ELEMENTS D'ALGEBRE COMMUTATIVE

Maîtrise de Mathématiques
Université d'Angers
2003/04

D. Schaub

Chapitre 1

Rappels sur les anneaux

1.1 Anneaux

Définition 1.1.1 *Un anneau est un ensemble A, muni de deux lois, notées en général par $+$ et $\times$ telles que $(A,+)$ soit un groupe abélien, $(A,\times)$ un monoïde (ie. la loi est associative) et vérifiant de plus une propriété de distributivité de l'addition par rapport à la multiplication.*

Si, de plus, la multiplication admet un élément neutre, noté 1 en général, on dira que l'anneau A est unitaire et si cette même multiplication est commutative, on dira que l'anneau est commutatif.

En fait, dans toute la suite, sauf mention expresse du contraire, tous les anneaux considérés seront commutatifs unitaires.

Exemples : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K[X]$, $K[X_1,\ldots,X_n]$, mais aussi, dans le cas non commutatif, $\mathrm{End}_K(E)$ où E est un K-espace vectoriel, l'ensemble des matrices carrées à coefficients dans K, l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, etc .... On peut aussi considérer que $A=\{0\}$ est un anneau.

Définition 1.1.2 *Un homomorphisme d'anneaux est une application $f : A \to B$ où A, B sont deux anneaux telle que, pour tous $a, a' \in A$, on ait $f(a+a') = f(a)+f(a')$ et $f(a\times a') = f(a)\times f(a')$. Si A et B sont unitaires, On dira que f est unitaire si $f(1)=1$.*

Définition 1.1.3 *Un sous-anneau d'un anneau A est un sous-groupe B de $(A,+)$ tel que, pour tous $x, y \in B$, $x\times y \in B$ (et, dans le cas unitaire, $1 \in B$).*

Donnons encore quelques définitions utiles :

- le *centre* d'un anneau A est l'ensemble des $x \in A$ tels que, pour tout $y \in A$, $x\times y = y\times x$. Le centre est un sous-anneau de A.

- Un élément $x \in A$ est dit *inversible* s'il existe $y \in A$ tel que $x\times y = y\times x = 1$. Les éléments inversibles de A forment un groupe pour la multiplication. Exemple : quels sont les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$? Si tout élément, non nul, de A est inversible, nous dirons que A est un *corps*.

- Un élément $x \neq 0$ de A pour lequel il existe $y \neq 0$ dans A tel que $xy = yx = 0$ est appelé *diviseur de zéro*. Un anneau qui ne possède aucun diviseur de zéro est dit *intègre*. Exemples : $\mathbb{Z}$ est intègre, un corps K est intègre, $\mathbb{Z}/6\mathbb{Z}$ ne l'est pas. Un type particulier de diviseur de zéro est donné par les éléments $x \in A$ tels qu'il existe un entier n avec $x^n = 0$. Un tel élément est dit *nilpotent*. L'ensemble des éléments nilpotents est appelé *nilradical* de A.

1.2 Idéaux

Nous pourrions donner la définition générale dans le cas d'anneaux non commutatifs d'idéal à droite, à gauche et bilatère, mais, comme rappelé ci-dessus, les anneaux considérés seront (presque) toujours commutatifs.

Définition 1.2.1 *Un idéal I d'un anneau A est un sous-ensemble de A tel que :*
1. $(I,+)$ est un sous-groupe de $(A,+)$;
2. pour tout $a \in A$ et tout $x \in I$, $a \times x \in I$.

Exemples : Si K est un corps, K n'a que deux idéaux $\{0\}$ et K lui-même. Si $f : A \to B$ est un homomorphisme d'anneaux, alors $\ker(f)$ est un idéal de A. Le nilradical d'un anneau est un idéal.

Soit $a \in A$, alors l'ensemble des éléments $\{ax | x \in A\}$ est un idéal de A, noté aA ou Aa, un tel idéal est dit *principal*. Un anneau **intègre** dans lequel tout idéal est principal est appelé *anneau principal*.

Exemples : $\mathbb{Z}$ ou $K[X]$ sont des anneaux principaux.

Définition 1.2.2 *soient I, J deux idéaux de A. L'ensemble $I + J = \{a + b | a \in I, b \in J\}$ est un idéal de A appelé somme de I et J.*
L'ensemble $IJ = \{$sommes finies de produits : $ab \mid a \in I, b \in J\}$ est un idéal de A appelé produit de I et J.

On peut encore noter que l'intersection $I \cap J$ est un idéal de A et on a $IJ \subseteq I \cap J$ tandis que la réunion $I \cup J$ **n'** est **pas** en général un idéal, mais on a $I \cup J \subseteq I + J$.

Définition 1.2.3 *Soit S une partie d'un anneau A, alors l'intersection de tous les idéaux de A contenant S est un idéal. On dit que c'est l'idéal engendré par S ou encore que les éléments de S sont des générateurs de cet idéal*

Exemple : L'idéal principal Aa est l'idéal engendré par a. Si $S = \{a_1, \ldots, a_n\}$ est une partie finie, on notera $(a_1, \ldots, a_n)$ l'idéal engendré par S. On peut par exemple vérifier que $I + J$ est l'idéal engendré par $I \cup J$.

1.3 Anneaux quotients

Soit A un anneau (commutatif !) et I un idéal. Définissons sur A la relation R par xRy ssi $x - y \in I$. On vérifie facilement que R est une relation d'équivalence ; on peut donc considérer l'ensemble quotient, ensemble des classes d'équivalence pour R, qu'on notera ici A/I, on notera $\overline{x}$, dans un premier temps et pour simplifier, la classe qui contient l'élément $x \in A$, par la suite, on écrira plus légitimement $a + I$.

On peut munir A/I d'une structure "naturelle" d'anneau en définissant deux lois :
- addition : $\overline{x} + \overline{y} = \overline{x + y}$, dont on vérifie la cohérence !
- multiplication : $\overline{x} \times \overline{y} = \overline{x \times y}$, pour laquelle également, on vérifie la légitimité.

On vérifie ensuite facilement que ces deux lois confèrent à A/I une structure d'anneau et que la surjection naturelle $\pi : A \to A/I$, $x \mapsto \overline{x}$, est un homomorphisme d'anneaux.

Théorème 1.3.1 *Pour tout homomorphisme d'anneaux $g : A \to B$ et tout idéal I de A tel que $I \subseteq \ker(g)$ se factorise à travers un unique homomorphisme d'anneaux $h : A/I \to B$.*

Preuve : Il n'y a pas de choix pour définir h car "factoriser" signifie que l'on doit avoir $h \circ \pi = g$ où $\pi : A \to A/I$ est la surjection naturelle ; on doit donc avoir $h(\overline{(x)}) = g(x)$ pour tout $x \in A$. Il suffit de voir que cette application est *bien définie*, c'est-à-dire qu'elle n'envoie pas un élémnent de A/I sur plusieurs éléments de B : en effet, on définit l'image de la classe de $x \in A$ comme l'image de *n'importe quel* élément x' qui se trouve dans la même classe, modulo I, que x. En somme, il faut vérifier que si xRx' alors $g(x) = g(x')$; mais c'est précisément ce que donne la condition $I \subseteq \ker(g)$, puisque $xRx' \Leftrightarrow x - x' \in I \subseteq \ker(g) \Rightarrow g(x - x') = 0 \Rightarrow g(x) = g(x')$. L'unicité provient du fait que l'on n'a eu aucun choix pour définir h.

Remarque : un cas particulier très important est le cas où précisément $I = \ker(g)$; dans ce cas, h devient injective.

Proposition 1.3.1 *Il y a une correspondance biunivoque entre les idéaux de A contenant un idéal I et les idéaux de A/I.*

La preuve est laissée en exercice.

1.4 Idéaux premiers. Idéaux maximaux

Définition 1.4.1 *Un idéal $\mathfrak{p} \neq A$ d'un anneau A est dit premier si $x \times y \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$.*
Un idéal $\mathfrak{m} \neq A$ est dit maximal si, pour tout idéal propre I, $I \supseteq \mathfrak{m} \Rightarrow I = \mathfrak{m}$.

Lemme 1.4.1 *$\mathfrak{p}$ est premier ssi $A/\mathfrak{p}$ est intègre.*

Preuve : Supposons $\mathfrak{p}$ premier, alors $\overline{x}\overline{y} = 0 \Rightarrow xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$, d'où $\overline{x} = 0$ ou $\overline{y} = 0$.

Inversement, si $A/\mathfrak{p}$ est intègre, on a $xy \in \mathfrak{p} \Rightarrow \overline{xy} = \overline{x}\overline{y} = 0$ dans le quotient, d'où $\overline{x} = 0$ ou $\overline{y} = 0$, c'est-à-dire $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$.

Lemme 1.4.2 *1. $\mathfrak{m}$ est maximal ssi $A/\mathfrak{m}$ est un corps.*
2. Si $\mathfrak{m}$ est maximal, alors $\mathfrak{m}$ est premier.

Preuve : 2. est une conséquence immédiate de 1.

1. Supposons d'abord $\mathfrak{m}$ maximal et soit $\overline{x} \neq 0$ un élément du quotient. Alors $x \notin \mathfrak{m}$, d'où l'idéal engendré par x et $\mathfrak{m}$ est l'anneau A tout entier, donc $1 \in A$ peut s'écrire $1 = \lambda x + m$ où $m \in \mathfrak{m}$, ce qui nous donne dans le quotient : $\overline{\lambda}\overline{x} = 1$ ie. $\overline{x}$ admet un inverse $\overline{\lambda}$.

Inversement, supposons que $A/\mathfrak{m}$ soit un corps. Considérons un idéal propre I et supposons que $I \supset \mathfrak{m}$ strictement, alors, il existe $x \in I$ tel que $\overline{x} \neq 0$, il existe donc $\overline{y}$ tel que $\overline{x}\overline{y} = 1$, ce qui se traduit dans A, par $xy - 1 \in \mathfrak{m}$ ou encore $1 = xy + m$, $m \in \mathfrak{m}$. Mais, $m \in \mathfrak{p} \subset I$ et $x \in I \Rightarrow xy \in I$ ce qui implique $1 \in I$, d'où $I = A$.

Exemples : Tous les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. Lesquels sont premiers ? Lesquels sont maximaux ? De même, pour $k[X]$ où k est un corps. Donner des exemples d'idéaux, d'idéaux premeirs, d'idéaux maximaux de $k[X, Y]$, de $k[X, Y, Z]$.

Théorème 1.4.1 *Tout idéal propre I de A est contenu dans un idéal maximal.*

Avant de prouver ce théorème, il nous faut faire un rappel sur un *axiome* de la théorie des ensembles (équivalent à l'axiome du choix) qu'on appelle le

Lemme 1.4.3 ***de Zorn*** *Tout ensemble inductivement ordonné non vide admet des éléments maximaux.*

Rappelons qu'un ensemble E est dit *inductivement ordonné* si tout sous-ensemble totalement ordonné F de E admet un majorant, c'est-à-dire qu'il existe un élément $x \in E$ tel que $\forall y \in F,\ y \leq x$. Un *élément maximal* de E est un élément $a \in E$ tel que $x \in E$ et $a \leq x \Rightarrow a = x$. Preuve du théorème : Considérons l'ensemble $\mathcal{E}$ des idéaux propres J de A tels que $I \subseteq J$. On ordonne $\mathcal{E}$ par inclusion. On a $I \in \mathcal{E}$, donc $\mathcal{E}$ est non vide.

Montrons que $\mathcal{E}$ est ordonné inductivement. Soit $\mathcal{F}$ un sous-ensemble totalement ordonné de $\mathcal{E}$. Alors, pour tout couple d'idéaux H et K de $\mathcal{F}$, on a $H \subseteq K$ ou $K \subseteq K$, 1 n'appartient à aucun et chacun contient I. Prenons alors la réunion L des éléments de $\mathcal{F}$. C'est un idéal de A : en effet, si $x, y \in L$, alors il existe $H \subseteq K$ tels que $x \in H, y \in K$, donc $x - y \in K \subset L$, donc $(L, +)$ est un groupe. De plus, pour tout $a \in A$, $ax \in H \subset L$. L est donc un idéal, ne contenant pas 1 (sinon, il existerait un H qui contiendrait 1). Enfin, il est clair que $I \subset L$. Donc L est un majorant de $\mathcal{F}$.

Par conséquent, $(\mathcal{E}, \subseteq)$ satisfait aux hypothèses du lemme de Zorn, donc admet un élément maximal M, c'est-à-dire qu'il existe M dans $\mathcal{E}$ tel que $K \in \mathcal{E},\ M \subseteq M \Rightarrow K = M$. Ce qui, par définition, dit que M est un idéal maximal de A qui contient I par construction.

Corollaire 1.4.1 *Tout élément non inversible de A est contenu dans un idéal maximal.*

Définition 1.4.2 *Un anneau A qui n'a qu'un seul idéal maximal est dit local. S'il possède un nombre fini d'idéaux, on dit qu'il est semi-local.*

Proposition 1.4.1 *i. Soit A un anneau et M un idéal propre de A tel que tout x n'appartenant pas à M est inversible. Alors A est local d'idéal maximal M.*

ii. Soit M un idéal maximal d'un anneau A et supposons que tout élément x de $1 + M = \{1 + m | m \in M\}$ est inversible, alors (A, M) est local.

Preuve : i. M est clairement maximal puisque la condition implique que tout élément non nul de A/M est inversible, donc A/M est un corps. De plus, si I est un idéal de A, non contenu dans M, alors il existe $x \in I, x \notin M$, mais alors l'hypothèse dit que x est inversible, donc que $1 = x^{-1}x \in I$, d'où $I = A$. Autrement dit, tout idéal propre de A est contenu dans M.

ii. Supposons qu'il existe un idéal I de A qui ne soit pas contenu dans M. Alors, par maximalité de M, $I + M = A$. D'où, il existe $x \in I,\ m \in M$ tels que $1 = x + m$ ou encore $x = 1 - m \in 1 + M$, donc x est inversible, d'où $I = A$.

1.5 Anneaux de fractions

Soit A un anneau. Nous dirons qu'un sous-enssemble S de A est une *partie multiplicative* si $1 \in S$ et $\forall x, y \in S,\ xy \in S$.

Considérons alors l'ensemble produit $S \times A$ et la relation d'équivalence sur ce produit :

$$(s, a)R(t, b) \Leftrightarrow \exists u \in S \text{ tq. } u(ta - sb) = 0.$$

On vérifie bien sûr que R est bien une relation d'équivalence et on note $S^{-1}A$ l'ensemble quotient et $\frac{a}{s}$ un représentant de la classe (s, a).

On peut munir $S^{-1}A$ d'une structure d'anneau en le munissant des deux opéraitions suivantes :

- addition : $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$; on vérifie que c'est bien défini et que cette loi confère à $S^{-1}A$ une structure de groupe abélien ;

- multiplication : $\frac{a}{s} \times \frac{b}{t} = \frac{ab}{st}$; là encore on fait les vérifications nécessaires et on définit :

Définition 1.5.1 *L'anneau $(S^{-1}A, +, \times)$ est appelée anneau des fractions de A relativement à S.*

On a une application naturelle : $\phi : A \to S^{-1}A$ définie par $\phi(a) = \frac{a}{1}$ qu'on vérifie être un homomorphisme d'anneaux unitaires. De plus, pour tout $s \in S$, $\phi(s)$ est inversible dans $S^{-1}A$.

Remarques : 1. Si $0 \in S$, alors $S^{-1}A = \{0\}$.

2. Si A est intègre, ϕ est injective et on identifie A au sous-anneau $\phi(A)$ de $S^{-1}A$ (on remarquera que, dans ce cas, la relation R s'écrit plus simplement : $(a,s)R(b,t) \Leftrightarrow at = bs$).

Exemples : le premier exemple qui vient à l'esprit évidemment est le passage de $\mathbb{Z}$ à $\mathbb{Q}$, autrement dit l'introduction des "vraies" fractions. Effectivement, prenons dans $\mathbb{Z}$, $S = \{n \in \mathbb{Z} | n \neq 0\}$, alors S est une partie stable et $S^{-1}\mathbb{Z} = \mathbb{Q}$. Comme $\mathbb{Z}$ est intègre, on réalise $\mathbb{Z}$ comme un sous-anneau de $\mathbb{Q}$.

Cet exemple se généralise à tout anneau A intègre en prenant pour S l'ensemble des éléments non nuls. On obtient ainsi $A \subset S^{-1}A$ qui est un corps, puisque tout élément non nul y est inversible. Dans ce cas, $S^{-1}A$ s'appelle le corps des fractions de A. Si $A = \mathbb{Z}$, c'est l'exemple ci-dessus, si $A = k[X]$, on obtient pour $S^{-1}A$ le corps des fractions rationnelles à une variable, et de même pour plusieurs variables.

Si $f \in A$ n'est pas un diviseur de zéro, alors l'ensemble $S = \{1, f, f^2, \ldots, f^k, \ldots\}$ est une partie multiplicative et $S^{-1}A = \{\frac{a}{f^n} | a \in A, k \in \mathbb{Z}\}$.

Dernier exemple, si $\mathfrak{p}$ est un idéal premier de A, alors $S = A \backslash \mathfrak{p}$ est une partie multiplicative et l'anneau des fractions correspondant $S^{-1}A$ est noté $A_{\mathfrak{p}}$ et appelé *localisé de A en $\mathfrak{p}$*.

Comme dans le cas des quotients (à ne pas confondre avec l'anneau des fractions ! ! !), on a une "propriété universelle" (càd. qui caractérise) d'un anneau de fractions :

Proposition 1.5.1 *Soit $f : A \to B$ un homomorphisme d'anneaux (unitaires) et S une partie multiplicative de A telle que, pour tout $s \in S$, $f(s)$ est inversible dans B. Alors, il existe un unique homomorphisme $h : S^{-1}A \to B$ tel que $f = h \circ \phi$.*

Preuve : il est naturel de vouloir définir h par

$$h(\frac{a}{s}) = f(a)f(s)^{-1}$$

en ayant remarqué déjà que $f(s)$ est inversible.

Il faut vérifier que c'est bien défini : prenons $\frac{a}{s} = \frac{b}{t}$, alors, il existe $u \in S$ tel que $u(at - bs) = 0$, d'où $f(u)(f(a)f(t) - f(b)f(s)) = 0$, mais comme $f(u)$ est inversible, on en déduit $f(a)f(t) = f(b)f(s)$ ou encore $f(a)f(s)^{-1} = f(b)f(t)^{-1}$. Il ne reste qu'à vérifier que c'est bien un homomorphisme d'anneaux ; l'unicité résulte immédiatement de la définition.

Proposition 1.5.2 *Soit A un anneau et S une partie multiplicative de A, alors :*

(i) pour tout idéal I de A, $S^{-1}I = \{\frac{a}{s} | a \in I, s \in S\}$ est le $S^{-1}A$-idéal engendré par $\phi(I)$. De plus, tout idéal propre J de $S^{-1}A$ provient d'un idéal de A ne rencontrant pas S.

(ii) S^{-1} respecte l'inclusion et l'on a : $S^{-1}(I+J) = S^{-1}I + S^{-1}J$, $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$, $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

(iii) Les idéaux premiers de $S^{-1}A$ sont en bijection avec les idéaux premiers de A ne rencontrant pas S.

Preuve : On vérifie facilement que $S^{-1}I$ est un idéal de $S^{-1}A$. De plus, $S^{-1}I \supseteq \phi(I)$, d'où $\phi(I)S^{-1}A$ (qui est précisément l'idéal engendré par $\phi(I)$ dans $S^{-1}A$) est inclus dans $S^{-1}I$. Mais, comme, pour tout $a \in I$, $\frac{a}{s} = \frac{a}{1}\frac{1}{s} \in \phi(I)S^{-1}A$, on en déduit que $S^{-1}I \subseteq \phi(I)S^{-1}A$.

Soit J un idéal de $S^{-1}A$. Alors $\phi^{-1}(J)$ est un idéal de A et $\phi^{-1}(J) \cap S = \emptyset$ (sinon, il existe $s \in S$, $s \in \phi^{-1}(J)$, d'où $\phi(s) = s/1 \in J$ et $1 = (\frac{1}{s})(\frac{s}{1}) \in J$ ie. $J = S^{-1}A$).

(ii) est immédiat.

(iii) Soit $\mathfrak{q}$ un idéal premier de $S^{-1}A$; alors $\phi^{-1}(\mathfrak{q})$ est un idéal premier de A ne rencontrant pas S et on a, comme dans (i), $S^{-1}(\phi^{-1}(\mathfrak{q})) = \mathfrak{q}$.

Inversement, soit $\mathfrak{p}$ un idéal de A ne rencontrant pas S, alors, par définition de $S^{-1}\mathfrak{p}$, $S^{-1}\mathfrak{p}$ est un idéal premier de $S^{-1}A$ et on vérifie que $\phi^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$. En effet, une des inclusions est purement ensembliste : $\mathfrak{p} \subseteq \phi^{-1}(S^{-1}\mathfrak{p})$. Mais, d'un autre côté, si $x \in \phi^{-1}(S^{-1}\mathfrak{p})$, alors $\phi(x) \in S^{-1}\mathfrak{p} \Rightarrow \exists y \in \mathfrak{p},\ t \in S$ tels que $\frac{x}{1} = \phi(x) = \frac{y}{t}$. Ce qui signifie qu'il existe $s \in S$ tel que $s(tx - y) = 0$, donc $stx \in \mathfrak{p}$ et, comme $st \notin \mathfrak{p}$, on en déduit $x \in \mathfrak{p}$.

Exemple-Remarque : Il n'est pas vrai que S^{-1} réalise une bijection entre l'ensemble des idéaux de A qui ne rencontrent pas S et l'ensemble des idéaux de $S^{-1}A$.

En effet, soit A un anneau et $\mathfrak{p}_1, \mathfrak{p}_2$ deux idéaux premiers. Soit $S = A \setminus \mathfrak{p}_1$ et $I = \mathfrak{p}_1 \cap \mathfrak{p}_2$. Alors, si $t \in \mathfrak{p}_2$, $t \notin \mathfrak{p}_1$, et $x \in \mathfrak{p}_1$, $x \notin \mathfrak{p}_2$, $y = tx \in I$, d'où $x = \frac{y}{t} \in S^{-1}I$, autrement dit $x \in \phi^{-1}(S^{-1}I)$, mais $x \notin I$, d'où $\phi^{-1}(S^{-1}I) \neq I$.

1.6 Compléments

Lemme 1.6.1 ***d'évitement*** *Soit A un anneau commutatif unitaire et I un sous-ensemble de A stable pour l'addition et la multiplication (en particulier, I peut être un idéal de A). Soit $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\}$ une famille d'idéaux dont 2 au plus ne sont pas premiers. Alors*

$$I \subseteq \bigcup_{i=1}^{s} \mathfrak{p}_i \Rightarrow \exists i \text{ tel que } I \subseteq \mathfrak{p}_i.$$

Preuve : On procède par récurrence sur s. Si $s = 1$, il n'y a rien à prouver.

(1) Soit il existe un j tel que $I \cap \mathfrak{p}_j \subseteq \cup_{i \neq j} \mathfrak{p}_i$, auquel cas, $I \subseteq \cup_{i \neq j} \mathfrak{p}_i$ et le lemme est prouvé par récurrence.

(2) Soit, pour tout j, $I \cap \mathfrak{p}_j \not\subseteq \cup_{i \neq j} \mathfrak{p}_i$. Choisissons alors, pour tout j, $x_j \in I \cap \mathfrak{p}_j$, $x_j \notin \cup_{i \neq j} \mathfrak{p}_i$.

Prenons k tel que si $s > 2$, alors $\mathfrak{p}_k$ est premier, si $s = 2$, alors k quelconque et posons

$$z = x_k + \prod_{i \neq k} x_i.$$

Je prétends que z, qui appartient évidemment à I, n'appartient à aucun des $\mathfrak{p}_j$. En effet :
• Si $s = 2$, $z = x_1 + x_2 \notin \mathfrak{p}_i$ pour $i = 1, 2$.
• Si $s > 2$, supposons d'abord que $z = x_k + \prod_{i \neq k} x_i \in \mathfrak{p}_k$. On en déduit que $\prod_{i \neq k} x_i \in \mathfrak{p}_k$ et, comme $\mathfrak{p}_k$ est premier, cela implique que l'un au moins de ces x_i appartient à $\mathfrak{p}_k$, ce qui contredit le choix de x_i.

Supposons maintenant que $z = x_k + \prod_{i \neq k} x_i \in \mathfrak{p}_j$, pour un $j \neq k$. Mais alors, cela signifie que $x_k \in \mathfrak{p}_j$, ce qui contredit le choix de x_k.
Conclusion : il existe $z \in I$ tel que z n'appartient à aucun $\mathfrak{p}_j$, ce qui évidemment contredit le fait que $I \subseteq \cup_{i=1}^{s} \mathfrak{p}_i$. Donc (2) est faux, donc (1) est vrai et on conclut par récurrence.

Exercice : Soient $I_1, \ldots, I_n$ des idéaux de A et $\mathfrak{p}$ un idéal premier tel que $\mathfrak{p} \supseteq \cap_{r=1}^{n} I_r$, alors il existe s tel que $\mathfrak{p} \supseteq I_s$. De plus, si $\mathfrak{p} = \cap_{r=1}^{n} I_r$, alors il existe s tel que $\mathfrak{p} = I_s$.

Définition 1.6.1 *Le radical (de Jacobson) d'un anneau A est l'intersection de tous les idéaux maximaux de A. C'est bien sûr un idéal, on le notera $R(A)$ ou encore $\sqrt{A}$.*

Proposition 1.6.1 *Un élément x de A appartient au radical $R(A)$ de A ssi $1 - xy$ est inversible dans A, pour tout $y \in A$.*

Preuve : $\Rightarrow$: Soit $x \in R(A)$. Si $1-xy$ n'est pas inversible pour au moins un $y \in A$, alors $1-xy$ est contenu dans un idéal maximal M. Mais $x \in R(A) \subseteq M$, d'où $xy \in M$ et, par conséquent, $1 \in M$ ce qui est impossible.

$\Leftarrow$: Supposons donc $1-xy$ inversible, pour tout $y \in A$ et supposons qu'il existe un idéal maximal M qui ne contient pas x. Alors, $xA + M = A$, d'où, il existe $m \in M$ et $y \in A$ tels que $xy + m = 1$; autrement dit, $m = 1 - xy \in M$, ce qui est absurde puisque $1 - xy$ est inversible.

Proposition 1.6.2 *Le nilradical $N(A)$ est l'intersection de tous les idéaux premiers de A.*

Preuve : Soit N' l'intersection de tous les idéaux premiers de A. Il nous faut montrer $N' = N(A)$.

Montrons d'abord $N \subseteq N'$. Pour cela , soit $x \in A$ nilpotent ; il existe donc $n \in \mathbb{N}$ tel que $x^n = 0$. Mais alors $x^n \in \mathfrak{p}$, d'où $x \in \mathfrak{p}$, pour tout idéal premier $\mathfrak{p}$ de A.

Inversement : soit $x \in A$ non nilpotent. On va montrer qu'il existe $\mathfrak{p}$, un idéal premier, tel que $x \notin \mathfrak{p}$.

Soit $\Sigma = \{I \text{ idéal} \mid \forall n > 0,\ x^n \notin I\}$. Clairement, $\{0\} \in \Sigma$, donc $\Sigma \neq \emptyset$ et Σ est une partie ordonnée inductivement ; par conséquent, d'après le lemme de Zorn, Σ admet un élément maximal, appelons-le $\mathfrak{p}$. On montre que $\mathfrak{p}$ est un idéal premier.

Soient $u, v \notin \mathfrak{p}$. Alors $\mathfrak{p}$ est strictement inclus dans $\mathfrak{p} + Au$ et dans $\mathfrak{p} + Av$, d'où, par maximalité de $\mathfrak{p}$, ni l'un, ni l'autre de ces idéaux n'appartient à Σ. Par conséquent, il existe $m > 0$ et $n > 0$ tels que $x^m \in \mathfrak{p} + Au$ et $x^n \in \mathfrak{p} + Av$, d'où $x^{m+n} \in (\mathfrak{p} + Au)(\mathfrak{p} + AV) = \mathfrak{p} + Auv$. D'où $\mathfrak{p} + Auv$ n'appartient pas à Σ, autrement dit, $uv \notin \mathfrak{p}$. Donc $\mathfrak{p}$ est un idéal premier qui, par construction, ne contient pas x.

Bibliographie

[1] S. LANG, Algèbre, Addison-Wesley.

[2] M.F. ATIYAH, I.G. MACDONALD, Introduction to Commutative Algebra, Addison Wesley Publishing.

[3] R. GODEMENT, Cours d'Algèbre, Herrmann

[4] H. MATSUMURA, Commutative Algebra, Benjamin.

[5] N. BOURBAKI, Algèbre

[6] S. MAC LANE, G. BIRKHOFF, Algèbre 2, les Grands Théorèmes, Gauthier-Villars.

[7] J.P. SERRE, Représentation linéaire des groupes finis.

[8] FULTON, HARRIS, Representations, Springer.

[9] O. ZARISKI, P. SAMUEL, Commutative Algebra, Van Nostrand.

Table des matières