau quotient de A. Le lecteur intéressé pourra étudier, par exemple, [Pe1, Chap.II, §5], où des arguments de ce type sont utilisés pour montrer que les anneaux $\mathbb{Z}[(1+i\sqrt{19})/2]$ et $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ ne sont pas euclidiens, bien que principaux (voir plus loin pour la définition et l'étude de ces anneaux).

Les anneaux quotients apparaissent aussi de façon naturelle chaque fois que l'on a un morphisme d'anneaux :

Théorème 1.3.2 [Théorème fondamental d'isomorphisme (pour les anneaux commutatifs)]

Soit $f : A \to B$ un morphisme d'anneaux commutatifs, soit $C = f(A)$ l'image de A (c.-à-d., $C = \{f(a) \mid a \in A\}$), et soit

$$\ker f = f^{-1}(0) = \{a \in A \mid f(a) = 0\}.$$

le noyau de f. Alors C est un sous-anneau de B, $\ker f$ est un idéal de A, et f induit un isomorphisme d'anneaux

$$\bar{f} : A/\ker f \cong C.$$

Démonstration. Il est clair que C est un sous-anneau de B et que $\ker f$ est un sous-groupe de $(A, +)$. C'est aussi un idéal, car si $x \in \ker f$ et $a \in A$, on a $f(ax) = f(a)f(x) = 0$. Ici, on suppose connu du lecteur qu'un morphisme $f : A \to B$ de groupes abéliens induit un isomorphisme de groupes abéliens

$$\bar{f} : A/\ker f \cong \mathrm{Im}(f);$$

ceci sera redémontré dans la section 2 consacrée aux modules.

Ceci étant, on voit facilement que $\bar{f}$ est un morphisme d'anneaux : avec des notations évidentes, on a

$$\bar{f}(\bar{a}\bar{b}) = \bar{f}(\bar{ab}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a})\bar{f}(\bar{b}).$$

Comme $\bar{f}$ est bijectif, c'est bien un isomorphisme d'anneaux de $A/\ker f$ sur C. □

À titre d'exemple, et pour se familiariser avec la notion d'anneau quotient, on pourra faire les exercices suivants.

Exercices 1.3.1 1) Soit $A = \mathbb{C}[X, Y]$ et soit $B = \mathbb{C}[t^2, t^3]$ le sous-anneau de $\mathbb{C}[t]$ engendré par t^2 et t^3. Montrer que les monômes 1 et t^i pour $i \geq 2$ forment une base de B comme $\mathbb{C}$-espace vectoriel. On considère le morphisme d'anneaux $f : A \to B$ défini par $f(X) = t^2$ et $f(Y) = t^3$. Soit I l'idéal de A engendré par $Y^2 - X^3$. On note x et y les images de X et Y dans A/I. Montrer que $I \subseteq \ker f$ et que tout élément de A/I s'écrit sous la forme $P(x) + yQ(x)$, avec $P, Q \in \mathbb{C}[X]$. En considérant leurs images dans B, montrer que les éléments x^p et yx^q, pour $p, q \geq 0$, forment une base de A/I comme $\mathbb{C}$-espace vectoriel. En déduire que $\ker f = I$ et que

$$A/I = \mathbb{C}[X, Y]/(Y^2 - X^3) \cong B.$$

2) Soient $A = \mathbb{C}[U, V, Z]$ et $B = \mathbb{C}[X, Y]$ et soit $f : A \to B$ le morphisme défini par $f(U) = X^2$, $f(V) = Y^2$ et $f(Z) = XY$. Soit I l'idéal de A engendré par $UV - Z^2$. Montrer que $I = \ker f$ et que A/I est isomorphe au sous-anneau de B engendré par X^2, Y^2 et XY.

1.3.1 Anneaux non-commutatifs et idéaux bilatères

Définition 1.3.1 *Soit R un anneau non-commutatif. Dans ce cas, on distingue les trois notions suivantes. Soit I un sous-groupe de $(R,+)$. On dit que I est un idéal à gauche (resp. à droite) si, pour tout $a \in A$, l'on a $aI \subseteq I$, (resp. $Ia \subseteq I$), et l'on dit que I est un idéal bilatère si c'est à la fois un idéal à gauche et à droite.*

Revenant à la démonstration de la Proposition 1.3.1, on voit, en considérant la formule (2), que si I est un idéal bilatère alors la formule (1) définit une structure d'anneau sur R/I. C.-à-d., on obtient la

Proposition 1.3.3 *Soit A un anneau et I un idéal bilatère. Alors, il existe une unique structure d'anneau sur A/I telle que la projection $\pi : A \to A/I$ soit un morphisme d'anneau. La multiplication dans A/I est définie par la formule*

$$(a+I)(b+I) = ab + I.$$

De même, on obtient le

Théorème 1.3.4 [Théorème fondamental d'isomorphisme (pour les anneaux)]

Soit $f : R \to S$ un morphisme d'anneaux. Alors $f(R)$ est un sous-anneau de S, $\ker f$ *est un idéal bilatère de R, et f induit un isomorphisme d'anneaux* $R/\ker f \cong f(R)$.

Revenant au cas d'un anneau commutatif, on a la proposition suivante.

Proposition 1.3.5 *Soit A un anneau commutatif, I un idéal de A. Alors :*
a) *I est premier ssi A/I est intègre.*
b) *I est maximal ssi A/I est un corps.*
En particulier, tout idéal maximal est premier.

Démonstration. a) est facile et laissé au lecteur. Démontrons b). Supposons que A/I soit un corps et soit $x \in A \setminus I$. Alors, l'image $\bar{x}$ de x dans A/I est $\neq 0$, donc inversible, donc il existe $a \in A$ tel que $\bar{a}\bar{x} = 1$. Ceci signifie que $ax - 1 \in I$. Alors

$$1 = ax + (1 - ax) \in Ax + I$$

et donc $I + Ax = A$, pour tout $x \notin I$. Ceci prouve que I est maximal.

Réciproquement, supposons que I soit maximal et soit $x \notin I$. Alors l'idéal $Ax + I$ égale A, donc il existe $a \in A$ et $y \in I$ tels que $ax + y = 1$. Alors, dans A/I on a $\bar{a}\bar{x} = 1$ et ceci prouve que $\bar{x}$ est inversible. Comme x est arbitraire dans $A \setminus I$ ceci prouve que A/I est un corps. □

Remarque 1.3.1 Soient R un anneau non-commutatif et I un idéal bilatère. Si A/I est un corps gauche, la 1ère partie de la démonstration ci-dessus montre que I est maximal comme idéal à gauche (et, de même, aussi comme idéal à droite), donc a fortiori comme idéal bilatère. Mais la réciproque est en défaut : si I est maximal comme idéal bilatère, A/I n'est pas nécessairement un corps. Par exemple, si $A = M_n(\mathbb{C})$, on peut montrer que (0) est un idéal bilatère maximal (c.-à-d., que A n'a aucun idéal bilatère autre que (0) et A), et pourtant A n'est pas un corps si $n \geq 2$.

1.4 Anneaux de fractions, localisation

Dans cette section, A est un anneau commutatif.

1.4.1 Le cas intègre

Pour commencer, supposons A intègre. Rappelons, ou expliquons, la construction du corps des fractions de A. On considère l'ensemble C des couples (a, s), où $a \in A$ et $s \in A \setminus \{0\}$. De façon informelle, on pense au couple (a, s) comme à un représentant de la fraction a/s. Tenant compte de l'égalité $a/s = b/t$ si $at = bs$, on considère sur C la relation définie par

$$(a, s) \sim (b, t) \Leftrightarrow at = bs.$$

Cette relation est clairement réflexive et symétrique ; elle est aussi transitive car si $(a, s) \sim (b, t) \sim (c, u)$, alors $at = bs$ et $bu = ct$ d'où $atu = bsu = cts$, soit

$$(au - cs)t = 0, \tag{3}$$

et comme A est intègre et $t \neq 0$, il vient $au = cs$, soit $(a, s) \sim (c, u)$. On note K l'ensemble quotient, c.-à-d., l'ensemble des classes d'équivalence, et pour tout $(a, s) \in C$ on désigne par $[a, s]$ son image dans K. On va définir sur K une structure d'anneau, déduite des lois d'addition et de multiplication des fractions :

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

C-à-d., guidés par les formules ci-dessus, on pose

$$[a,s]+[b,t]=[at+bs,st], \qquad [a,s][b,t]=[ab,st].$$

On vérifie facilement que ceci définit sur K une structure d'anneau, dont le 0 est $[0,1]$ et l'élément unité $[1,1]$. De plus, un élément $[a,s]$ est non-nul ssi $a\neq 0$; dans ce cas on a

$$[a,s][s,a]=[as,as]=1,$$

et donc $[a,s]$ est inversible. Ceci prouve que K est un corps. Enfin, l'application $a\mapsto[a,1]$ est un morphisme d'anneaux de A dans K, et ce morphisme est injectif car si $[a,1]=0$ alors $a=0$. On peut donc identifier A au sous-anneau de K formé des éléments $[a,1]$, pour $a\in A$. Pour $b\neq 0$, $[1,b]$ est l'inverse de $[b,1]$. Par conséquent, si on identifie chaque élément a de A avec son image $[a,1]$ dans K, on obtient que tout élément $[a,b]$ de K (où $b\neq 0$, est égal à la fraction $ab^{-1}=a/b$. Ceci prouve que K est "le" corps des fractions de A. Pour le moment, les guillemets sont nécessaires car il n'est pas tout-à-fait évident que K soit uniquement déterminé par les propriétés ci-dessus. En fait, c'est bien le cas, car K vérifie la propriété universelle ci-dessous. Notons τ le morphisme $A\to K$, $a\mapsto[a,1]$.

Proposition 1.4.1 *Le corps K vérifie la propriété universelle suivante : pour tout morphisme d'anneaux $\phi:A\to B$ tel que $\phi(a)$ soit inversible pour tout $a\neq 0$, il existe un* **unique** *morphisme $\Phi:K\to B$ tel que $\Phi\circ\tau=\phi$.*

Démonstration. Si Φ existe, on a nécessairement, pour tout $a\in A$, $\Phi(\tau(a))=\phi(a)$. Alors, pour $s\neq 0$, l'égalité

$$1=\Phi(1)=\Phi(\tau(s)\tau(s)^{-1})=\phi(s)\Phi(\tau(s)^{-1})$$

entraîne $\Phi(\tau(s)^{-1})=\phi(s)^{-1}$. Enfin, comme $[a,s]=\tau(a)\tau(s)^{-1}$, nécessairement Φ doit vérifier

$$\Phi([a,s])=\phi(a)\phi(s)^{-1}. \tag{1}$$

Ceci montre que Φ, s'il existe, est nécessairement unique. Il reste à vérifier que la formule (1) définit Φ sans ambiguités. Or, si $[a,s]=[b,t]$, on a $at=bs$ d'où

$$\phi(a)\phi(t)=\phi(at)=\phi(bs)=\phi(b)\phi(s).$$

Comme $\phi(s)$ et $\phi(t)$ sont inversibles, on en déduit $\phi(a)\phi(s)^{-1}=\phi(b)\phi(t)^{-1}$. Ceci montre que Φ est bien définie, et la proposition est démontrée. □

Un corollaire standard de ce type de propriété universelle est que K est unique à isomorphisme unique près. C.-à-d., on a le corollaire suivant.

Corollaire 1.4.2 *Soit $\tau' : A \to K'$ un autre morphisme d'anneaux tel que $\tau'(s)$ soit inversible pour tout $s \neq 0$ et vérifiant la propriété universelle ci-dessus. Alors il existe un unique morphisme $\Phi : K \to K'$ tel que $\Phi \circ \tau = \tau'$, et c'est un isomorphisme. En particulier, K' est un corps isomorphe à K.*

Démonstration. Par la propriété universelle de K (resp. K') il existe un unique morphisme $\Phi : K \to K'$ tel que $\Phi \circ \tau = \tau'$. De même, par la propriété universelle de K' il existe un unique morphisme $\Psi : K' \to K$ tel que $\Psi \circ \tau' = \tau$.

Alors, $\Psi \circ \Phi \circ \tau = \Psi \circ \tau' = \tau$, donc, par la propriété universelle de K, appliquée à $B' = K$ et $\tau' = \tau$, on obtient que $\Psi \circ \Phi = \mathrm{id}_K$. On obtient de même que $\Phi \circ \Psi = \mathrm{id}_{K'}$. Ceci prouve le corollaire. □

Remarque 1.4.1 1) Cet argument montre qu'un problème universel du type ci-dessus a au plus une solution (à isomorphisme unique près). Mais il ne dit rien quant à l'existence d'une solution. Il faut donc bien construire K comme on l'a fait plus haut.

2) On prendra garde au fait que dans la propriété universelle, l'hypothèse qu'il existe un **unique** Φ joue un rôle essentiel : on l'a vu dans la démonstration du corollaire. On peut aussi remarquer que le morphisme $A \to K \to K[X]$, vérifie la propriété universelle sans l'unicité, c.-à-d., pour tout $\phi : A \to B$ comme dans la proposition, on peut de façon arbitraire étendre le morphisme $\Phi : K \to B$ à $K[X]$, en envoyant X sur un élément arbitraire de B.

Exemples 1.4.1 1) Le corps des fractions de $\mathbb{Z}$ est le corps des rationnels

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0 \right\}.$$

2) Soit k un corps et $A = k[X]$ l'anneau des polynômes à coefficients dans k ; c'est un anneau intègre (exercice !). Son corps des fractions est le corps des fractions rationnelles

$$k(X) = \left\{ \frac{P(X)}{Q(X)} \mid P, Q \in k[X],\ Q \neq 0 \right\}.$$

On a ainsi traité, pour un anneau intègre A, le cas où l'on rend inversible tous les éléments de $A \setminus \{0\}$. Dans diverses situations, on souhaite inverser seulement une partie S des éléments de A. De plus, comme on va le voir, cette construction est valable pour tout anneau commutatif A, sans hypothèse d'intégrité.

1.4.2 Le cas général

Commençons par quelques remarques préliminaires. D'abord, si l'on rend inversibles deux éléments s et t, on rendra aussi inversible leur produit. On peut donc, sans perte de généralité, supposer que l'ensemble S est stable par multiplication (c.-à-d., $s, t \in S \Rightarrow st \in S$). On peut aussi supposer que $0 \notin S$; en effet, si B est un anneau dans lequel 0 est rendu inversible, alors B est l'anneau nul, ce qui ne présente pas d'intérêt.

On dira donc que S est une partie multiplicative de A si $0 \notin S$ et si S est stable par multiplication. Dans ce cas, considérons l'ensemble $C = C_S$ des couples (a, s), où $a \in A$ et $s \in S$. Comme précédemment, on veut identifier deux couples (a, s) et (b, t) si $at = bs$. Mais d'autres identifications sont nécessaires. En effet, si un élément $a \in A$ vérifie $au = 0$, pour un $u \in S$, alors a doit être nul dans tout anneau où u est rendu inversible. On doit donc,pour un tel a, identifier dans notre construction $(a, 1)$ à $(0, 1)$. Pourtant, on n'a pas $a = 0$, mais seulement $au = 0$! Ceci conduit à considérer la relation suivante sur $C_S = A \times S$: on pose

$$(a, s) \sim (b, t)$$

s'il existe $u \in S$ tel que $(at - bs)u = 0$. Cette relation est clairement réflexive et symétrique. Elle est aussi transitive. En effet, si

$$(a, s) \sim (b, t) \sim (c, v),$$

il existe $u, u' \in S$ tels que $(at - bs)u = 0 = (bv - ct)u'$. Alors

$$atuvu' = bsuvu' = bvu'su = ctu'su = cstuu'$$

et donc $(av - cs)tuu' = 0$, avec $tuu' \in S$ puisque S est stable par multiplication. Ceci montre que $(a, s) \sim (c, v)$ et donc $\sim$ est une relation d'équivalence. Notons A_S l'ensemble quotient (c.-à-d., l'ensemble des classes d'équivalence), et, pour tout $(a, s) \in C_S$, désignons par $[a, s]$ son image dans A_S. Comme précédemment, on définit sur A_S une addition et une multiplication par les formules suivantes :

$$[a, s] + [b, t] = [at + bs, st], \qquad [a, s][b, t] = [ab, st]. \tag{2}$$

À nouveau, il faut vérifier que ces formules sont bien définies. Supposons que $[a, s] = [a', s']$. Alors, il existe $u \in S$ tel que $as'u = a'su$. Alors

$$abs'tu = a'subt = a'bstu \quad \text{et} \quad (at + bs)s'u = a'sut + bss'u = (a't + bs')su$$

et donc $[a'b, s't] = [ab, st]$ et

$$[at + bs, st] = [(at + bs)s'u, sts'u] = [(a't + bs')su, s'tsu] = [a't + bs', s't].$$

Ceci montre que, dans les égalités (2), les termes de droite ne dépendent que de la classe $[a, s]$ (et non du couple (a, s)). De même, ces termes ne dépendent que de la classe $[b, t]$. Ceci montre que l'addition et la multiplication sont bien définies.

À ce stade, on a fait tout le travail. On obtient alors sans difficultés, comme précédemment, le résultat suivant.

Théorème 1.4.3 *A_S est un anneau et l'application $\tau : A \to A_S$, $a \mapsto [a, 1]$ est un morphisme d'anneaux. Ce morphisme n'est en général pas injectif; plus précisément, on a*

$$\ker \tau = \{a \in A \mid \exists s \in S \text{ tel que } as = 0\}.$$

Pour tout $s \in S$, $\tau(s)$ est inversible dans A_S et pour tout $a \in A$ l'on a $[a, s] = \tau(a)\tau(s)^{-1}$.

De plus, A_S vérifie la propriété universelle suivante : pour tout morphisme d'anneaux $\phi : A \to B$ tel que $\phi(s)$ soit inversible pour tout $s \in S$, il existe un **unique** *morphisme $\Phi : A_S \to B$ tel que $\Phi \circ \tau = \phi$.*

Exemples : 1) $S = \{f^n, n \geq 1\}$, notation A_f.

2) $\mathfrak{p}$ idéal premier, $S = A \setminus \mathfrak{p}$, notation $A_{\mathfrak{p}}$.

En général, il n'y pas d'ambiguité. Mais pour $A = \mathbb{Z}$, on désigne en général par $\mathbb{Z}_p$ l'anneau des entiers p-adiques. Donc, pour éviter des erreurs d'interprétation, il vaut mieux noter $\mathbb{Z}[1/p]$ le localisé de $\mathbb{Z}$ en la partie multiplicative $S = \{p^n, n \geq 1\}$. On définit de même $\mathbb{Z}[1/N]$, pour tout entier $N \geq 2$.

Exercice 1.4.1 1) Soit $A = \mathbb{C}[X]$. Avec les notations A_f et $A_{\mathfrak{p}}$ introduites plus haut, décrire $\mathbb{C}[X]_X$ et $\mathbb{C}[X]_{(X)}$.

2) Soit $A = K_1 \times K_2$, où K_1, K_2 sont deux corps. On note $e_1 = (1, 0)$ et $e_2 = (0, 1)$. Montrer que $S_1 = \{e_1\}$ est une partie multiplicative. Qu'est-ce que A_S ?