Anneau et corps

G Philippe,S Rouzes,E Vieillard-Baron

janvier 2001

Table des matières

Chapitre 1

Anneaux et corps

Par Emmanuel Vieillard Baron

1.1 Introduction

Après avoir étudié la structure de groupes nous allons nous pencher sur celles d'anneau et de corps. Les structures d'anneau et de corps sont des enrichissements de celle de groupe. En effet, un anneau (ou un corps) est un groupe muni d'une deuxième loi interne. Cette deuxième loi n'aura généralement pas, pour la structure d'anneau, toutes les propriétés de la première. Il lui manquera, en particulier, la possibilité d'un inverse pour chacun des éléments de l'anneau. La seconde loi d'un corps possèdera, quant à elle, toutes les propriétés de la première. La structure d'anneau sera le plus souvent rencontrée sur des ensembles de fonctions ou de matrices. Celle de corps, beaucoup plus rare, est celle des ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de leurs lois additives et multiplicatives. D'autres ensembles bénéficient de cette structure mais ils sont moins accessibles. Il s'agit de $\mathbb{F}^p \simeq \mathbb{Z}/p\mathbb{Z}$ quand p est un nombre premier ou encore du corps des quaternions qui peut être vu comme un certain sous ensemble des matrices 4×4.

1.2 Anneau

Définition Soit A un ensemble possédant deux lois internes que l'on note, par analogie avec $\mathbb{Z}$, + et . . On dit que le triplet (A,+,.) possède une structure d'**anneau** si:

- (A,+) a une structure de groupe abélien. Le neutre de la loi + est noté 0.
- La loi . est distributive par rapport à la loi + :

$$\forall\, x,y,z \in A, x.(y+z) = x.y + x.z$$

- La loi . est associative:

$$\forall\, x,y,z \in A, x.(y.z) = (x.y).z$$

- Si de plus, il existe un élément neutre dans A pour la loi . (que l'on note 1 et qu'on appelle **élément unité de l'anneau**) alors l'anneau A sera dit **unitaire**.

Remarque On considérera toujours dans la suite des anneaux qui sont unitaires et on utilisera le mot anneau pour anneau unitaire.

Remarque On notera -a l'inverse (l'opposé...) de a pour la loi +. Par abus d'écriture, on notera A l'anneau (A,+,.).

Définition Si l'élément x d'un anneau possède un inverse pour la deuxième loi de cet anneau, on dira que x est un **élément inversible** de cet anneau et on notera x^{-1} son inverse.

Remarque Rien n'empêche, dans le cas général, que 1=0 !!!

Proposition L'ensemble des éléments inversibles d'un anneau possède une structure de groupe pour la multiplication de l'anneau.

Démonstration C'est facile.

Proposition (Propriétés arithmétiques sur les anneaux) Soit (A,+,.) un anneau. Pour tout x,y∈A, on a:

1. $0.x = 0$
2. $(-1).x = -x$
3. $(-1).(-1) = 1$
4. $(-x).y = -x.y$

Démonstration

1. $0.x + x = 0.x + e.x = (0 + e).x = e.x = x$. Donc $0.x = 0$.
2. $0 = 0.x = (1 - 1).x = 1.x - 1.x = x - 1.x$ donc $-x = -1.x$.
3. On multiplie par -1 l'égalité $(-1)+1 = 0$. Cela donne $(-1).(-1)+(-1).(1) = 0$ et donc $(-1).(-1) + (-1) = 0$ ce qui prouve que $(-1).(-1) = 1$.
4. $x.y + (-x).y = (x + (-x)).y = (x - x).y = 0.y = 0$ donc l'opposé de $x.y$ qui est, par convention d'écriture, $-x.y$, est égal à $(-x).y$.

Définition Un anneau A sera dit **intègre** si 1≠0 et si pour tout élément $x,y \in A$ on a:

$$x.y = 0 \Rightarrow x = 0 \ \ ou\ y = 0.$$

Dans le cas contraire, c'est à dire dans le cas où A n'est pas intègre, il existe des éléments x et y dans A tout deux non nuls et tels que x.y=0.

Définition Soit A un anneau et x, y des éléments de A non nuls tels que x.y=0. x et y sont des **diviseurs de 0**.

Définition Un anneau sera dit **commutatif** si la deuxième loi de l'anneau est commutative.

Définition Soit (A,+,.) un anneau et soit A' un sous ensemble de A. A' est **un sous anneau de A** si et seulement si A' muni des lois de A restreintes à A possède lui aussi une structure d'anneau.

Proposition Voici quelques formules algébriques vraies dans un anneau A commutatif: si x,y∈A, n,m∈$\mathbb{N}$:

- $x^{m+n}=x^m x^n$.
- $(x^m)^n=x^{mn}$.
- $(xy)^n=x^n y^n$.
- **Formule du binôme de Newton**:$(x+y)^n=\sum_{i=0}^{n} C_n^i x^i y^{n-i}$.

Ces formules sont valables avec la convention $x^0=1$ pour tout x de A.

Démonstration On passera sous silence la démonstration des trois premiers points qui se traitent sans problème par récurrence.
Le dernier point se démontrer lui aussi par récurrence:
si n=1 la formule est triviale, supposons la donc vraie à l'ordre n-1 et démontrons la à l'ordre n: $(x+y)^n = (x+y).(x+y)^{n-1} = (x+y).\sum_{i=0}^{n-1} C_{n-1}^i x^i y^{n-1-i}$ ce qui donne, en distribuant la parenthèse sur chacun des termes de la somme:

$$\sum_{i=0}^{n-1} C_{n-1}^i x^{i+1} y^{n-1-i} + \sum_{i=0}^{n-1} C_{n-1}^i x^i y^{n-i}.$$

Le premiere partie de l'expression précédente peut encore s'écrire:

$$\sum_{i=1}^{n} C_{n-1}^{i-1} x^i y^{n-i}.$$

Voila qui permet de l'additionner à la seconde partie et cela donne:

$$\sum_{i=0}^{n} (C_{n-1}^{i-1} + C_{n-1}^i) x^i y^{n-i}$$

mais comme $C_{n-1}^{i-1}+C_{n-1}^i=C_n^i$ la formule est démontrée.

1.3 Idéaux

Définition Soit (A,+,.) un anneau et I un sous ensemble de A. I est un **idéal à gauche** (resp. **à droite**) de A si et seulement si:

- I est un sous groupe abélien de A pour la loi +.
- Pour tout élément a de A et x de I, a.x (resp x.a) est un élément de I.

Définition Soit A un anneau et I un sous ensemble de A. I est un **idéal bilatère** de A si et seulement si I est à la fois un idéal à gauche et un idéal à droite de A. On utilisera de manière générale le mot idéal pour idéal bilatère.

Définition Soit A un anneau et I un un idéal (bilatère) de A. I est un **idéal premier** de A si et seulement si I n'est pas égal à A tout entier et si I vérifie:

$$\forall x,y \in A,\, x.y \in I \Rightarrow x \in I \;\; ou\, y \in I.$$

Définition Soit A un anneau et I un idéal de A. I est un **idéal principal** de A si et seulement si I est engendré par un unique élément a de A. Autrement dit:

$$I = \{x.a; a \in A\}.$$

On notera dans ce cas (a), l'idéal engendré par l'élément a de A.

Définition L'idéal (0) engendré par l'élément 0 d'un anneau A sera appelé l'**idéal nul** de A.

Définition Un anneau est dit **principal** si il est intègre et que tout ses idéaux sont principaux.

Définition Un idéal I dans un anneau A est dit **strict** ou **propre dans A** si il n'est pas égal à l'anneau tout entier.

Définition Un idéal est **maximal** si il strict et si il n'est contenu dans aucun idéal autre que l'anneau tout entier.

Proposition Si un idéal d'un anneau A contient l'élément unité de l'anneau alors cet idéal est égal à l'anneau tout entier.

Démonstration Supposons que l'idéal I de l'anneau A contienne l'élément 1 de A. Alors pour tout a$\in$A, a=a.1 est, par définition d'un idéal, élément de I. Donc A$\subset$I et I=A.

Définition Un idéal dans un anneau A sera dit **finiment engendré** si l'ensemble de ses générateurs est fini, c.a.d si il existe n$\in\mathbb{N}$ et des éléments $a_i \in$ A pour i=1,...,n tels que $\forall x \in I, \exists x_1,...,x_n \in A / x = \sum_{i=1}^{n} x_i.a_i$.

Théorème de Krull Soit I un idéal d'un anneau A. Alors il existe un idéal maximal de A contenant I.

Démonstration Considérons l'ensemble $\mathcal{I}$ des idéaux de A contenant I et non égaux à A. $\mathcal{I}$ est non vide car il contient I. $\mathcal{I}$ est un ensemble partiellement ordonné par l'inclusion. $\mathcal{I}$ est inductif car tout partie P non vide de $\mathcal{I}$ totalement ordonnée pour l'inclusion possède un majorant. Ce majorant est donné par la réunion des éléments de

P, à savoir que cette réunion est bien un idéal propre de $\mathcal{I}$ car la réunion est prise sur une suite croissante d'idéaux propres de $\mathcal{I}$. On peut appliquer le lemme de Zorn. $\mathcal{I}$ possède un élément maximal. Ce dernier est un idéal propre de A contenant I et contenu dans aucun autres idéaux propres de A.

1.4 Corps

Définition Soit k un ensemble et soient + et . deux lois internes sur k. Le triplet (k,+,.) possède une structure de **corps** si:

- (k,+,.) a une structure d'anneau commutatif unitaire.
- (k$\backslash\{0\}$,.) a une structure de groupe (abélien).

Exemple $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ ont des structures de corps pour leur addition et multiplication respectives. D'autres corps existent mais ils sont beaucoups moins accessibles. Nous pensons, par exemple, au corps des quaternions d'Hamilton.

Remarque Par abus d'écriture et quand aucune confusion n'est à craindre, nous noterons k le corps (k,+,.).

Proposition Soit k un corps. Alors:

- 1$\neq$0.
- k ne possède pas de diviseurs de 0 (k est donc intègre).

Démonstration

- Autrement la définition d'un corps n'a plus de sens (cf 2^{ieme} point).
- Supposons qu'il existe x et y dans k tels que x.y=0. Supposons de plus que x n'est pas nul. Alors x est inversible et x^{-1}.x.y=x^{-1}.0=0 . Donc y=0 et x, y ne sont pas des diviseurs de 0.

Proposition fondamentale Les seuls idéaux d'un corps sont l'idéal nul et le corps tout entier. Réciproquement si A est un anneau n'ayant comme seuls idéaux que l'idéal nul et lui même alors A est un corps.

Démonstration

- Supposons que k est un corps. Soit I un idéal non nul de A. Soit donc x un élément non nul de I. x est, par définition d'un corps, inversible dans k. Soit x^{-1} l'inverse de x dans k. x^{-1}.x est, par définition d'un idéal, élément de I. Mais x^{-1}.x est égal à l'élément unité de k. Donc 1$\in$I et I=k.
- Supposons maintenant que les seuls idéaux de l'anneau A sont l'idéal nul et A tout entier. Il nous suffit de montrer que tout les éléments non nuls de A sont inversibles. Soit x$\neq$0 un élément de A. Soit (x) l'idéal engendré par x. Comme x n'est pas nul, cet idéal n'est pas nul non plus. Il est alors égal à A tout entier. L'unité de A est donc élément de (x). Ceci signifie qu'il existe y dans A tel que x.y=1. x est donc inversible d'inverse y, Cqfd.

Définition Soit k un corps. Soit A le sous anneau de k engendré par l'élément unité de k. Les éléments de A sont de la forme $\underbrace{1+1+...+1}_{n\ fois}$. Si A est de cardinal fini alors la **caractéristique de k** est le cardinal de A. Sinon on dit que la caractéristique de k est nulle. Remarqons que si k est de caractéristique n alors $\underbrace{1+1+...+1}_{n\ fois}=0$.

1.5 Anneaux Noethériens

La notion d'anneau noethérien a un rôle un peu analogue à celle de la notion de compacité en topologie dans le sens où on ramène une propriété ayant "un caractère infini" à une propriété ayant un caractère fini. Cette remarque prend encore plus de sens quand on s'intéresse à des anneaux munis d'une topologie (Topologie de Zariski). Mais nous ne nous étendrons pas et nous contenterons dans ce paragraphe de donner quelques définitions.

Définition - Proposition Soit A un anneau. A est un **anneau Noethérien** si il vérifie une des propriétés équivalentes suivantes:

- Tout idéal de A est finiment engendré.
- Toute suite croissante d'idéaux de A est stationnaire.
- Tout ensemble non vide d'idéaux de A possède un élément maximal pour l'inclusion.

Remarque Explicitons les différents termes intervenant dans cette définition:

Définition On entend par **suite croissante d'idéaux de A** une suite $(I_n)_{n\in IN}$ d'idéaux de A telle que pour tout $n\in\mathbb{N}$ $I_n\subset I_{n+1}$. Dire que cette suite est stationnaire revient à dire qu'il existe $m\in\mathbb{N}$ tel que si $n\geq m$ alors $I_n=I_{n+1}$.

Définition Si l'on considère un ensemble X constitué de sous ensembles d'un ensemble donné (désolé pour la formulation!), on peut considérer la relation "*être inclus dans*" comme un ordre partiel sur X. Un élément Y_0 sera dit **maximal pour la relation d'inclusion** si pour tout élément Y de X, Y est inclus dans Y_0.

Démontrons maintenant la propriété.

Démonstration

- Supposons que tout idéal de A est finiment engendré et montrons que toute suite croissante d'idéaux de A est finiment engendré. Soit $(I_n)_{n\in IN}$ une suite croissante d'idéaux de A. Chacun de ses idéaux I_k possède, par hypothèse, un ensemble fini de générateurs que l'on note Jk. Comme la suite $(I_n)_{n\in IN}$ est croissante, il en est de même de la suite $(J_n)_{n\in IN}$. Intéressons nous à l'idéal donné

par $I = \bigcup_{n\in IN} I_n$. C'est bien un idéal de A (Exercice!). Et l'ensemble de ses générateurs est donné par $J = \bigcup_{n\in IN} J_n$. Comme J est fini et que la suite $(J_n)_{n\in IN}$ est croissante, ceci implique que la suite $(J_n)_{n\in IN}$ est stationnaire. Mais donc, pour un certain n$\in\mathbb{N}$, J_m=J_n si m$\geq$n et I_m=I_n si m$\geq$n. La suite $(I_n)_{n\in IN}$ est bien stationnaire.

- Supposons maintenant que toute suite croissante d'idéaux de A $(I_n)_{n\in IN}$ est stationnaire. Soit $\mathcal{A}$ un sous ensemble de l'ensemble de tous les idéaux de A. Montrons que $\mathcal{A}$ possède un élément maximal pour l'inclusion. Pour cela construisons la suite d'idéaux de A suivante: Soit I un élément de $\mathcal{A}$, on pose I_0=I. Si I est le seul idéal de $\mathcal{A}$ alors on cesse notre construction et I est l'élément maximal de $\mathcal{A}$ recherché. Sinon il existe un idéal I de J dans $\mathcal{A}$ différent de I. On pose I_1=I$\cup$J. Supposons ainsi construits les n premiers termes de la suite I_k et construisons le n+1^{ieme} terme. Si il n'existe pas d'idéal dans $\mathcal{A}$ qui soit différent de I_0,...,I_n alors on pose I_{n+1}=I_n. Sinon on choisit un idéal K de $\mathcal{A}$ qui n'est pas égal à l'un des I_0,...,I_n. La suite $(I_n)_{n\in IN}$ est ainsi construite par récurrence sur n. Cette suite est, par construction, croissante, et par hypothèse, stationnaire. Il existe donc n$\in\mathbb{N}$ tel que $\forall k \in \mathbb{N}\, I_k \subset I_n$. Cela signifie qu'au rang n, on ne peut trouver d'idéal I dans $\mathcal{A}$ qui ne soit égal à un n premiers termes de la suite $(I_n)_{n\in IN}$. Cela signifie aussi que tout les idéaux de $\mathcal{A}$ sont sous ensembles de I_n et que I_n est élément maximal de $\mathcal{A}$, Cqfd.
- Montrons enfin la dernière implication. Supposons donc que toute famille d'idéaux de A possède un élément maximal et montrons que tout idéal est finiment engendré. Soit I un idéal de A. Supposons que I ne soit pas finiment engendré. Alors il existe a$\in$A tel que I_1=I+(a) est un idéal de A contenant I mais non contenu dans I. I_1 n'est pas non plus finiment engendré car si c'était le cas, il en serait de même de I. On construit de la même façon un idéal I_2=I_1+(b) où b est un élément de A tel que I_2 ne soit pas contenu dans I_1. Par récurrence on construit une suite $(I_n)_{n\in IN}$ d'idéaux de A tel que chaque idéal I_n est inclu strictement dans l'idéal I_{n+1}. Mais la suite $(I_n)_{n\in IN}$ possède, par hypothèse, un élément maximal et est donc stationnaire. Ceci est en contradiction avec le fait qu'elle soit strictement croissante. L'idéal I est donc finiment engendré.

Proposition Un anneau principal est noethérien.

Démonstration En effet, par définition, tout idéal d'un anneau principal est principal et donc engendré par un unique élément.

1.6 Homomorphismes d'anneaux et anneaux quotients

Définition Soient A et A' deux anneaux. On notera + et . leur addition et multiplication respectives sans chercher à les distinguer. De même, on notera indifféremment 1 l'élément unité de l'anneau A et celui de l'anneau A'. On dira qu'une application $f : A \longrightarrow A'$ est **un (homo)morphisme d'anneau** si:

- $\forall x,y \in A, f(x+y) = f(x) + f(y)$.

– $\forall x,y \in A, f(x.y) = f(x).f(y)$.
– $f(1) = 1$.

Remarque Les propriétés vraies pour les morphismes de groupes restent vraies pour les morphismes d'anneaux. On retrouvera de plus les mêmes objets qu'en théorie des groupes. Par exemple, un morphisme d'anneaux bijectifs sera un isomorphisme d'anneaux. Afin de ne pas alourdir cette leçon, nous épargnerons le lecteur d'une série de définitions évidentes si l'on a pris connaissance du cours de théorie des groupes.

Proposition Si f est un homomorphisme entre les anneaux A et A' alors Ker f est un idéal de l'anneau de A.

Démonstration Un homomorphisme d'anneaux étant un homomorphisme de groupe, on sait déjà que Ker f est un sous groupe de A pour la loi +. Soit maintenant un élément a de A et soit x un élément de Ker f. On a: $f(a.x) = f(a).f(x) = f(a).0 = 0$. Ainsi Ker f est un idéal à gauche. On démontrerait de même que c'est un idéal à droite et donc que c'est un idéal bilatère.

Proposition L'image d'un anneau par un homorphisme d'anneau est un sous-anneau de l'anneau d'arrivée du morphisme.

Démonstration Facile!!

Définition - Proposition Soit A un anneau et I un idéal de A. On considère la relation d'équivalence suivante: Si x,y∈A alors x∼y ⇔ x-y∈I. L'ensemble des classes d'équivalences A/∼ de cette relation d'équivalence peut être muni d'une structure d'anneau par: si $\overline{x}$ et $\overline{y}$ désignent les classes d'équivalences de x et y dans A/∼)

$$\overline{x} + \overline{y} = \overline{x + y}$$

et

$$\overline{x}.\overline{y} = \overline{x.y}.$$

L'ensemble des classes d'équivalences A/∼ sera appelé anneau quotient et sera noté A/I.

Démonstration Il faut évidemment commencer par vérifier que les lois additives et multiplicatives ainsi posées sont bien définies et qu'elles engendrent une structure d'anneau sur A/∼. La loi additive sur A étant commutative et tout idéal de A étant un sous groupe de A, on est assuré du fait que I est un sous groupe normal de A et donc que (A/∼,+) possède une structure de groupe. Considérons maintenant la loi multiplicative. Il faut vérifier que si x et x' sont dans une même classe d'équivalence et que y et y' sont dans une autre même classe d'équivalence alors $\overline{x.y} = \overline{x'.y'}$. Pour ce faire étudions la différence x.y-x'.y'. On a l'égalité: x.y-x'.y'=(x-x').y-x'(y-y'). Mais x-x' est élément de I donc, I étant un idéal bilatère, (x-x').y est élément de I. De même y'-y est élément de I et x'.(y'-y) aussi. La différence de deux éléments de I est encore un élément de I. x.x'-y.y' est donc bien un élément de I, Cqfd. On vérifie ensuite sans peine que la loi multiplicative complète la loi additive de A/I en engendrant une structure d'anneau sur cet anneau.

Théorème (**Théorème d'isomorphisme pour les anneaux**) Soient A et A' des anneaux, soit f un morphisme d'anneau de A dans A'. A/Ker f est un anneau isomorphe à l'anneau f(A). De plus, cet isomorphisme est donné par l'application $\overline{f}$ définie par

$$\overline{f} \circ \Pi(x) = f(x)$$

où Π désigne la projection Π:A$\rightarrow$A/Ker f x $\rightarrow \overline{x}$.

Démonstration A et A' étant des groupes additifs et f étant aussi un homomorphisme entre groupes additifs, le premier théorème d'isomorphisme nous assure de l'existence d'une application $\overline{f}$ définissant un isomorphisme de groupe entre A/Ker f et f(A). Reste à voir que cet isomorphisme est un isomorphisme d'anneaux. Pour cela, il faut vérifier que $\overline{f}(\overline{x}.\overline{y}) = \overline{f}(\overline{x}).\overline{f}(\overline{y})$. Mais si l'on se souvient que f est un morphisme d'anneau ainsi que la définition de $\overline{f}$, cela devient évident.

Notation Si P est une partie de l'anneau A, on notera $\overline{P}$ l'ensemble des classes d'équivalence des éléments de P.

Proposition fondamentale On a une bijection entre les idéaux de A/I et les idéaux de A contenant I via l'application:

$$\Pi : \{ ideaux\ de\ A\ contenant\ I\} \rightarrow \{ideaux\ de\ A/I\}$$

$$J \rightarrow \Pi(J) = \overline{J}.$$

Démonstration Remarquons que Π est bien définie et qu'à un idéal de A contenant I, elle associe bien un idéal de A/I.
Soit M un idéal de A/I. Montrons que Π^{-1}(M) est un idéal de A contenant I.
Tout d'abord Π^{-1}(M) est un idéal de A: si x et y $\in \Pi^{-1}$(M), l'élément x-y de A vérifie Π(x-y)=$\overline{x}$-$\overline{y}$ qui est élément de M. Ceci nous permet d'affirmer que x-y$\in \Pi^{-1}$(M). De plus comme $\overline{0}$ est élément de l'idéal M, 0 est élément de Π^{-1}(M). Ainsi Π^{-1}(M) a une structure de groupe additif.
Soit maintenant un élément m de Π^{-1}(M) et un élément a de A. Montrons que a.m est élément de Π^{-1}(M). Il suffit pour cela de remarquer que Π(a.m)=Π(a).Π(m)=$\overline{a}.\overline{m}$ qui est élément de M car M est un idéal de A/I. Ainsi Π^{-1}(M) a une structure d'idéal à gauche. On montrerait de même que Π^{-1}(M) a une structure d'idéal à droite et donc que c'est un idéal bilatère.
Remarquons que Π^{-1}(M) est un idéal de A contenant I. En effet, comme M est un idéal de A/I, il contient l'élément nul de A/I, et donc Π^{-1}(M) contient Π^{-1}(0)=I.
Cette étude de Π^{-1}(M) pour un idéal M de A/I nous permet d'être assuré du fait que l'application Π^{-1} est bien définie de l'ensemble des idéaux de A/I dans l'ensemble des idéaux de A qui contiennent I.
De plus si M est un idéal de A/I, $\Pi(\Pi^{-1}$(M))=M et si K est un idéal de A contenant I, $\Pi^{-1}(\Pi$(K))=K. L'application Π est donc une bijection, Cqfd.

Proposition Soit A un anneau et I un idéal de A. La bijection Π qui à un idéal J de A contenant I associe l'idéal $\overline{J}$ de A/I respecte l'inclusion (J_1, J_2 sont des idéaux de A contenant I et J_1', J_2' sont des idéaux de A/I):

$$J_1 \subset J_2 \Rightarrow \Pi(J_1) \subset \Pi(J_2)$$

et

$$J_1' \subset J_2' \Rightarrow \Pi^{-1}(J_1') \subset \Pi^{-1}(J_2').$$

Démonstration C'est évident!!

Voyons maintenant comment les propriétés de l'anneau passent à l'anneau quotient.

Proposition Soit A un anneau et I un idéal de A.
- Si A est commutatif, il en est de même de A/I.
- Si A est unitaire, A/I est aussi unitaire.

Démonstration
- Supposons que A est commutatif et reprenons la définition de la multiplication de A/I. Cela donne:
$$\overline{x}.\overline{y} = \overline{x.y} = \overline{y.x} = \overline{y}.\overline{x}$$
.
- Supposons maintenant que A est unitaire. Considérons aussi l'élément $\overline{1}$ de A/I. Montrons que cet élément est le neutre de la multiplication de l'anneau quotient. Il faut vérifier ici que pour tout $\overline{x}$ de A/I, $\overline{x}.\overline{1} = \overline{1}.\overline{x} = \overline{x}$. Mais à nouveau en écrivant
$$\overline{x}.\overline{1} = \overline{x.1} = \overline{1.x} = \overline{1}.\overline{x} = \overline{1.x} = \overline{x},$$
on obtient l'égalité voulue.

Proposition Si I est un idéal dans un anneau A, on a l'équivalence suivante: I est un idéal premier $\Leftrightarrow$ A/I est intègre.

Démonstration Supposons que I est premier alors I n'est pas égal à A tout entier et donc A/I n'est pas réduit à $\{0\}$. De plus si $\overline{x}$ et $\overline{y}$ sont des éléments de A/I tels que $\overline{x}.\overline{y} = 0$ alors cela implique que x.y est élément de I et, I étant premier, que x ou y est élément de I ce qui se traduit encore par $\overline{x} = 0$ ou $\overline{y} = 0$, Cqfd.
Réciproquement si A/I est intègre alors A/I n'est pas réduit à l'élément nul de l'anneau et I n'est pas égal à l'anneau tout entier. Si x et y sont éléments de A et que x.y est élément de I alors $\overline{x}.\overline{y} = 0$ et comme A/I est intègre, soit $\overline{x} = 0$, soit $\overline{y} = 0$, ce qui implique que soit x$\in$I, soit y$\in$ I et I est bien un idéal premier.

Proposition Si A est un anneau noethérien et que I est un idéal de A alors A/I est aussi un anneau noethérien.

Démonstration Supposons que A est un anneau noethérien. Soit $(I_n)_{n\in IN}$ une suite croissante d'idéaux de A/I. Soit aussi la suite $(\Pi^{-1}(I_n))_{n\in IN}$ où Π désigne la bijection qui à un idéal de A contenant I associe un idéal de A/I. $(\Pi^{-1}(I_n))_{n\in IN}$ est encore une suite croissante d'idéaux de A. Cette suite est donc stationnaire. Mais il en est alors de même de la suite $(\Pi(\Pi^{-1}(I_n)))_{n\in IN}$=$(I_n)_{n\in IN}$. L'anneau A/I est donc noethérien.

La propriété qui suit est bien agréable quand on fait de l'arithmétique.

Théorème Soit A un anneau et I un idéal de A: I est maximal $\Leftrightarrow$ A/I est un corps.

Démonstration Rappellons nous tout d'abord qu'un anneau est un corps si et seulement si ses seuls idéaux sont l'idéal nul et l'anneau tout entier.
Supposons que I est un idéal maximal de A. Les idéaux de A/I sont en bijection avec les idéaux de A contenant I. Les seul idéaux de A contenant I sont A et I lui même. Donc les seuls idéaux de A/I sont A/I et l'idéal nul. A/I est donc un corps.
Réciproquement si A/I est un corps, ses seuls idéaux sont l'idéal nul et A/I tout entier. Les idéaux de A contenant I ne peuvent donc être que I et l'anneau tout entier. Ceci prouve que I est maximal dans A/I.

Voici, pour terminer, une jolie application de la notion d'anneau quotient:

Proposition Soit A un anneau. Si I est un idéal maximal de A alors I est aussi un idéal premier.

Démonstration Supposons que I soit un idéal maximal de A. Alors A/I est un corps. Mais tout corps est intègre. Donc A/I est intègre. Cela est équivalent au fait que I est premier dans A.

Corollaire Tout idéal dans un anneau est inclu dans un idéal premier (et maximal).

Démonstration Le théorème de Krull permet d'affirmer que tout idéal I d'un anneau A est inclu dans un idéal maximal I'. Tout idéal maximal étant premier, la proposition est démontrée.

Chapitre 2

Anneaux factoriels, Anneaux euclidiens

Par Emmanuel Vieillard Baron

2.1 Introduction

Les anneaux factoriels sont des anneaux dans lesquels les éléments s'écrivent comme des produits d'"éléments de base". Une bonne connaissance du comportement de ces éléments de base permettra une bonne compréhension de l'anneau. Donnons tout de suite un exemple: $\mathbb{Z}$ est un anneau factoriel et ses "éléments de base" sont les nombres premiers. Comme on le verra, la notion de factorialité est plutôt lourde à exprimer et à mettre en évidence. On préfèrera toujours, mais ce n'est malheureusement pas toujours possible, travailler dans des anneaux euclidiens, qui sont des anneaux munis d'une division euclidienne, et qui sont factoriels.
On ne s'interessera ici qu'à des anneaux commutatifs.

2.2 Anneaux factoriels

Définition Soit A un anneau. Soient a et b des éléments de A. On dira que **a divise b** (et on notera a|b) si il existe un élément c de A tel que b=a.c.

Proposition Soient A un anneau, a et b des éléments de A. Si a divise b alors $(b)\subset(a)$.
Démonstration Supposons qu'il existe $c\in A$ tel que b=a.c. Soit x un élément de (b). Alors il existe y dans A tel que x=b.y. Donc x=y.c.a et donc $x\in(a)$. (Rappelons que les anneaux considérés ici sont supposés commutatifs.)

Proposition Définissons la relation $\mathcal{R}$ sur l'anneau A par $a\mathcal{R}b\Leftrightarrow a|b$. $\mathcal{R}$ est transitive et réflexive.
Démonstration On vérifie facilement que si a|b et b|c alors a|c. On vérifie aussi sans

trop de peine que a|a !

Proposition Soit un anneau A, soient a et b des éléments de A et soit $\mathcal{R}$ la relation définie précédemment alors: a$\mathcal{R}$ b $\Leftrightarrow$ (b)$\subset$(a).
Démonstration C'est juste la réécriture de la propriété précédente.

Définition On notera A^* l'ensemble des éléments inversibles d'un anneau A.

Proposition Soit A un anneau intègre et unitaire, soient deux éléments a et b de cet anneau. On a: (a)=(b) $\Leftrightarrow \exists u \in A^*$ a=ub.

Démonstration Supposons que (a)=(b). Si a est nul, b aussi et la propriété est démontrée. Supposons donc que a n'est pas nul. Alors il existe u$\in$A tel que a=u.b et u'$\in$A tel que b=u'.a. En particulier a=u.u'.a, ou encore: a(1-u.u')=0. Comme a n'est pas nul et que l'anneau est intègre, cela implique que 1-u.u'=0 ou encore que u.u'=1. u est donc élément de A^*.
Supposons maintenant qu'il existe un élément u de A^* tel que a=ub. Cette égalité permet d'affirmer que b divise a et donc que (a)$\subset$(b). Comme u est inversible, on a: b=u^{-1}.a ce qui signifie que a divise b et que (b)$\subset$(a), Cqfd.

Définition Dans le cas ou a et b sont éléments d'un anneau unitaire A et qu'il existe un élément u de A^* tel que a=u.b, on dira que a et b sont des éléments **associés** de l'anneau.

Définition Soit p un élément d'un anneau A intègre. p est **irréductible** si il vérifie:
- p$\notin A^*$.
- si il existe a et b$\in$A tels que p=a.b alors a$\in A^*$ ou b$\in A^*$.

On notera $\mathcal{P}$ l'ensemble des éléments irréductibles de A.

Proposition (p) est maximal $\Rightarrow$ p est irréductible.

Démonstration Supposons que p ne soit pas irréductible. Alors on peut trouver un diviseur a de p qui ne soit pas un élément inversible. Donc (p)$\subset$(a) et (p) n'est pas maximal.

Proposition Si A est un anneau principal alors: (p) est maximal $\Leftrightarrow$ p est irréductible.

Démonstration Il s'agit donc de démontrer la réciproque dans le cas où les idéaux de l'anneau sont tous de la forme (a) avec a$\in$A. Supposons que (p) ne soit pas maximal. On peut trouver un idéal I=(a) de A tel que (p)$\subset$I=(a). Mais a est alors un diviseur de p. Ceci implique que a est ou inversible ou associé à p. Si a est associé à p, (a)=(p). Si a est inversible alors (a)=A. Dans les deux cas, (a) n'est pas un idéal de A contenant (p) autre que A ou (p). Cela prouve la maximalité de (p).

Proposition Soit A un anneau intègre et soit p un élément de A. Supposons que l'idéal (p) est un idéal premier de A. Alors p est un élément irréductible de A.

Démonstration Soient a et b dans A tels que p= a.b. Alors a.b est élément de (p).

L'idéal (p) étant premier cela implique que a ou b est élément de (p). Supposons que a∈(p). Alors il existe c∈A tel que a=p.c. On peut écrire: p=p.c.b. Soit encore: p(1-cb)=0. Comme A est intègre, on en déduit que cb=1 et donc que b∈A^*. Ceci démontre l'irréductibilité de p.

Définition Deux éléments a et b d'un anneau intègre A sont dits **premiers entre eux** si ils vérifient: $\forall c \in$A c|a et c|b$\Rightarrow$ c∈A^*.

Définition n éléments a_1,...,a_n d'un anneau intègre sont dits premiers entre eux si ils vérifient: $\forall c \in$A c| a_1,...,c| a_n $\Rightarrow$ c∈A^*.

Définition Soit A un anneau. A est dit **factoriel** si il vérifie chacune des 3 propriétés suivantes:

- P_1: A est intègre.
- P_2: Tout élément x non nul de A s'écrit x=u.p_1. ... . p_n avec u∈A^* et p_i irréductibles dans A pour i=1,...,n.
- P_3 La décomposition précédente, à permutation près des éléments irréductibles et à produit par un inversible près, est unique.

Voila une définition équivalente à la précédente:

Proposition - **définition** A est factoriel si et seulement si:

- P_1: A est intègre.
- P'$_2$: Tout élément x de A s'écrit

$$x = \prod_{p \in \mathcal{P}} p^{v_p(x)}.$$

- P'$_3$: On a unicité de l'écriture précédente.

Les entiers v_p(x) sont appelés **valuation p-adique** de x.

Démonstration Il est évident que les propriétés P_2 et P'$_2$ sont équivalentes. L'unicité de ces deux écritures modulos les remarques faites dans les définitions sont elles aussi équivalentes.

Proposition Si a et b sont des éléments d'un même anneau factoriel alors a|b est équivalent à v_p(a)$\leq$$v_p$(b) $\forall$ p $\in \mathcal{P}$.

Nous allons énoncer maintenant deux lemmes qui sont équivalent, d'une certaine façon, à l'unicité d'écriture de la décomposition des éléments de l'anneau. Ces deux lemmes servent de pierres angulaires à l'arithmétique.

Théorème Soit A un anneau intègre et vérifiant la propriété P_2. On a équivalence entre:

1. A vérifie P_3.
2. Le **lemme d'Euclide**: Si p est irréductible et si p divise ab alors p divise a ou p divise b.

3. p irréductible $\Leftrightarrow$ (p) est premier.
4. Le **lemme de Gauss**: Si c est premier avec a et que c divise ab alors c divise b.

Démonstration Commençons par rappeler que dans un anneau intègre, il est toujours vrai que si (p) est un idéal premier alors p est irréductible. Supposons alors que 2 est vrai et démontrons que p irréductible $\Rightarrow$ (p) est premier. Soit a et b des éléments de A tels que ab$\in$(p). On sait donc que p|ab. Le lemme d'Euclide permet d'affirmer que p divise a ou que p divise b. Donc que a ou b est élément de (p), Cqfd.

Montrons aussi que 3 $\Rightarrow$2. Supposons pour cela que 3 est vrai. Soit p un élément irréductible de A et soient a et b$\in$A tels que p|ab. ab est alors élément de (p). Cet idéal étant premier, a ou b,nécessairement, est élément de (p). Donc p|a ou p|b. Cela implique le lemme d'Euclide.

On a donc démontré 2$\Leftrightarrow$3.

Montrons maintenant que 1$\Rightarrow$2. Supposons dons que A vérifie P'$_3$ (qui est équivalent à P_2). Soit x un élément irréductible de A et soient a,b$\in$A tels que x|ab. Il suffit de démontrer que v_x(a)$\geq$1 ou que v_x(b)$\geq$1. Comme les propriétés P'$_2$ et P'$_3$ sont, par hypothèse, vérifiées, on peut écrire:

$$ab = u \prod_{p\in\mathcal{P}} p^{v_p(a.b)} = u \prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)}.$$

x divise ce produit, donc v_x(ab)$\geq$1. Mais pour tout p$\in\mathcal{P}$, v_p(ab)=v_p(a)+v_p(b). Donc v_x(a)+v_x(b)$\geq$1. v_x(a) et v_x(b) étant des entiers positifs, cela implique que soit v_x(a)$\geq$1, soit v_x(b)$\geq$1. C'est à dire, soit x divise a, soit x divise b. Ceci permet de vérifier le lemme d'Euclide.

Montrons que 2$\Rightarrow$1. Si l'anneau A vérifie le lemme d'Euclide, et si a$\in$A,montrons qu'on a une unique décomposition de a en produit d'éléments irréductibles. Supposons que

$$a = u \prod_{p\in\mathcal{P}} p^{v_p(a)} = u' \prod_{p\in\mathcal{P}} p^{v'_p(a)}.$$

Nous devons montré que v_p(a)=v'$_p$(a) pour tout p$\in\mathcal{P}$. Soit p$\in\mathcal{P}$ tel que v_p(a)$\geq$1. p est donc un diviseur de a. Il divise par conséquent le produit

$$a = u' \prod_{p\in\mathcal{P}} p^{v'_p(a)}$$

Comme p est premier avec tout les p'$\in\mathcal{P}$ qui sont différents de p, il est nécessaire que v'$_p$(a)$\geq$1. En répétant ce raisonnement sur

$$a = \prod_{q\in\mathcal{P},q\neq p} q^{v_q(a)}.p^{v_p(a)-i}$$

et sur

$$a = \prod_{q\in\mathcal{P},q\neq p} q^{v'_q(a)}.p^{v'_p(a)-i}$$

pour i=1,...,v_p(a), on démontre que v_p(a)$\geq$v'$_p$(a). De même on démontrerait que v'$_p$(a) $\geq$ v_p(a). On a alors établis que v_p(a)=v'$_p$(a). Cela est vrai pour tout p$\in \mathcal{P}$. L'unicité de la décomposition en éléments irréductibles est donc assurée.

Intéressons nous à 4$\Rightarrow$2. Supposons que sur l'anneau A, le lemme de Gauss soit vérifié. Soit p un élément irréductible de A. Soient a,b$\in$A tels que p|ab. Si p n'est pas premier avec a alors, comme p est irréductible, p divise a, Cqfd (comme p et a ne sont pas premiers entre eux, il existe d un élément de A tel que d divise a et d divise p. Mais comme p est irréductible, cet élément d est soit inversible soit égal à p. Si il est inversible alors p et a sont premiers entre eux. cet élément d est donc égal à p et p divise bien a). Sinon p est premier avec a et d'après le lemme de Gauss, p divise b.

Cette dernière implication permet de terminer la démonstration de l'équivalence des quatres points du théorème.

Proposition Si A est un anneau intègre et noethérien alors A vérifie P_2.

Démonstration Considérons l'ensemble $\mathcal{F}$ des idéaux de A de la forme (a) ou a est un élément de A qui n'a pas de décomposition de la forme u.p_1. ... . p_r où u$\in A^*$ et où $p_i \in \mathcal{P}$ pour i=1,...,r. On suppose que $\mathcal{F}$ est non vide. Comme A est noethérien, $\mathcal{F}$ possède un élément maximal (x) pour l'inclusion. Pour tout (a)$\in \mathcal{F}$, (a)$\subset$(x). Si x était irréductible alors (x) ne serait pas élément de $\mathcal{F}$. Donc on peut écrire x sous la forme x=ab avec a,b$\in$A et a,b non inversibles. Mais a et b ne peuvent, en même temps, possèder une décomposition en élément irréductible de la forme u.p_1. ... . p_r car sinon il en serait de même de leur produit et donc de x. (a) ou (b) est donc élément de$\mathcal{F}$. Supposons que (a) est élément de $\mathcal{F}$, on peut écrire (x)$\subset$(a). Ceci est en contradiction avec la maximalité de (x). Par conséquent $\mathcal{F}$ est vide et tout élément de A possède une décomposition en facteurs irréductibles.

Proposition Si A est un anneau principal alors A est factoriel.

Démonstration Si A est principal il est noéthérien et intègre. On peut alors lui appliquer la propriété précédente et conclure.

2.3 Pgcd, Ppcm, Théorème de Bezout

Définition - Proposition Soit A un anneau factoriel. Si on considère deux éléments a et b de A, on peut trouver des éléments c et d de A tels que:

- (c) soit le plus grand idéal principal de A (au sens de l'inclusion) tel que (c)$\subset$(a) et (c)$\subset$(b).
- (d) est le plus petit idéal principal de A (au sens de l'inclusion) tel que (a)$\subset$(d) et (b)$\subset$(d).

c est le **plus petit commun multiple** (ppcm) de a et b.
d est le **plus grand commun diviseur** (pgcd) de a et b.
On notera de plus d=a$\wedge$b.

Démonstration Il suffit de considérer pour c:

$$c = \prod_{p \in \mathcal{P}} p^{sup(v_p(a), v_p(b))}$$

et pour d:

$$d = \prod_{p \in \mathcal{P}} p^{inf(v_p(a), v_p(b))}.$$

Proposition Soit A un anneau principal et soient a,b$\in$A$\backslash\{0\}$. Soit c=ppcm(a,b) et d=a$\wedge$b. c et d vérifient les égalités:

$$(c) = (a) \cap (b)$$

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

Démonstration Soit x un élément de (c) alors c|x. Comme a|c et que b|c, a|x et b|x. Mais x est alors élément de (a) et de (b) donc de (a)$\cap$(b). De plus, (a)$\cap$(b) est un idéal de A contenu dans (a) et (b). Comme (c) est le plus grand idéal de A vérifiant cette propriété, (a)$\cap$(b) est contenu dans (c), d'où l'inclusion réciproque.
Soit x un élément de (a)+(b). Alors il existe des éléments k et k' de A tels que x=ka+k'b. Mais d divise a et b donc d divise une combinaison linéaire de leur somme et d divise donc x. x est alors élément de (d). Donc (a)+(b)$\subset$(d). De plus (a)$\subset$(a)+(b) et (b)$\subset$(a)+(b). (a)+(b) est donc un idéal de A qui contient (a) et (b). Il est par définition de (d) contenu dans (d). Donc (d)=(a)+(b).

Théorème de Bezout A est un anneau principal. Alors a et b sont des éléments de A premiers entre eux si et seulement si il existe u et v dans A tels que au+bv=1.
Démonstration Supposons que a et b sont premiers entre eux, a$\wedge$b=1. On en déduit que (a)+(b)=A. En particulier, il existe u et v dans A tels que au+bv=1. Réciproquement si il existe u et v tel que au+bv=1, alors si d est un élément de A qui divise à la fois a et b, il existe a' et b' dans A tels que a=d.a' et b=d.b'. Mis dans l'égalité précédente, cela donne: d(a'.u+b'.v)=1. Cette égalité signifie que d est inversible et donc élément de A^*. a et b sont donc bien premiers entre eux.

Définition De la même façon que l'on a défini le pgcd de deux éléments d'un anneau principal A, on peut définir le pgcd de n éléments a_1,...,a_n de cet anneau: c'est le générateur du plus petit idéal de A qui contient chacun des idéaux (a_i).

Définition On peut encore définir le ppcm de n éléments a_1,...,a_n d'un anneau principal en affirmant que c'est le générateur du plus grand idéal de A qui est contenu dans chacun des (a_i).

Proposition de Bezout généralisée Soit A un anneau principal. Soient a_1,...,a_n des éléments de A. On a équivalence entre a_1,...,a_n sont premiers entre eux et pgcd(a_1,...,a_n)=1.

Démonstration La démonstration est absolument l'analogue de celle faite pour le théorème de Bezout précédent.

2.4 Anneaux Euclidiens

La difficulté pour définir une division sur un anneau est que l'anneau considéré n'est pas forçément un ensemble ordonné (Pensez par exemple aux anneaux polynomiaux). C'est pour cela qu'il nous faut recourir à une fonction qui nous permettra de "plonger" les éléments de notre anneau dans $\mathbb{N}$ qui lui est ordonné.

Définition Soit A un anneau. On dit que A est muni d'**une division Euclidienne** si il existe une application u:$A\backslash 0 \to \mathbb{N}$ telle que si a et b sont éléments de $A\backslash 0$ alors il existe q et r $\in$A vérifiant a=bq+r et r=0 ou u(r)<u(b).

Remarquons que cette application u est dans le cas des anneaux polynômiaux l'application qui à un polynôme associe son degré.

Définition Un anneau A est **Euclidien** si:
- A est intègre.
- A possède une division Euclidienne.

Proposition Un anneau Euclidien est principal.

Démonstration Soit A un anneau Euclidien. A est par définition intègre. Soit I un idéal de A et soit u l'application de A dans $\mathbb{N}$ permettant de définir une division euclidienne sur A. Soit x un élément de I tel que u(x) soit minimal. Alors pour tout a dans I, il existe q et r dans A tels que a=xq+r. De plus soit r est nul soit il vérifie u(r)<u(x). Remarquons que x étant élément de I, il en est de même de xq. De plus, comme a-xq est aussi élément de I, r est élément de I. L'inégalité u(r)<u(b) est donc, par choix de x, impossible. Nécessairement, r=0 et a=qx. Comme a est quelconque dans I, I=(x). A est par conséquent principal.

Chapitre 3

Anneaux polynomiaux

Par Emmanuel Vieillard Baron

3.1 Introduction

Les polynômes sont parmi les fonctions les plus accessibles en Mathématiques et parmi aussi les plus riches et les plus intéressantes. L'étude des polynômes est à cheval entre l'analyse et l'algèbre et leur utilité est autant importante dans ces deux parties des mathématiques. Une façon d'illustrer cette idée est de rappeler que le théorème communément appelé **théorème fondamental de l'algèbre**, qui est un théorème sur les polynômes à coefficients réels, ne possède aucune démonstration qui ne recourt pas à l'analyse. Les polynômes seront souvent utilisés en algèbre sous forme d'équation. De nombreux problèmes algébriques se ramènent à la résolution d'une équation polynomiale. Nous pensons à des problèmes d'arithmétiques, par exemple, comme les équations diophantiennes. Nous pensons aussi à la recherche des valeurs propres pour les matrices. En analyse, ils serviront à approximer les fonctions. Citons par exemple le théorème de Weierstrass qui affirme que les polynômes définis sur un compact de $\mathbb{R}$ forment une famille dense dans l'ensemble des fonctions continues définies elles aussi sur ce compact pour la topologie de la convergence uniforme. Cette leçon n'étudiera que le côté algébrique des polynômes. On étudiera ici les liens, en particulier, entre les propriétés de l'anneau sur lequel les polynômes sont définis et les propriétés de l'anneau polynomial. Une leçon du cours d'analyse s'occupera de leur autre visage.

3.2 Qui sont-ils?

Définition Soit A un anneau. On appelle **polynôme** sur A ou à coefficient dans A toute application P vérifiant:

- P:A$\rightarrow$A.
- Il existe n$\in\mathbb{N}$ et a_0,...,a_n dans A tels que $\forall$ x$\in$A, P(x)=a_0+a_1X+...+$a_n X^n$.

Les éléments a_i de P sont appelés **les coefficients** de P.
$a_i X^i$ est **le terme de degré i** de P.
a_i est **le coefficient du terme de degré i**.

L'ensemble des polynômes sur A est noté A[X].

Remarque Le polynôme nul est le polynôme ayant comme coefficient pour le terme de degré i l'élément nul de A et ce pour tout i dans $\mathbb{N}$.

Remarquons que pour tout n$\in\mathbb{N}$, le polynôme P possède un terme de degré n. Dans le pire des cas, ce terme est nul.

Définition Un polynôme P de la forme P(X)=aX^k est appelé **un monôme de degré k**.

Définition Soit A un anneau. Soient P et Q des polynômes sur A définis par :

$$P(X) = \sum_{i=0}^{n} a_i x^i$$

et

$$Q(X) = \sum_{i=0}^{m} b_i X^i.$$

On définit la somme de P et Q comme étant le polynôme noté P+Q et dont le terme d'ordre i a pour coefficient a_i+b_i
On définit aussi le produit des deux polynômes P et Q par le polynôme que l'on note PQ ou P.Q et dont le coefficient du terme de degré i vaut $\sum_{k=0}^{i} a_k.b_{i-k}$.

Proposition Soit A un anneau. L'ensemble A[X] des polynômes définit sur A muni de la multiplication et de l'addition précédemment définies possède une structure d'anneau.

Démonstration C'est facile à vérifier mais un peu long à écrire dans un traitement de texte.

3.3 Racines d'un polynôme

Définition Soit α $\in$A et soit P$\in$A[X]. α est **une racine** de P si et seulement si P(α)=0.

Avant toute chose, nous allons énonçer et démontrer ce petit lemme qui semble bien anodin:

Lemme Soit A un anneau et soit P un élément de A[X]. Soit aussi α $\in$A. On peut alors trouver des éléments b_0,...,b_n $\in$A tels que P s'écrive:

$$P(X) = \sum_{i=0}^{n} b_i (X - \alpha)^i.$$

Démonstration P s'écrit:

$$P(X) = \sum_{i=0}^{n} a_i X^i.$$

Posons t=X+α. Alors

$$P(X) = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} a_i (X - \alpha + \alpha)^i = \sum_{i=0}^{n} a_i ((X - \alpha) + \alpha)^i.$$

La formule du binôme donne, pour tout i=0,...,n:

$$((X - \alpha) + \alpha)^i = \sum_{k=0}^{i} C_i^k (X - \alpha)^k \alpha^{i-k}.$$

P(X) est donc de la forme:

$$P(X) = \sum_{i=0}^{n} \sum_{k=0}^{i} c_k (X - \alpha)^k$$

où les c_k sont éléments de A. On peut encore, en réunissant dans cette expression de P(X), les termes (X-α) de même puissance, écrire P(X) sous la forme:

$$P(X) = \sum_{i=0}^{n} b_i (X - \alpha)^i$$

où les b_i sont éléments de A.

Proposition Soit A un anneau et P un élément de A[X]. Si $\alpha \in$A est une racine de P alors il existe un polynôme Q de A[X] tel que $P(X) = (X - \alpha)Q(X)$.

Démonstration On suppose que P s'écrit

$$P(X) = \sum_{i=0}^{n} a_i X^i.$$

On utilise le lemme fraichement démontré: On peut trouver des coefficients b_i dans A tel que P s'écrive:

$$P(X) = \sum_{i=0}^{n} b_i (X - \alpha)^i.$$

Comme α est une racine de P, P(α)=0 et donc le coefficient b_0 est nul. P s'écrit donc:

$$P(X) = b_1(X - \alpha) + b_2(X - \alpha)^2 + ... + b_n(X - \alpha)^n.$$

On peut mettre, dans cette expression, (X-α) en facteur. Cela donne:

$$P(X) = (X - \alpha)(b_1 + b_2(X - \alpha) + ... + b_n(X - \alpha)^{n-1}).$$

Le polynôme Q(X) est alors tout trouvé et la proposition est démontrée.

Définition Soit α une racine d'un polynôme P définit sur un anneau A. Le plus grand entier n tel que $(X-\alpha)^n$ divise P est appelé la **multiplicité** de α dans P. Si n=1, on dit que α est une **racine simple** de P.

Proposition Soit A un anneau et P un élément de A[X]. On suppose que P s'écrit

$$P(X)=\sum_{i=0}^{n} a_i x^i$$

où les $a_i \in$A et où les a_i ne sont pas tous nuls. Alors P a au plus n racines dans A.

Démonstration Montrons la propriété par récurrence. Si n=1, P ressemble à un polynôme du type aX+b. Il est clair que P a au plus une racine dans A. Supposons le résultat vrai à l'ordre n-1.Supposons aussi que P a plus de n racines dans A. Soient alors α_1,...,α_{n+1} n+1 racines distinctes de P. Appliquons la proposition précédente à $\alpha=\alpha_1$. Il existe un polynôme Q1 de A[X] tel que P s'écrive P(X)=(X-α_1)Q1(X). Notons que Q1(X) a une écriture de la forme $b_1+b_2X+...+b_nX^{n-1}$ où les b_i sont éléments de A. Mais P(α_i) est nul pour tout i=2,...,n+1. Q a donc plus de n-1 racines. On peut appliquer notre hypothèse de récurrence et donc affirmer que l'on a aboutit à une contradiction. P ne peut avoir plus de n racines.

Proposition Soit A un anneau possédant **un nombre infini d'éléments** et P un polynôme sur A. Alors P est égal au polynôme nul si et seulement si tous ses coefficients sont nuls.

Démonstration Si tous les coefficients de P sont nuls alors P est égal au polynôme nul. Réciproquement si P est identiquement nul, alors P a plus de n racines et ce quelque soit n dans $\mathbb{N}$ (car A possède un nombre infini d'éléments). La seule possibilité pour P est, d'après la proposition précédente, d'avoir tous ses coefficients nuls.

Corollaire Soient P et Q des polynômes définis sur un anneau A possédant une infinité d'éléments. On suppose que

$$P(X)=\sum_{i=0}^{n} a_i X^i$$

et que

$$Q(X)=\sum_{i=0}^{m} b_i X^i.$$

Si P et Q sont égaux en tout point de A alors P et Q ont la même écriture polynomiale: n=m et $\forall$ i=0,...,n a_i=b_i.

Démonstration Il suffit d'appliquer le résultat précédent à P-Q: ce polynôme est nul donc ces coefficients sont nuls. Ceci implique l'égalité entre les coefficients de P et ceux de Q.

On vient de démontrer un résultat plus important qu'il n'y paraît. En effet, on vient de prouver qu'une fonction polynomiale n'a qu'une écriture possible sous la forme

$$\sum_{i=0}^{n} a_i X^i.$$

En particulier, le plus grand entier n tel que $a_n \neq 0$ est uniquement déterminé. Cet entier n s'appelle le degré du polynôme.

Définition Soit P un polynôme non nul de la forme

$$P(X) = \sum_{i=0}^{n} a_i X^i.$$

Le plus grand entier n tel que $a_n \neq 0$ est appelé **le degré du polynôme P**. On notera: deg(P) ou deg P le degré de P. Si P est le polynôme nul, on convient que deg(P)=-∞.

Définition Soit P un polynôme de degré n. Le coefficient du monôme de degré n est appelé **coefficient dominant** de P.

Définition Si le coefficient dominant d'un polynôme est 1 alors on dit que le polynôme est **unitaire**. (1 désigne l'unité de l'anneau sur lequel le polynôme est défini).

La notion de degré d'un polynôme va permettre de travailler sur les anneaux polynomiaux et d'en fixer les propriétés.

Remarque On suppose pour tout ce qui suit que les anneaux utilisés ont une infinité d'éléments.

3.4 Quelques propriétés des anneaux polynomiaux

Convention: Afin de rendre valide la propriété suivante, on supposera les règles d'additions suivantes:

$$-\infty + -\infty = -\infty, \ -\infty + n = -\infty.$$

Proposition Soit A un anneau **intègre** et P,Q deux polynômes sur A. Alors:

$$deg(P.Q) = deg(P) + deg(Q).$$

Démonstration On suppose tout d'abord que les deux polynômes, P et Q sont non nuls. On peut écrire

$$P(X) = \sum_{i=0}^{n} a_i X^i$$

et

$$Q(X) = \sum_{i=0}^{m} b_i X^i.$$

où n=deg(P) et où m=deg(Q). P.Q s'écrit alors:

$$(P.Q)(X) = \sum_{i=0}^{n+m} \sum_{k=0}^{i} a_k.b_{i-k}X^i.$$

Remarquons que le monôme de degré n.m a pour coefficient $a_n.b_m$. Les deux facteurs de ce produit ne sont pas nuls (autrement P et Q ne seraient pas du degré supposé), l'anneau étant intègre, le produit n'est donc pas nul et donc le degré de P.Q est bien n+m. Si P ou (et) Q est (sont) nul(s), la convention précédente nous permet de vérifier là encore la formule sur le degré.

Voici une application directe de cette formule.

Proposition Soit A un anneau intègre. Alors A[X] est aussi un anneau intègre.

Démonstration Soient P et Q des éléments de A[X]. On suppose que P.Q=0. La formule précédente qui est vraie dès que l'anneau est intègre nous permet d'écrire: deg(P)+deg(Q)=-∞. Ceci n'est possible que si deg(P) ou deg(Q)=-∞ et donc que si P ou Q est nul. A[X] est bien intègre.

Voici une autre application de cette formule

Proposition Si A est un anneau intègre et que P est un élément inversible de A[X] alors P est en fait élément de A^*.

Démonstration P est inversible dans A[X]. On peut donc trouver Q∈A[x] tel que P.Q=1. On peut alors écrire: 0=deg(P.Q)=deg(P)+deg(Q). Ceci implique que deg(P) = deg(Q) = 0. P et Q sont donc éléments de A. Comme P.Q=1, ils sont aussi éléments de A^*

Grâce à la notion de degré d'un polynôme, nous allons pouvoir définir une division Euclidienne sur les anneaux polynomiaux. Rappelons que l'existence de cette division était conditionnée par l'existence d'une application de A[X]$\backslash\{0\}$ $\rightarrow\mathbb{N}$. Cette application sera bien évidemment l'application qui à un polynôme de A[X]$\backslash\{0\}$ associe son degré. Cette division ne sera par contre définie que pour les polynômes de coefficient dominant inversible.

Proposition Soit A un anneau intègre et soit P un élément non nul de A[X]. On suppose de plus que P est de coefficient dominant inversible. Soit L un autre élément de A[X]. Il existe Q et R dans A[X] tels que:

- L=P.Q+R.
- deg R <deg P ou R=0.

Démonstration Comme le coefficient dominant de P est inversible, on peut supposer (quitte à multiplier P par l'inverse de son coefficient dominant) que P est unitaire.Notons:

$$P = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$$

Etudions l'image de L dans l'anneau quotient A[X]/(P). (Rappelons que (P) désigne l'idéal engendré par P). Si la classe d'équivalence de L dans ce quotient a pour repré-

sentant un polynôme de degré plus petit que deg P ou a pour représentant le polynôme nul, c'est gagné car (si on note M le représentant recherché), il existe Q dans A[X] tel que L-M=Q.P et on a obtenu le résultat escompté. Si L est un polynôme de degré plus petit que deg P ou est le polynôme nul, alors le représentant est tout trouvé: c'est L. Sinon, la classe d'équivalence de P dans A[X]/(P) admet le polynôme nul comme représentant. L'égalité suivante est donc vraie dans le quotient:

$$x^n = a_0 + a_1 x + ... + a_{n-1} x^{n-1}.$$

Cette égalité nous permet d'écrire le monôme x^n ainsi que tous les monômes de la forme x^{n+i}, i>0 en fonction des monômes 1,x,...,x^{n-1}. Dans A[X]/(P), le polynôme L est donc égal à un polynôme ne s'écrivant qu'avec des monômes de degré strictement plus petit que deg P. On a ainsi trouvé un représentant de la classe de L dans A[X]/(P) comme voulu. Cela démontre notre proposition.

Corollaire Si k est un corps, k[X] muni de la division définie via la fonction degré est un anneau Euclidien.

Démonstration Les éléments de k[X] ont leur coefficient dominant (et les autres...) qui sont éléments de k et qui sont donc inversibles. On peut alors leur appliquer la proposition précédente.

3.5 Propriétés de A passants sur A[X]

Proposition Si A est un anneau noethérien alors A[X] est aussi noethérien.

Démonstration Supposons que A est noethérien. Considérons, pour n donné dans $\mathbb{N}$, et I un idéal de A[X], l'ensemble $d_n(I)$ qui est la réunion de l'ensemble des coefficients dominants des polynômes de degré n de I et du sous ensemble de A constitué de l'élément nul. On montre sans problème que $d_n(I)$ est un idéal de A. De plus:

- Pour tout n dans $\mathbb{N}$, si $I \subset J$ alors $d_n(I) \subset d_n(J)$.
- Pour tout n dans $\mathbb{N}$, $d_n(I) \subset d_{n+1}(J)$.
- Si $I \subset J$, on a équivalence entre I=J et $\forall n \in \mathbb{N}$ $d_n(I)=d_n(J)$.

La première propriété est évidente. Pour la seconde, il suffit de remarquer que si a_n est le coefficient dominant du polynôme P de degré n de I, alors X.P est encore un polynôme de I de coefficient dominant a_n mais de degré n+1. La troisième propriété est un peu plus difficile à établir. Le sens direct ne pose pas de problème. Supposons que $I \subset J$ et que $\forall n \in \mathbb{N}$ $d_n(I)=d_n(J)$. Supposons aussi qu'il existe des polynômes de J qui ne soient pas éléments de I. Soit $P \neq 0$ un polynôme de degré minimal vérifiant cette propriété. Soit n le degré de P et a_n son coefficient dominant. Par hypothèse, a_n est aussi élément de $d_n(I)$. Soit alors Q un élément de I de degré n ayant a_n comme coefficient dominant. Comme $I \subset J$, et que J est un idéal, P-Q est élément de J. Mais P-Q n'est pas élément de I car sinon il en serait de même de P. Cependant P-Q est un polynôme de degré plus petit que celui de P et qui vérifie la propriété de ne pas appartenir à I. Notre hypothèse de départ est donc fausse. Par conséquent I=J.
Nous sommes maintenant en mesure de démontrer que A[X] est noethérien.
Soit $(I_n)_{n \in \mathbb{N}}$ une suite croissante d'idéaux de A. L'ensemble des idéaux de la forme $d_n(I_k)$ pour $n,k \in \mathbb{N}$ possède, comme A est noethérien un élément maximal que l'on

note $d_m(I_l)$. D'autre part pour tout k≤m la suite $d_k(I_n)$ est croissante relativement à n. Donc pour tout k≤m, on peut trouver $n_k \in \mathbb{N}$ tel que $d_k(I_{n_k})$ soit élément maximal de cette suite. Choisissons pour j l'élément maximal de la famille constituée de l et de n_1,...,n_m.
On va montrer que $\forall i \geq j$ I_i=I_j.
Remarquons que, comme on a l'inclusion $I_j \subset I_i$, il suffit de démontrer que $d_n(I_j)$=$d_n(I_i)$ pour tout n∈$\mathbb{N}$ .Mais:
si p<m,alors $d_p(I_i)$=$d_p(I_{n_p})$=$d_p(I_j)$.
si p≤m, $d_p(I_i)$=$d_p(I_j)$. L'égalité est ainsi établie, Cqfd.

Proposition Soit A un anneau. A[X] est principal si et seulement si A est un corps.

Démonstration Si A est un corps, alors tout polynôme de A[X] a son coefficient dominant inversible. La division Euclidienne est donc définie sur A[X]. De plus si A est un corps, alors A est intègre et A[X] aussi. A[X] est donc Euclidien. Mais tout anneau Euclidien est principal.
Supposons maintenant que A[X] est principal. A est nécessairement intègre. La notion de degré d'un polynôme de A[X] est donc correctement définie. Si le polynôme P(X)=X n'était pas irréductible, il aurait une décomposition de la forme M.N où M et N sont des éléments de A[X]. Mais deg(M).deg(N)=1. Ce qui n'est possible que si, par exemple, M est de degré nul dans A[X] et N de degré 1. M s'écrit donc N(X)=a où a∈A et N(X)=b.X. Mais M.N=X implique que a.b=1. M est donc un élément invesible de A. P est alors nécessairement irréductible. Rappelons qu'un anneau principal est factoriel. On a donc équivalence entre X est irréductible et (X) (= l'idéal engendré par X dans A[X]) est un idéal premier dans A[X]. Ceci, associer à la principalité de A[X] permet d'affirmer que (X) est un idéal maximal dans A[X]. Par conséquent A[X]/(X) est un corps. Mais A[X]/(X)≃A, donc A est un corps.

3.6 Petite étude des éléments irréductibles dans A[X]

Définition Soit A un anneau factoriel. Soit P un polynôme de A[X]. On suppose que P s'écrit

$$P = a_0 + a_1 x + ... + a_{n-1} x^{n-1} + a_n x^n.$$

Le **contenu** de P est l'élément de A que l'on note c(P) et qui est égal au pgcd(a_0,...,a_n).

Définition Un polynôme est dit **primitif** si son contenu vaut 1.

Lemme Soit A un anneau factoriel. Soient P et Q des éléments de A[X]. L'égalité suivante est vraie dans A/A^*:

$$c(P.Q) = c(P).c(Q).$$

Démonstration Démontrons déjà cette égalité dans le cas où P et Q sont primitifs. Il suffit en fait de démontrer que le contenu de P.Q vaut 1. C'est à dire que si le pgcd des coefficients de P et Q est 1 modulo un élément de A^*, alors il en est de même pour celui des coefficients de P.Q. Si a_l désignent les coefficients de P et b_m ceux de q, les

coefficients de P.Q sont de la forme: $\sum_{k=0}^{i} a_k.b_{i-k}$ pour i allant de 0 à deg P + deg Q. Soit d un diviseur de c(PQ). Comme A est factoriel, on peut supposer que d est irréductible. d divise donc les quantités $\sum_{k=0}^{i} a_k.b_{i-k}$ pour tout i allant de 0 à deg P+deg Q. Comme c(P)=1 et c(Q)=1, on peut trouver k_1 et k_2 tels que d|$a_k \forall k$<k_1 et d|$b_k \forall k$<k_2 mais d ne divise ni a_{k_1} ni b_{k_2}. Comme d|c(PQ), d divise en particulier le coefficient du terme de degré k_1+k_2

$$a_0 b_{k_1+k_2} + ... + a_{k_1+k_2} b_0$$

de PQ. Remarquons que d|$a_i b_{k_1+k_2-i} \forall$i=0,...,$k_1$+$k_2$ sauf si i=k_1 (car d'après le lemme d'Euclide, si un irréductible divise un produit, il divise nécessairement un des facteurs du produit). d ne peut diviser le coefficient d'ordre k_1+k_2 de PQ. Ce qui est en contradiction avec notre hypothèse de départ. Donc c(PQ)=1.
Si c(P)$\neq$1 ou c(Q)$\neq$l, alors P s'écrit P=c(P).P' où P' est un élément de A[X] vérifiant c(P')=1 et Q s'écrit Q=c(Q).Q' où Q' vérifie c(Q')=1. Clairement, c(PQ) = c((c(P).c(Q).P'.Q') = c(P).c(Q)c(P'.Q') = c(P).c(Q).

Proposition A est un anneau factoriel. K est le corps des fractions de A. Les polynômes irréductibles dans A[X] sont:

- Les polynômes de degré 0 (qui sont des éléments de A) qui sont irréductibles dans A.
- Les polynômes de degré $\geq$1 primitifs et irréductibles dans K[X] où K désigne le corps des fractions de A..

Démonstration Commençons par montrer que ces éléments sont bels et bien des irréductibles. Soit a un élément irréductible de A. Supposons qu'il existe P,Q$\in$A[X] tels que a=P.Q. Comme A est factoriel, il est intègre. La notion de degré d'un polynôme de k[X] est donc bien définie. Mais deg(P.Q)=deg(P)+deg(Q). Ceci implique que deg(P)=deg(Q)=0. P et Q sont donc des éléments de A. Comme a est irréductible dans A, soit P est inversible dans A et donc dans A[X], soit Q est inversible dans A (et donc aussi dans A[X]). a est bien irréductible dans A[X].
Supposons que R est un polynôme de degré $\geq$1 de A[X] primitif et irréductible dans K[X]. Supposons qu'il existe P,Q$\in$A[X] tels que R=P.Q. Cette égalité est encore vraie dans K[X]. Donc P ou Q est un élément inversible de k[X]. On en déduit que P ou Q est élément de K. Supposons que Q est élément de K. Q est donc aussi élément de A. Re-nommons alors Q par q. Comme A est factoriel, l'égalité R=q.P nous permet d'affirmer que q divise c(R). Mais c(R)=1. q est donc un élément de A^* et R est bien irréductible dans A[X].
Montrons maintenant que ce sont les seuls irréductibles. Soit R un élément irréductible de A[X]. Si deg(R)=0 alors R est clairement un irréductible de A. Sinon, deg(R)>0. Il est nécessaire que c(R)=1. Reste à voir que R est aussi irréductible dans K[X]. Supposons qu'il existe P et Q dans K[X] tels que R=P.Q. P et Q peuvent se re-écrire sous la forme : P=$\frac{a_1}{b_1}$P' Q=$\frac{a_2}{b_2}$Q' où P' et Q' sont des éléments de A[X] et où a_i,b_i, i=1,2 sont des éléments de A. On peut de plus supposer que les contenus respectifs de P' et Q'

sont égaux à 1. En effet, si par exemple P s'écrit:

$$P = \sum_{i=0}^{n} \frac{c_i}{d_i} X^i,$$

en prenant pour d le ppcm des d_0,...,d_n, P peut être mis sous la forme

$$P = \sum_{i=0}^{n} \frac{c'_i}{d} X^i.$$

Prenant maintenant pour c le pgcd des c'_0,...,c'_n, P s'écrit

$$P = c.\sum_{i=0}^{n} \frac{c''_i}{d} X^i$$

et si l'on prend pour P': $P' = \sum_{i=0}^{n} \frac{c''_i}{d} X^i$, on a bien c(P')=1. R s'écrit alors: R=$\frac{a}{b}$P'.Q' où a=$a_1.a_2$ et où b=$b_1.b_2$ e où c(P')=c(Q')=1. Cela conduit à l'égalité b.R=a.P'.Q'. Cette dernière égalité entraîne l'égalité b=b.c(R)=a.c(P').c(Q')=a. Donc R=P'.Q'. Comme R est irréductible, on peut supposer, par exemple, que P'est élément de A^*. P est alors un élément de K^* et R est bien irréductible dans K[X].

Théorème de Gauss Si A est un anneau factoriel alors A[X] est factoriel.

Démonstration Rappelons que si A est intègre il en est de même de A[X]. Rappelons aussi que les inversibles de A[X] sont les éléments de A^*: $A[X]^*=A^*$. Ajoutons encore que si K est un corps, K[X] est principal et que si K[X] est principal, K[X] est factoriel. K désignera ici le corps des fractions de A.
Prouvons pour commencer l'existence d'une décomposition en facteurs irréductibles pour tout élément de A[X]. Soit P∈A[X] que l'on suppose primitif. Comme K[X] est factoriel, on peut trouver des polynômes P1,...Pr irréductibles dans K[X] tels que P=$P1^{\alpha_1}$. ... . Pr^{α_r}. Les polynômes peuvent être mis sous la forme Pi=$\frac{a_i}{b_i}$P'i, comme on l'a fait dans la démonstration de la propriété précédente, avec P'i primitif dans A[X]. On obtient alors l'égalité:

$$(\prod_{i=1}^{r} b_i)P = \prod_{i=1}^{r} a_i P' i^{\alpha_i}.$$

En passant au contenu, on voit que cette égalité n'est possible que si le produit des b_i est égal à celui des a_i modulo un élément de A^*. P vérifie alors

$$P = a.\prod_{i=1}^{r} P' i^{\alpha_i}$$

où a est élément de A^*. Si P n'est pas primitif, on peut l'écrire comme produit d'un élément de A et d'un élément primitif de A[X]. Cette décomposition de P permet d'écrire ensuite celle désirée en facteurs irréductibles.
Montrons enfin l'unicité de la décomposition des éléments de P en facteurs irréductibles. Rappelons que cette unicité est équivalente au fait que si P est irréductible dans A[X] ⇔ (P) est un idéal premier de A[X]. Supposons donc que P est irréductible et montrons ue (P) est un idéal premier de A[X].

Si deg(P)=0 alors P est un irréductible de A et A étant factoriel, (P) est bien premier dans A[X].
Si deg(P)>0, remarquons que K[X] étant factoriel et P étant aussi irréductible dans K[X], (P) est premier dans K[X]. (Il faut préciser au passage que l'idéal (P) dans K[X] est égal à P.K[X] tandis que l'idéal (P) dans A[X] est égal à P.A[X]). Cela est équivalent à l'intégrité de K[X]/(P). Considérons l'application i:A[X]/(P)→K[X]/(P) qui à la classe d'équivalence dans A[X]/(P) d'un polynôme R de A[X] associe sa classe d'équivalence dans K[X]/(P). i est clairement un morphisme d'anneau. Si de plus i est injective, l'intégrité de K[X]/(P) passe sur A[X]/(P). Et cela démontrerait la primalité de (P) dans A[X]. Montrons donc que i est injective. Pour montrer qu'un morphisme est injectif, il suffit de démontrer que son noyau est réduit à 0. Soit Q un polynôme de A[X]. Soit $\overline{Q}$ sa classe d'équivalence dans A[X]/(P). Supposons que i($\overline{Q}$)=0. Cela revient à supposer que Q est élément de l'idéal engendré par P.K[X]. Montrons que Q est alors aussi élément de P.A[X]. Cela établira en effet l'égalité $\overline{Q}$=0. Comme Q est élément de P.K[X], il existe R dans K[X] tel que Q=P.R. Q peut s'écrire d.Q' où Q' est primitif et où d∈A. On peut écrire, comme déjà fait dans la démonstration précédente R sous la forme $\frac{a}{b}$.R' où R' est un élément primitif de A[X] et où a,b∈A. On peut de plus supposer que a et b sont premiers entre eux. On obtient l'égalité suivante: b.d.Q'=a.R.Q. En passant au contenu, on voit que b divise a. Donc b=a dans A/A^*. Autrement dit Q=uP.R' où u∈A et où Q'∈A[X], Cqfd.

Chapitre 4

Quelques Thèmes sur les anneaux commutatifs

Par Sigfried Rouzes

4.1 Introduction

Voici une succession de quelques thèmes sur les anneaux commutatifs unitaires.

4.2 Idéaux premiers

Proposition Soit A un anneau commutatif et unitaire; soient a un idéal de A, n un entier non nul et b_1,...,b_n des idéaux premiers de A. Alors on a:

$$a \subset \bigcup_{1\leq i\leq n} b_i \Rightarrow \exists k \in \{1,...,n\}/a \subset b_k.$$

Démonstration Montrons cette propriété par récurrence sur n :
Pour n=1, c'est clair. Supposons la propriété vraie jusqu'à l'ordre n (n$\geq$1), soient a un idéal de A et b_1,...,b_n,b_{n+1} des idéaux premiers avec $a \subset \bigcup_{1\leq i\leq n+1} b_i$.

- 1er cas : il existe i$\neq$j dans $\{1,...,n+1\}$ tels que $b_i \subset b_j$. Cela implique qu'il existe une sous partie $\{b'_i\}_{1\leq i\leq n} \subset \{b_i\}_{1\leq i\leq n+1}$ avec $\bigcup_{1\leq i\leq n} b'_i = \bigcup_{1\leq i\leq n+1} b_i$, et donc la propriété est prouvée car on peut appliquer l'hypothèse de récurrence.
- 2ème cas : pour tout i$\neq$j dans $\{1,...,n+1\}$ on a $b_i \not\subset b_j$. Alors pour tout i dans $\{1,...,n+1\}$, il existe x$_i$ vérifiant :
  - x$_i \in b_i$.
  - x$_i \notin b_j$ pour tout j$\neq$i dans $\{1,...,n+1\}$.

Notons x= $\prod_{i\in\{1,...,n\}} x_i$. Il est alors clair que pour tout k tel que 1≤k≤n, x∈ b_k et que x∉ b_{n+1} (car b_{n+1} est premier).
Supposons que l'on ait $a \not\subset \bigcup_{1\leq i\leq n} b_i$ et $a \not\subset b_{n+1}$ alors il existe:

- a∈ a tel que a∉ $\bigcup_{1\leq i\leq n} b_i$ (et donc a∈ b_{n+1}).
- a'∈ a tel que a'∉ b_{n+1} (et donc a'∈ $\bigcup_{1\leq i\leq n} b_i$).

Considérons alors a"=a+xa'. Clairement, a"∈ a , donc a∈ $\bigcup_{1\leq i\leq n+1} b_i$. Soit r dans $\{1,...,n+1\}$ tel que a"∈ b_r. Si r=n+1, i.e. a"∈ b_{n+1}, alors (a"-a)∈ b_{n+1} car a∈ b_{n+1} , et donc xa'∈ b_{n+1} , ce qui est impossible car x∉ b_{n+1}, a'∉ b_{n+1} et b_{n+1} est premier. Donc on a 1≤r≤n; mais alors (a"-xa')∈ b_r car x∈ b_r , et donc a∈ b_r , ce qui est absurde. Ainsi, l'hypothèse $a \not\subset \bigcup_{1\leq i\leq n} b_i$ et $a \not\subset b_{n+1}$ est fausse ; donc, ou bien $a \subset b_{n+1}$, ce qui montre la propriété, ou bien $a \subset \bigcup_{1\leq i\leq n} b_i$, ce qui montre aussi la propriété car on peut alors appliquer l'hypothèse de récurrence.

Corollaire Soit A un anneau commutatif et unitaire; soient n≥2 un entier et $b_1,...,b_n$ des idéaux premiers de A tels que pour tout i≠j dans $\{1,...,n\}$ on ait $b_i \not\subset bj$. Alors $\bigcup_{1\leq i\leq n} b_i$ n'est pas un idéal de A.

Démonstration Supposons que $\bigcup_{1\leq i\leq n} b_i$ soit un idéal. Alors, comme $\bigcup_{1\leq i\leq n} b_i \subset \bigcup_{1\leq i\leq n} b_i$, la proposition qui précède permet de dire qu'il existe k∈ $\{1,...,n\}$ tel que $\bigcup_{1\leq i\leq n} b_i \subset b_k$. Soit alors k'∈ $\{1,...,n\}$, tel que k'≠k (Cela existe car n≥2). Alors $\bigcup_{1\leq i\leq n} b_i \subset b_k \Rightarrow b_{k'} \subset b_k$, ce qui est contraire aux hypothèses. Ainsi $\bigcup_{1\leq i\leq n} b_i$ n'est pas un idéal.

4.3 Parties multiplicatives et idéaux premiers

Définition Soit A un anneau commutatif et unitaire ; on dit qu'une partie S de A est **multiplicative** (ou **multiplicativement fermée**) si, et seulement si, 1∈S et (x,y)∈S×S⇒ xy∈S.

Exemple soit P un idéal de A. Alors par définition, P est idéal premier si, et seulement si, A\P est une partie multiplicative de A.

Proposition Soit A un anneau commutatif et unitaire; soient a un idéal de A et S une partie multiplicative de A. On suppose que a∩S=∅. Alors il existe b idéal premier

de A tel que $a \subset b$ et $b \cap S = \emptyset$.

Démonstration Soit W l'ensemble des idéaux I de A qui vérifient $a \subset I$ et $I \cap S = \emptyset$.
- W est non vide car il contient a.
- Montrons que l'ordre induit sur W par l'inclusion fait de W un ensemble inductif:
  Soit B une partie de $\mathcal{P}(W)$. B est un ensemble constitué de sous ensembles de W. On suppose que B est totalement ordonné pour l'inclusion. Soit $m = \bigcup_{f \in B} f$; clairement, m est, par construction, la borne supérieure de B ; reste à montrer que m est dans W. Soit $f \in B$, alors $f \in W$, donc $a \subset f$, et donc $a \subset m$. Supposons maintenant que $m \cap S \neq \emptyset$; alors il existe s dans S tel que $s \in \bigcup_{f \in B} f$, donc il existe $f \in B$ tel que $s \in f$, et donc $f \cap S \neq \emptyset$, ce qui est absurde. Ainsi $m \cap S = \emptyset$. m est donc dans W, et l'ordre induit sur W par l'inclusion est bien inductif.
  Comme W est non vide et que l'ordre induit sur W par l'inclusion est inductif, le lemme de Zorn nous permet d'affirmer qu'il existe dans W un élément b maximal pour cet ordre.
  Montrons que b est premier et la démonstration sera achevée.
  Tout d'abord, b est strict car $A \cap S \neq \emptyset$ ($1 \in A \cap S$) et donc $A \notin W$.
  Supposons que b ne soit pas premier. Alors, comme b est strict, cela implique qu'il existe x et x' dans $A \setminus b$ tels que $xx' \in b$. Le fait que x et x' soient hors de b implique que : $b \subset b + xA$ et que $b \subset b + x'A$. Attention ces deux inclusions sont strictes. Comme b est maximal dans W, on en déduit que $b + xA$ et $b + x'A$ sont hors de W. Comme d'autre part il est clair que $(x) \subset b + xA$ et que $(x) \subset b + x'A$, le fait que $b + xA$ et$b + x'A$ soient hors de W implique que $b + xA$ et $b + x'A$ coupent S. Ainsi, il existe s et s' dans S, b et b' dans b, et a et a' dans A tels que : s=b+xa et s'=b'+a'x' . En faisant le produit membre à membre, on obtient : ss'=bb'+x'a'b'+aa'xx'. Dans cette égalité, chacun des termes de droite est clairement dans b, donc le terme de droite est dans b, et le terme de gauche est dans S (car S est une partie multiplicative) ; ainsi $b \cap S \neq \emptyset$, ce qui est absurde.
  Ainsi l'hypothèse : b est non premier, est fausse.

4.4 Racine d'un idéal

Définition Soit A un anneau commutatif et unitaire ; soit a un idéal de A. On appelle **racine** de a, l'ensemble (noté $\sqrt{a}$) défini par :

$$\sqrt{a} = \{x \in A / \exists n \in \mathbb{N}^* / x^n \in a\}.$$

En particulier, $\sqrt{(0)}$ s'appelle le **nilradical** de A, et ses éléments s'appellent les **éléments nilpotents de l'anneau** A.

(N.B. il s'agit bien de la définition classique d'un élément nilpotent).

Proposition Soit A un anneau commutatif et unitaire; soient a et b deux idéaux de A.

1. $\sqrt{a}$ est un idéal de A, et $a \subset \sqrt{a}$.

2. $\sqrt{\sqrt{a}} = \sqrt{a}$. (i.e. une racine est un **idéal radiciel**).
3. $\sqrt{ab} = \sqrt{a \cap b}$.
4. $\sqrt{a \cap b} = \sqrt{a} \cap \sqrt{b}$.
5. $\sqrt{a}$ =A $\Rightarrow a$ =A.
6. b est un idéal premier $\Rightarrow \forall n \geq 1$, $\sqrt{b^n} = b$. (En particulier tout idéal premier est radiciel).
7. $\sqrt{a+b} = \sqrt{\sqrt{a} + \sqrt{b}}$.

Démonstration On utilise, sans les (re)démontrer les formules établies pour tout a, b de A (qui est commutatif) et m, n de $\mathbb{N}$:

- x^{m+n}=$x^m x^n$.
- $(x^m)^n$=x^{mn}.
- $(xy)^n$=$x^n y^n$.
- $(x+y)^n$=$\sum_{i=0}^{n} C_n^i x^i y^{n-i}$.

Ces formules sont valables avec la convention x^0=1 pour tout x de A.

1. Il est immédiat que $a \subset \sqrt{a}$. Montrons que $\sqrt{a}$ est un idéal de A ; soient donc x, y dans $\sqrt{a}$, et t dans A. Soient n et m dans $\mathbb{N}^*$ tels que $x^n \in a$ et $y^m \in a$; alors

$$(x+y)^n = \sum_{i=0}^{n+m} C_n^i x^i y^{n+m-i} = \sum_{i=0}^{n} C_n^i x^i y^{n+m-i} + \sum_{i=n+1}^{n+m} C_n^i x^i y^{n+m-i} =$$

$$y^m \sum_{i=0}^{n} C_n^i x^i y^{n-i} + x^n \sum_{i=n+1}^{n+m} C_n^i x^{i-n} y^{n+m-i}$$

   Par suite, $(x+y)^{n+m} \in a$, et donc (x+y)$\in \sqrt{a}$. D'autre part, $(t.x)^n = t^n x^n \in a$ donc (t.a)$\in \sqrt{a}$.
2. D'après 1. On a $\sqrt{a} \subset \sqrt{\sqrt{a}}$. Soit x$\in \sqrt{\sqrt{a}}$: il existe n dans $\mathbb{N}^*$ tel que $x^n \in \sqrt{a}$; par suite il existe m dans $\mathbb{N}^*$ tel que $(x^n)^m \in a$, i.e. $x^m \in a$, et donc x$\in \sqrt{a}$.
3. On a $ab \subset a \cap b$, donc $\sqrt{ab} \subset \sqrt{a \cap b}$. Soit x$\in \sqrt{a \cap b}$; il existe n dans $\mathbb{N}^*$ tel que $x^n \in a \cap b$. Ainsi, $x^n \in a$, $x^n \in b$, donc $(x^n x^n) \in ab$, i.e. $x^{n+n} \in ab$, et donc x$\in \sqrt{ab}$.
4. On a $a \cap b \subset a$, donc $\sqrt{a \cap b} \subset \sqrt{a}$; de même, $\sqrt{a \cap b} \subset \sqrt{b}$, donc $\sqrt{a \cap b} \subset \sqrt{a} \cap \sqrt{b}$. Soit s$\in \sqrt{a \cap b}$; il existe n et m dans $\mathbb{N}^*$ tels que $x^n \in a$ et $x^m \in b$; par suite $x^n x^m \in a$ et $x^n x^m \in b$, i.e. $x^n x^m \in a \cap b$ et x$\in \sqrt{a \cap b}$.
5. Il est clair que $\sqrt{A}$=A; Soit a tel que $\sqrt{a} = A$; alors 1$\in \sqrt{a}$, i.e. il existe n dans $\mathbb{N}^*$ tel que $1^n \in a$; donc a$\in a$, et par suite a=A.
6. Il est immédiat qu'un idéal premier est radiciel, i.e. $\sqrt{b} = b$; on montre alors la propriété par récurrence : elle est donc vrai pour n=1, et supposons que $\sqrt{b}^n = b$; Alors $\sqrt{b^{n+1}} = \sqrt{bb^n}$, et, d'après 3., $\sqrt{bb^n} = \sqrt{b \cap b^n}$, puis, d'après 4., $\sqrt{b \cap b^n} = \sqrt{b} \cap \sqrt{b^n}$; or $\sqrt{b} = b$ et $\sqrt{b^n} = b$, donc $\sqrt{b} \cap \sqrt{b^n} = b \cap b = b$; ainsi $\sqrt{b^{n+1}} = b$.

7. $a \subset \sqrt{a}$ et $b \subset \sqrt{b}$, donc $a+b \subset \sqrt{a}+\sqrt{b}$ et $\sqrt{a+b} \subset \sqrt{\sqrt{a}+\sqrt{b}}$. Soit x$\in \sqrt{\sqrt{a}+\sqrt{b}}$; il existe n dans $\mathbb{N}^*$ tel que x$^n \in \sqrt{a}+\sqrt{b}$; soient y$\in \sqrt{a}$ et z$\in \sqrt{b}$ tels que, x^n=y+z. Soient aussi r et s dans $\mathbb{N}^*$ tels que y$^r \in a$ et z$^s \in b$. Alors, par le même calcul qu'en 1., on a

$$(y+z)^{r+s} = z^s \sum_{i=0}^{r} C_{r+s}^i y^i z^{r-i} + y^r \sum_{i=r+1}^{r+s} C_{r+s}^i y^{i-s} z^{r+s-i}.$$

Par suite, (x^n)$^{r+s}$=z^{s}u+y^{r}v, i.e. x$^{n(r+s)} \in a+b$, et donc x$\in \sqrt{a+b}$.

4.5 Idéal premier et racine d'un idéal

Proposition Soit A un anneau commutatif et unitaire ; soit a un idéal strict de A. Notons $P(a)$ l'ensemble des idéaux premiers de A qui contiennent a.
Alors :

1. $P(a) \neq \emptyset$.
2. $\sqrt{a} = \bigcap_{b \in P(a)} b$.

Démonstration

1. P(a)$\neq \emptyset$: En effet, a est un idéal strict de A, donc il existe un idéal maximal m contenant a. Or m est maximal donc premier. Par suite P(a) contient m.
2. Montrons la double inclusion :
   A/: $\sqrt{a} \subset \bigcap_{b \in P(a)} b$: Soit x$\in \sqrt{a}$; il existe donc un entier n$\geq$1 tel que x$^n \in a$.
   Soit b un idéal premier contenant a. On montre aisément par récurrence que si un élément y de A n'est pas dans b, alors aucune puissance de y n'est dans b. (Car b est premier). Comme x$^n \in a$, alors x$^n \in b$, et d'après ce que l'on vient d'énoncer, on a x$\in b$. Comme ceci est vrai pour tout idéal premier contenant a, on a bien $x \in \bigcap_{b \in P(a)} b$.
   B/ $\bigcap_{b \in P(a)} b \subset \sqrt{a}$: Soit x$\in \bigcap_{b \in P(a)} b$. Supposons que x$\notin \sqrt{a}$. Soit S=$\{1,x,...,x^n,...\}$ l'ensemble des puissances de x. Alors x$\notin \sqrt{a}$ implique que $a \cap S = \emptyset$. Facilement, S est une partie multiplicative de A. Alors on sait qu'il existe un idéal d premier tel que $a \subset d$ et $d\cap$S=$\emptyset$. $a \subset d$ implique que $d \in$P(a) , et par suite x$\in d$ (puisque x$\in \bigcap_{b \in P(a)} b$). Mais d'autre part $d\cap$S=$\emptyset$ implique que x$\notin$d (puisque x$\in$S) : absurde ! Donc l'hypothèse x$\notin \sqrt{a}$ est fausse.

Corollaire Soit A un anneau commutatif et unitaire; soit x un élément de A.
Alors on a équivalence entre:

1. x est nilpotent.

2. x est élément de tout idéal premier de A.

Démonstration Soit spp(A) l'ensemble des idéaux premiers de A (le spectre premier de A). Alors la proposition précédente implique que $\sqrt{(0)}$= $\bigcap_{b\in spp(A)} b$; ce qui démontre le corollaire. (cf. exo3 pour la définition de nilpotent).

Corollaire Soit A un anneau commutatif, unitaire et intègre.
Alors l'intersection de tous les idéaux premiers de A est $\{0\}$.

Démonstration Si A est intègre, il est immédiat que le seul élément nilpotent est 0 ; autrement dit, $\sqrt{(0)} = (0)$ (i.e. l'idéal (0) est radiciel, i.e. l'anneau A est réduit). Ainsi d'après le corollaire précédent, $\bigcap_{b\in spp(A)} b$=(0).

4.6 Anneau local

Définition Soit A un anneau commutatif et unitaire ; On dit que A est un **anneau local** si, et seulement si A possède un unique idéal maximal. (Rappelons que d'après le théorème de Krull, tout anneau non nul possède toujours au moins un idéal maximal).

Exemple Un corps est un anneau local. (car son seul idéal maximal est $\{0\}$).

Proposition Soit A un anneau commutatif et unitaire ; on note N l'ensemble des éléments non inversibles de A (N n'est pas vide car il contient toujours 0). Alors les propositions suivantes sont équivalentes :

1. A est un anneau local.
2. N est un idéal de A.

Démonstration Notons tout d'abord que tout idéal strict de A est inclus dans N, puisqu'un idéal strict ne peut contenir d'inversible.

1⇒2 : Soit m l'unique idéal maximal de A. m est strict, donc $m \subset N$. Soit x$\in N$. x n'est pas inversible, donc l'idéal xA est strict ; par suite il est contenu dans un idéal maximal. Or m est l'unique idéal maximal, donc xA$\subset m$, et par suite x$\in m$: N$\subset m$.

2⇒1 : N est idéal strict car $1\notin N$. Comme il contient tout idéal strict, c'est maximum (pour l'inclusion) dans l'ensemble des idéaux stricts. Cela entraîne qu'il est idéal maximal, et unique maximal.

4.7 Anneau des fractions d'un anneau

Proposition Soient A un anneau unitaire et commutatif. Soit S une partie multiplicative de A qui ne contient pas 0. On définit sur S$\times$A deux opérations. Si a,a' sont éléments de A, s,s' sont éléments de S:

$$(s,a) + (s',a') = (ss',sa' + s'a)$$
$$(s,a).(s',a') = (ss',aa').$$

De plus, on considère la relation binaire $\mathcal{R}$ sur S×A définie par: (s,a)$\mathcal{R}$(s',a') $\Leftrightarrow$ $\exists$t$\in$S/t(sa'-s'a)=0.

Alors:

1. $\mathcal{R}$ est une relation d'équivalence ; l'ensemble des classes d'équivalence est noté $S^{-1}A$, et la classe de (s,a) est notée $\frac{a}{s}$.
2. Les deux opérations définies plus haut sont stables vis-à-vis de la relation R ; elles induisent sur $S^{-1}A$ une structure d'anneau commutatif unitaire. L'élément nul est donné par $\frac{0}{1}$ et l'unité est $\frac{1}{1}$. $S^{-1}A$ s'appelle **l'anneau des fractions** de A sur S.
3. Soit i l'application de A dans $S^{-1}A$ qui à a associe $\frac{a}{1}$. Alors i est un homomorphisme d'anneau. De plus i est injectif si, et seulement si, S ne contient aucun diviseur de 0. Si cette condition est réalisée, on pourra donc considérer A comme un sous-anneau de $S^{-1}A$.
4. $S^{-1}A$ est l'anneau nul si, et seulement si, S contient un élément nilpotent, ce qui est aussi équivalent au fait que S contient 0.

Démonstration

1. Montrons que $\mathcal{R}$ est bien une ralation d'équivalence. Tout d'abord (s,a) $\mathcal{R}$ (s,a) car sa-as=0. Donc $\mathcal{R}$ esr réflexive. Ensuite, il est clair que si (s,a)$\mathcal{R}$(s',a') alors (s',a')$\mathcal{R}$(s,a). $\mathcal{R}$ est donc symétrique. Reste à montrer la transitivité: Pour cela prenons (s,a), (s',a') et (s",a") des éléments de S×A tels que (s,a)$\mathcal{R}$(s',a') et (s',a')$\mathcal{R}$(s",a"). Il existe donc t et t' dans S tels que t(sa'-s'a)=0 et t'(s'a"-a's")=0. Alors tt's'(sa"-s"a)=tst's'a"-tt's's"a=tt'sa's"-tt's's"a=t's"t(a's-s'a)=0. Donc (a,s)$\mathcal{R}$(a",s"). $\mathcal{R}$ est bien une relation d'équivalence.
2. Montrons que les deux opérations sont compatibles avec la relation d'équivalence. Si (a,b), (a',b'), (c,d) et (c',d') sont des éléments de S×A, tels que (a,b)$\mathcal{R}$(a',b') et (c,d)$\mathcal{R}$(c',d'), il faut montrer d'une part que (a,b)+(c,d) $\mathcal{R}$ a',b')+(c',d') et d'autre part que (a,b)(c,d)=(a',b')(c',d'). Montrons d'abord la compatibilité par rapport à l'addition. Comme (a,b)$\mathcal{R}$(a',b'), il existe t$\in$S tel que t(ab'-a'b)=0. Comme (c,d)$\mathcal{R}$(c',d') il existe t'$\in$S tel que t'(cd'-c'd)=0.Nous cherchons un élément T de S tel que T[ac(a'd'+b'c')-a'c'(ad+bc)]=0. Soit T tel que T[(ab'-a'b)cc'+(cd'-c'd)aa']=0. Si on prend T=tt' cela donne l'égalité voulue. Montrons la compatibilité par rapport à la multiplication. On a tt'(acb'd'-bda'c')=tt'(ab'cd'-a'bdc')=tt'(a'bcd'-a'bdc')=tt'a'b(cd'-d'c')=0, Cqfd.
3. Soit i:A $\longrightarrow$ $S^{-1}A$ a$\longrightarrow$ i(a)=$\frac{a}{1}$. Vérifions tout d'abord que i est un homomorphisme d'anneaux. Tout d'abord: si x,y $\in$A, i(x+y)=$\frac{x+y}{1}$=$\frac{x}{1}$+$\frac{y}{1}$. i est donc un morphisme de groupes additifs. D'autre part i(xy)=$\frac{xy}{1}$=$\frac{x}{1}\frac{y}{1}$=i(x)i(y). De plus i(1)=$\frac{1}{1}$. i est donc bien un homomorphisme d'anneaux. D'autre part i est injectif si et seulement si son noyau se réduit à l'élément nul de A. Soit donc x$\in$Ker i. Si i(x)=0 cela est équivalent au fait que $\frac{x}{1}$=0. Cela revient à dire qu'il existe s dans S tel que sx=0. Cette dernière affirmation est équivalente à l'existence d'un diviseur s de 0 dans A.

4. Supposons que $S^{-1}A=\{0\}$ alors $\forall a\in A\ \exists s\in S/sa=0$. En particulier $s^2=0$. Ainsi S contient un élément nilpolent. Ensuite si S contient un élément nilpotent, $s^n=0$. 0 est donc élément de S. Enfin si 0 est élément de S, $S^{-1}A=\{0\}$ car pour tout a de A, 0a=0. Donc $a=\frac{0}{1}$.

Définition - Proposition Soit A un anneau commutatif unitaire. A est une partie miltiplicative de A. Considérons $\mathcal{A}=(A\setminus\{0\})^{-1}A=A\setminus\{0\}\times A/\mathcal{R}$ (où $\mathcal{R}$ est la relation d'équivalence précédemment définie) muni de l'addition et de la multiplication précédemment définie a une strucuture de corps. C'est le **corps des fractions de l'anneau A**. Les classes d'équivalcences des couples (b,a) sont notés $\frac{a}{b}$. L'injection canonique $i:A\longrightarrow\mathcal{A}$ définie par $i(x)=\frac{x}{1}$ permet de voir A comme un sous anneau de $\mathcal{A}$.

Démonstration Par construction, tout élément de $\mathcal{A}$ est inversible dans $\mathcal{A}$. Ce dernier, qui au départ possède une structure d'anneau, possède donc une structure de corps.

4.8 Produit de sous parties d'un anneau

Proposition Soit A un anneau commutatif et unitaire , soient X et Y deux parties non vides de A, et a un idéal de A.
Par définition, XY est l'ensemble des éléments z de A du type :

$$z=\sum_{1\leq i\leq n}x_iy_i$$

où n est un entier naturel non nul, et où pour tout $i\in\{1,...,n\}$ $x_i\in X$ et $y_i\in Y$.

Alors :

1. Xa est un idéal.
2. En particulier, XA est le plus petit idéal de A contenant X ; de plus, X est un idéal si et seulement si X=XA . XA est appelé idéal engendré par X.
3. Soit B un anneau commutatif unitaire et f un homomorphisme d'anneaux de A dans B. Soit b un idéal de B ; alors $f^{-1}(b)$ est un idéal de A. Si de plus f est surjective, alors f(a)=f(a)B et par suite f(a) est un idéal de B.

Démonstration

1. Montrons que si X est une partie de A et si a est un idéal de A alors Xa est un idéal de A. Il suffit pour cela de remarquer que si x,x'∈X et si a,a'∈A alors xa-xa'=xa+x(-a'). Comme a' est élément de a, il en est de même de -a'. Compte tenu de l'écriture des éléments de Xa, cette somme est bien élément de Xa. En refaisant ce raisonnement sur une somme du type $\sum_{1\leq i\leq n}x_ia_i$ où $x_i\in X$ et $a_i\in A$, on démontre que Xa est un sous groupe de A. D'autre part si α est élément de A et si $z\sum_{1\leq i\leq n}x_ia_i$ est élément de Xa, alors $\alpha z=\sum_{1\leq i\leq n}x_i(\alpha a_i)$ qui est encore élément de Xa. Xa est bien un idéal de A.

2. XA est clairement un idéal et si un idéal contient X, il contient nécessairement XA. XA est donc le plus petit idéal contenant X. De plus si X est un idéal, alors, A étant unitaire, X est contenu dans XA. Comme XA est le plus petit idéal contenant A, XA=X. Réciproquement si X=XA alors XA étant un idéal de A, il en est de même de X.
3. Soit B un anneau commutatif unitaire. Soit f:A$\longrightarrow$B un morphisme d'anneaux. Soit aussi b un idéal de B. Utilisons le critère que l'on vient de montrer pour prouver que $f^{-1}(b)$ est un idéal de A. Il faut dont montrer que $f^{-1}(b)$A=$f^{-1}(b)$. Mais $f(f^{-1}(b))$=bf(A)=b car b est un idéal de B. $f^{-1}(b)$ est bien un idéal de A. De plus, si f est surjective et si a est un idéal de A, $f(a)$=$f(aA)$=$f(a)f(A)$=$f(a)$B donc $f(a)$=$f(a)$B

Proposition Soient A un anneau commutatif unitaire , S une partie multiplicative de A, a un idéal de A et i l'homomorphisme canonique de A dans $S^{-1}A$.
Alors :

$$i(a)S^{-1}A = \{\frac{x}{s}; x \in a;\ s \in S\}.$$

D'autre part, si b est un idéal de $S^{-1}A$, alors:

$$b = i(i^{-1}(b))S^{-1}A.$$

Chapitre 5

THEME: une démonstration du théorème de Wedderburn.

Par Sigfried Rouzes

5.1 Introduction

Avant d'énoncer le théorème de Wedderburn, il faut effectuer une petite précision lexicale. La loi multiplicative d'un corps est généralement toujours supposée commutative. Ce ne sera pas le cas ici et on appellera corps un ensemble K muni de deux lois + et . telles que (K,+) ait une structure de groupe abélien et telles que (K\{0},.) ait une structure de groupe non nécessairement abélien. On dira alors qu'un corps est **commutatif** *si sa multiplication est commutative.*
Rappelons aussi qu'un corps est dit fini si son cardinal est fini.

Théorème de Wedderburn Tout corps fini est commutatif.

Afin d'établir la démonstration de ce théorème, il faut procéder à quelques rappels sur les racines de l'unité.

5.2 Racines de l'unité

Notons C le cercle trigonométrique, i.e.

$$C = \{z \in \mathbb{C} \ / \ |z| = 1\} = \left\{e^{i\theta} \ ; \ \theta \in \mathbb{R}\right\} = \left\{e^{i\theta} \ ; \ \theta \in [0\,;\,2\pi[\right\}.$$

Pour tout entier $n \geq 1$, on note R_n l'ensemble des racines n-ièmes de l'unité, à savoir

$$R_n = \{z \in \mathbb{C} \ / \ z^n = 1\}.$$

Bien sûr, $R_n \subset C$ et

$$R_n = \left\{e^{i\frac{2k\pi}{n}} \ ; \ k \in \{1, \cdots, n\}\right\}.$$

Ainsi, $card\,(R_n) = n$. Rappelons que R_n a une structure de groupe multiplicatif.

Définition On appelle **ensemble des racines entières de l'unité** l'ensemble $R = \bigcup_{n\geq 1} R_n$ où R_n désigne l'ensemble des racines n-ièmes de l'unité.

Proposition A toute racine entière de l'unité z, on peut associer l'idéal des entiers i tels que $z^i = 1$; cet idéal est non nul et son unique générateur strictement positif est le rang de z, noté ici $\rho\,(z)$.

Ainsi on a : $z \in R_n \;\Leftrightarrow\; \rho\,(z) \mid n$.

Démonstration Soit z une racine entière de l'unité. Il existe $n \in \mathbb{N}$ tel que $z^n = 1$. Par conséquent, l'ensemble $\mathcal{I}$ des entiers i tels que $z^i = 1$ est non vide. On vérifie facilement que c'est un idéal de $\mathbb{Z}$. Ce dernier étant principal, $\mathcal{I}$ est aussi principal et donc monogène. Ceci permet d'être assuré que $\rho\,(z)$ est bien défini.

Rappelons aussi que, par définition, un élément de R est une racine primitive d$^{\text{ièmes}}$ de l'unité si et seulement si c'est un générateur de R_d. Enonçons la propriété:

Proposition Soit $d \geq 1$ un entier. Soit F_d désigne l'ensemble des racines primitives d$^{\text{ièmes}}$ de l'unité. Soit z une racine entière de l'unité et soit $\rho(z)$ son rang alors:

$$F_d = \{z \in R \;\; / \;\; \rho\,(z) = d\}.$$

On a, plus précisément,

$$F_d = \left\{ e^{i\frac{2k\pi}{d}} \;;\; k \in \{1, \cdots, d\} \; et \; k \wedge d = 1 \right\}$$

où $k \wedge d$ désigne le pgcd de k et d.

Démonstration

- Démontrons l'inclusion de F_d dans $\{z \in R \;\; / \;\; \rho\,(z) = d\}$. Soit $z \in F_d$. z est donc un générateur de R_d. Rappelons que R_d est un groupe cyclique à d éléments. Par conséquent, pour tout élément $z' \neq 1$ de R_d, il existe $0 \leq i < d$ tel que $z' = z^i$ et $z^d = 1$. On a ainsi montré que $\rho(z) = 1$ et donc l'inclusion demandée. Démontrons l'inclusion réciproque. Soit z une racine entière de l'unité de rang d. Le sous groupe de R engendré par z est un sous groupe cyclique de R d'ordre d. Ce sous groupe contient alors toutes les racines du polynômes $X^d - 1 = 0$ car pour chaque élément z' de ce sous groupe, $z'^d = 1$. Ce sous groupe est par conséquent le groupe des racines d-ième de l'unité et z est bien un générateur de ce groupe.
- Montrons la seconde égalité. Soit z un élément de F_d. z est une racine entière de l'unité, donc il existe k et $n \in \mathbb{N}$ tels que $z = e^{i\frac{2k\pi}{n}}$. Comme $z^d = 1$, n est un diviseur de d. En particulier n≤d. Mais $z^n = 1$ donc n est élément de l'idéal engendré par d et donc $n \geq d$. En conclusion $n = d$ et $z = e^{i\frac{2k\pi}{d}}$. Montrons maintenant que $k \wedge d$=1. Si ce n'est pas le cas alors il existe un élément p de $\mathbb{N}$ tel que d=k.p et p<d. Mais $z^p = 1$, et le rang de z ne peut être d. Ceci est contraire à nos hypothèses. Donc forcément $k \wedge d = 1$. Pour démontrer l'inclusion réciproque, choisissons un élément $z = e^{i\frac{2k\pi}{d}}$ tel que $k \in \{1,...,d\}$ et tel que $k \wedge d = 1$. Montron que le rang m de cette racine entière de l'unité est égal à d. Il est évident que m est au plus égal à d. Supposons que m<d. Alors

$z^m = 1$ implique $e^{i\frac{2k.m\pi}{d}} = 1$. Donc d divise k.m, mais comme d est premier avec k, en vertu du lemme de Gauss, d divise m ce qui est contraire au choix fait pour m. Donc d=m et z est de rang d. Par conséquent, comme les éléments de rang d sont les racines primitives d-ièmes de l'unité, l'inclusion réciproque est prouvée.

Définition Soit F_d l'ensemble des racines primitives d[ièmes] de l'unité. Le polynôme

$$\Phi_d(X) = \prod_{z \in F_d} (X - z)$$

est appelé **d[ièmes] polynôme cyclotomique**.

Etablissons maintenant quelques propriétés préalables à la démonstration du théorème de Weddenburn.

5.3 Propriétés préléminaires

Proposition (P1) Soient K un corps commutatif, $A \subset K$ un sous-anneau de K et $\Phi \in K[X]$. S'il existe un polynôme $Q \in A[X]$ unitaire tel que $\Phi.Q \in A[X]$, alors $\Phi \in A[X]$.

Démonstration Cette propriété se démontre assez simplement par récurrence sur $d^\circ\Phi$; néanmoins nous préférons une preuve plus " élégante ".

Notons $P = \Phi.Q \in A[X]$. Comme $Q \in A[X]$ est unitaire, il existe une unique division euclidienne de P par Q dans $A[X]$, i.e. il existe un unique couple (Q_1,R_1)de $A[X]^2$ tel que $P = Q_1Q + R_1$ et $d^\circ R_1 < d^\circ Q$.

D'autre part, K étant un corps, il existe une unique division euclidienne de P par Q dans $K[X]$, i.e. il existe un unique couple (Q_2,R_2)de $K[X]^2$ tel que $P = Q_2Q + R_2$ et $d^\circ R_2 < d^\circ Q$.

Comme $(Q_1,R_1) \in A[X]^2$ et que A est sous-anneau de K, on a $(Q_1,R_1) \in K[X]^2$; alors l'unicité du couple de division euclidienne de P par Q dans $K[X]$ implique que $(Q_1,R_1) = (Q_2,R_2)$.

Enfin, comme $P = \Phi.Q$, cette même unicité implique : $(Q_2,R_2) = (\Phi,0)$.

On a donc $(Q_1,R_1) = (\Phi,0)$, donc $\Phi = Q_1$, i.e. $\Phi \in A[X]$.

Proposition (P2) Soient L un corps fini, $K \subset L$ un sous-corps de L. Alors il existe $s \in IN^*$ tel que $card(L) = (card(K))^s$.

Démonstration

L'opération de $K \times L$ dans L définie par $k * l = kl$ (le produit dans L) induit sur L une structure de K-espace vectoriel. L est fini, donc de dimension finie s, et on a bien classiquement $card(L) = (card(K))^s$.

Proposition (P3) Soient m et n deux entiers avec $1 \leq m \leq n$, $T \in \mathbb{Z}(X)$ la fraction rationnelle définie par : $T(X) = \frac{X^n-1}{X^m-1}$, et Φ_n le n-ième polynôme cyclotomique.

Alors on a:

1. $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$;
2. $\Phi_n \in \mathbb{Z}[X]$;
3. $m \mid n \Rightarrow T \in \mathbb{Z}[X]$;
4. $m \mid n \ et \ m < n \Rightarrow$ Φ_n divise le polynôme T dans $\mathbb{Z}[X]$.

Démonstration

1. Rappelons que l'ensemble des racines primitives d[ièmes] de l'unité F_d vérifie

$$F_d = \left\{ e^{i\frac{2k\pi}{d}} \ ; \ k \in \{1, \cdots, d\} \ et \ k \wedge d = 1 \right\}.$$

Un corollaire immédiat de cette égalité est, φ étant la fonction indicatrice d'Euler ($\varphi(d) = card\{k \in \{1,...,d\}, k \wedge d = 1\}$), $card(F_d) = \varphi(d)$.
D'autre part, l'ensemble des définitions implique aisément que $\{F_d\}_{d \mid n}$ forme une partition de R_n ; cela donne deux résultats intéressants :

$$card(R_n) = \sum_{d \mid n} card(F_d),$$

i.e.

$$n = \sum_{d \mid n} \varphi(d);$$

Identité des polynômes

$$\prod_{z \in R_n} (X - z) \text{ et } \prod_{d \mid n} \prod_{z \in F_d} (X - z).$$

En notant

$$\Phi_d(X) = \prod_{z \in F_d} (X - z),$$

le d-ième polynôme cyclotomique, et en développant $\prod_{z \in R_n} (X - z)$, cette identité donne :

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

Ceci est le 1/ de la propriété.

2. $\Phi_n \in \mathbb{Z}[X]$; montrons-le par récurrence sur n :
Pour $n = 1$, $\Phi_1(X) = X - 1$, donc $\Phi_1 \in \mathbb{Z}[X]$.
Supposons démontré jusqu'à n ; on a

$$X^{n+1} - 1 = \prod_{d \mid n+1} \Phi_d(X),$$

ce qui entraîne que

$$X^{n+1} - 1 = \Phi_{n+1}(X) \cdot \prod_{\substack{d \mid n+1 \\ d \leq n}} \Phi_d(X).$$

La récurrence s'applique aux Φ_d avec $d \leq n$, et donc le polynôme

$$\prod_{\substack{d \mid n+1 \\ d \leq n}} \Phi_d(X)$$

appartient à $\mathbb{Z}[X]$. De plus il est clairement unitaire, et comme $\left(X^{n+1}-1\right) \in \mathbb{Z}[X]$, la propriété (P1) nous dit que $\Phi_{n+1} \in \mathbb{Z}[X]$: la récurrence est achevée.

3. $m \mid n \quad \Rightarrow \quad T \in \mathbb{Z}[X]$; montrons cela : $m \mid n$, donc l'ensemble des diviseurs de n est la réunion disjointe de l'ensemble des diviseurs de m et de l'ensemble Q des diviseurs de n ne divisant pas m ; par suite, on a

$$\prod_{d \mid n} \Phi_d(X) = \prod_{\delta \mid m} \Phi_\delta(X) \cdot \prod_{q \in Q} \Phi_q(X).$$

D'après 1/, cela donne

$$X^n - 1 = (X^m - 1) \cdot \prod_{q \in Q} \Phi_q(X).$$

La propriété (P1) nous dit alors que

$$\left(\prod_{q \in Q} \Phi_q(X) \right) \in \mathbb{Z}[X],$$

et par suite $T \in \mathbb{Z}[X]$ (car $T = \prod_{q \in Q} \Phi q$).

4. $m \mid n$ implique que

$$T = \prod_{q \in Q} \Phi_q \in \mathbb{Z}[X]$$

(c'est le point 3/), et $m < n$ implique que $n \in Q$, et par suite,

$$T = \Phi_n \cdot \prod_{q \in Q - \{n\}} \Phi_q,$$

puis (P1) implique que

$$\left(\prod_{q \in Q - \{n\}} \Phi_q \right) \in \mathbb{Z}[X],$$

et donc Φ_n divise le polynôme T dans $\mathbb{Z}[X]$.

Proposition (P4) Soit G un groupe fini (non nécessairement commutatif) agissant sur un ensemble E non vide fini ; soient $\{s_1, \cdots, s_r\} \subset E$ un système de représentants des orbites, et $G_1, \cdots, G_r$ les stabilisateurs respectifs de $s_1, \cdots, s_r$. Alors on a :

1. Pour tout i, $1 \leq i \leq r$, $card(G_i)$ divise $card(G)$;

2. Formule des classes:

$$card\,(E) = \sum_{1\leq i\leq r} \frac{card\,(G)}{card\,(G_i)}.$$

Démonstration

Ici aussi, rappel des faits... On dit qu'un groupe G (noté ici multiplicativement et d'élément neutre noté 1) agit sur un ensemble E (non vide) s'il existe une opération $(\cdot * \cdot)$ de $G \times E$ dans E telle que :

$$\forall x \in E,\ 1 * x = x$$

$$\forall x \in E,\ \forall\,(g,g') \in G \times G,\ g' * (g * x) = (g'g) * x.$$

On note alors, pour tout x de E :

– $G * x = \{g * x\}_{g\in G}$, sous-ensemble de E appelé orbite de x .

– $G_x = \{g \in G\ /\ g * x = x\}_{g\in G}$, sous-ensemble de G appelé stabilisateur de x .

– s_x l'application de G dans $G * x$ qui à $g \in G$ associe $g * x$.

G_x est un sous-groupe de G; d'autre part, on constate que la relation d'équivalence factorisant l'application s_x coïncide avec la relation de quotient $\frac{G}{G_x}$; comme il est clair que s_x est surjective, on en déduit que les ensembles $\frac{G}{G_x}$ et $G * x$ sont équipotents.

Enfin, il est aisé de vérifier que l'ensemble des orbites, $\{G * x\}_{x\in E}$, forme une partition de E.

Dans le cas où E et G sont finis, tout cela implique la formule des classes : en effet, soient $G * x_1, \cdots, G * x_r$ les orbites, alors elles forment une partition de E, donc

$$card\,(E) = \sum_{1\leq i\leq r} card\,(G * x_i).$$

Comme $G * x_i$ est équipotent à $\frac{G}{G_{x_i}}$, cela donne

$$card\,(E) = \sum_{1\leq i\leq r} card\left(\frac{G}{G_{x_i}}\right)$$

La démonstration s'achève en remarquant que

$$card\left(\frac{G}{G_{x_i}}\right) = \frac{card\,(G)}{card\,(G_{x_i})}.$$

Nous pouvons passer désormais à la démonstration du théorème.

5.4 Démonstration du théorème de Wedderburn

Démonstration Soit K un corps fini. On note Z le centre de K, i.e. l'ensemble des éléments de K qui commutent avec tous les autres. Z est un sous-corps de K.

Notons q le cardinal de Z ; la propriété (P2) nous dit alors qu'il existe un entier naturel non nul n tel que $card\,(K) = q^n$.

Nous allons supposer désormais que K n'est pas commutatif ;

Cela implique que $Z \neq K$, et donc que $n \geq 2$.

Pour tout $x \in K$, on note Z_x l'ensemble des éléments de K qui commutent avec x.

Alors Z_x est un sous-corps de K, et une extension de Z.

Z est un sous-corps de Z_x, donc d'après la propriété (P2) il existe un entier naturel non nul $d\,(x)$ tel que

$$card\,(Z_x) = q^{d(x)}.$$

Z_x est un sous-corps de K, donc la propriété (P2) nous dit qu'il existe un entier naturel non nul m tel que $card\,(K) = (card\,(Z_x))^m$.

Mais comme $card\,(K) = q^n$, donc on obtient

$$q^n = \left(q^{d(x)}\right)^m,$$

et donc $n = m\,d\,(x)$.

Retenons de cela que $d\,(x)$ **divise n pour tout x de K**.

Le groupe (multiplicatif) K^* agit sur l'ensemble K^* via l'opération de conjugaison $k * x = kxk^{-1}$. Vérifions cela :

$$1 * x = 1x1^{-1} = x,$$

$$k'*(k*x) = k'\,(k*x)\,k'^{-1} = k'\left(kxk^{-1}\right)k'^{-1} = (k'k)\,x\left(k^{-1}k'^{-1}\right) = (k'k)\,x\,(k'k)^{-1} = (k'k)*x.$$

Pour tout x de K^*, on note $K^* * x$ l' orbite de x, et $stab\,(x)$ le stabilisateur de x.

Pour tout y de K^*, on a

$$Z_y = stab\,(y)\ \cup\ \{0\}.$$

Ainsi,

$$card\,(stab\,(y)) = q^{d(y)} - 1.$$

On a de plus, pour x dans K^* :

$$card\,(K^* * x) = 1 \quad \Leftrightarrow \quad K^* * x = \{x\} \quad \Leftrightarrow \quad stab\,(x) = K^* \quad \Leftrightarrow \quad x \in Z^*.$$

Notons $z_0, \cdots, z_{q-1}$ les éléments de Z (avec $z_0 = 0$); d'après les équivalences ci-dessus, les orbites qui coupent Z^* sont exactement $K^* * z_1, \cdots, K^* * z_{q-1}$. Soient $K^* * y_1, \cdots, K^* * y_r$ les autres orbites ; alors la formule des classes nous donne :

$$card\,(K^*) = \sum_{1 \leq i \leq q-1} \frac{card\,(K^*)}{card\,(stab\,(z_i))} \ + \ \sum_{1 \leq i \leq r} \frac{card\,(K^*)}{card\,(stab\,(y_i))}.$$

Comme $stab\,(z_i) = K^*$, que $card\,(stab\,(y_i)) = q^{d(y_i)} - 1$, et que $card\,(K^*) = q^n - 1$, cela donne :

$$q^n - 1 = (q-1) + \sum_{1 \leq i \leq r} \frac{q^n - 1}{q^{d(y_i)} - 1},$$

et donc enfin :

$$q - 1 = (q^n - 1) - \sum_{1 \leq i \leq r} \frac{q^n - 1}{q^{d(y_i)} - 1}.$$

Considérons la fraction rationnelle

$$F(X) = (X^n - 1) - \sum_{1 \leq i \leq r} \frac{X^n - 1}{X^{d(y_i)} - 1}.$$

On a vu que pour tout i, $d(y_i)$ divise n, et la propriété (P3) nous permet alors de dire que $F \in \mathbb{Z}[X]$.

Mieux, il est clair que $d(y_i) < n$, en effet, $d(y_i) = n$ impliquerait $orb(y_i) = K^*$, et donc $y_i \in Z$, ce qui est faux.

Alors la propriété (P3) permet d'affirmer que le polynôme cyclotomique Φ_n divise le polynôme

$$\frac{X^n - 1}{X^{d(y_i)} - 1}$$

dans $\mathbb{Z}[X]$. Comme Φ_n divise aussi $(X^n - 1)$ dans $\mathbb{Z}[X]$, on obtient que Φ_n divise le polynôme F dans $\mathbb{Z}[X]$. Autrement dit :

Il existe un polynôme $Q \in \mathbb{Z}[X]$ tel que $F = Q\,\Phi_n$.

En particulier, cela implique

$$F(q) = Q(q)\ \Phi_n(q).$$

Or (3) $F(q) = q - 1$, donc

$$q - 1 = Q(q)\ \Phi_n(q).$$

Comme $Q \in \mathbb{Z}[X]$, $Q(q)$ est un entier, non nul car $q \neq 1$ (Z contient au moins 0 et 1). Ainsi cette dernière égalité implique que $|\Phi_n(q)| \leq q - 1$. Par conséquent il existe (au moins) une racine complexe u de Φ_n telle que $|q - u| \leq q - 1$.

Or u est racine primitive n-ième de l'unité, et comme $n \geq 2$, $u \neq 1$; comme la distance de q au cercle trigonométrique est atteinte en 1, on a facilement $|q - u| > q - 1$. Mais on vient de prouver l'inverse !

D'où l'absurdité, et la preuve que K est bien commutatif.

Chapitre 6

La quintessence de la primalité n'est elle pas l'inversibilité ?

Par Guy Philippe

6.1 Notations

Dans la suite acu sera l'abréviation pour anneau commutatif unitaire et acui celle pour anneau commutatif unitaire intègre.
$\mathcal{D}_p$ désignera l'ensemble des diviseurs de p.
"ou" désignera le ou inclusif et "ou bien" le ou exclusif.

6.2 Introduction

A l'origine de cet article il y a un certain malaise que j'ai éprouvé(et je ne dois pas être le seul) en constatant que la définition d'élément premier d'un acui,qui est censée généraliser celle d'entier premier dans $\mathbb{N}$, fluctuait suivant les auteurs avec des propositions qui n'étaient pas toujours logiquement équivalentes. Ceci m'a amené à proposer

une définition ne faisant appel qu'à l'inversibilité

en partant du principe que ce qui caractérise un élément premier c'est le fait qu'il ne puisse se factoriser en un produit de 2 facteurs que si l'un des facteurs est inversible et pas l'autre.D'où le titre.
Par négation un élément non premier n sera donc un élément pour lequel il existera une factorisation en 2 facteurs inversibles(n sera alors inversible) ou en 2 facteurs non inversibles(on dira alors que n est un élément composé). La structure la plus générale où l'on puisse développer ces idées est celle de demi-goupe

multiplicatif abélien, comme $(\mathbb{N},\text{x})$, pour disposer de la notion d'élément inversible. On se retrouve ainsi dans le cadre naturel où s'est forgé le concept de nombre entier premier. Formalisons cela en considérant un demi-groupe abelien (E,x) d'élément neutre 1.On notera $\mathcal{U}$ l'ensemble des éléments inversibles de $E(1 \in \mathcal{U})$ et $\mathcal{P}(E)$ l'ensemble des éléments
premiers de E obtenu grâce à l'une des 2 définitions équivalentes suivantes:

$\forall p \in E$ p premier $\Longleftrightarrow \forall (a,b) \in E^2 \quad p = ab \Rightarrow (a,b) \notin \mathcal{U}^2 \bigcup (E \backslash \mathcal{U})^2$(I)
$\forall p \in E$ p premier $\Longleftrightarrow \forall (a,b) \in E^2 \quad p = ab \Rightarrow a$ ou bien $b \in \mathcal{U}$
C'est à dire que p ne peut s'écrire comme produit de 2 facteurs que si l'un est inversible et pas l'autre.
D'où par négation:
$\forall p \in E$ p non premier $\Longleftrightarrow \exists (a,b) \in E^2 \quad p = ab$ et $(a,b) \in \mathcal{U}^2 \bigcup (E \backslash \mathcal{U})^2$
On obtient ainsi une classification des éléments d'un demi-groupe abélien multiplicatif: Chaque élément d'un tel demi-groupe est soit **premier**,soit **inversible**,soit **composé**(i.e. factorisable en un produit de 2 éléments non inversibles) chaque cas excluant les deux autres.
On peut remarquer facilement que tout élément inversible x n'est pas premier car il est produit de 2 inversibles $x = x.1$ donc dans un groupe il n'y a pas d'éléments premiers.
Un carré x^2 n'est jamais premier car suivant que x est inversible ou pas x^2 est le produit de 2 inversibles ou de 2 non inversibles.
D'autre part dans le cas du demi-groupe (A,x) d'un acui A l'élément 0 n'est pas premier car il est produit de 2 non inversibles $0 = 0.0$. Donc 0 est même un élément composé.
Si A est un acu on pourra bien sûr appliquer cette définition au demi-groupe abelien (A,x) i.e. hors intégrité de l'anneau.

6.3 Définitions consensuelles

A étant un acu rappelons 2 définitions pour lesquelles il y a consensus de tous les auteurs cités dans cet article.
A intègre $\Longleftrightarrow A \neq \{0\}$ et $\forall (a,b) \in A^2 \quad ab = 0 \Longrightarrow a = 0$ ou $b = 0$

I idéal premier de $A \Longleftrightarrow A/I$ est intègre$\Longleftrightarrow$
$A/I \neq \{0\} (A \neq I) \quad$ et $\quad \forall (\overline{x},\overline{y}) \in A/I \quad \overline{x}.\overline{y} = \overline{0} \Longrightarrow \overline{x} = \overline{0}$ ou $\overline{y} = \overline{0} \Longleftrightarrow$
$A/I \neq \{0\} (A \neq I) \quad$ et $\quad \forall (a,b) \in A^2 \quad ab \in I \Longrightarrow a \in I$ ou $b \in I$

Par conséquent si A est intègre l'idéal nul $I = \{0\}$ est premier.

6.4 Quelques liens logiques

p étant un élément d'un acui A considérons 3 propositions utilisées par différents auteurs pour définir un élément premier.

$p \neq 0$ et $p \notin \mathcal{U}$ et $\mathcal{D}_p = \mathcal{U} \bigcup p\mathcal{U}$ (II) Maclane et Birkhoff[1]

pA est un idéal premier (III) Arnaudiès et Bertin[2] ,Bouvier,George...[3]

$p \notin \mathcal{U}$ et $\forall (a,b) \in A^2 \quad p|ab \Longrightarrow p|a$ ou $p|b$ (IV) Duverney[4]

Montrons que (III)$\Longleftrightarrow$(IV)

(III)$\Longrightarrow^{?}$(IV)
On utilisera les équivalences suivantes qui caractérisent un idéal(principal)premier:
pA idéal premier $\Longleftrightarrow A/pA$ est intègre $\Longleftrightarrow$
$A/pA \neq \{0\}$ et $\forall (a,b) \in A^2 \quad ab \in pA \Longrightarrow a \in pA$ ou $b \in pA$
D'abord $p \notin \mathcal{U}$ (sinon $p \in \mathcal{U} \Longrightarrow pA = A \Longrightarrow A/pA = \{0\}$ ce qui contredirait (III))
Ensuite $p|ab \Longrightarrow ab \in pA$ d'où d'après (III) $a \in pA$ ou $b \in pA$ c'est à dire $p|a$ ou $p|b$ et ainsi (IV) est bien vérifié.

(IV)$\Longrightarrow^{?}$(III)
D'abord $A/pA \neq \{0\}$ (sinon $pA = A \Longrightarrow p \in \mathcal{U}$ ce qui contredirait (IV))
Ensuite $ab \in pA \Longrightarrow p|ab$ d'où d'après (IV) $p|a$ ou $p|b$ c'est à dire $a \in pA$ ou $b \in pA$ et ainsi (III) est bien vérifié.

En définissant un élément premier p d'un acui A grâce à l'une des 2 propositions équivalentes(III) ou (IV) on aurait l'inconvénient que 0 soit premier.
En effet $0A = \{0\}$ est un idéal premier vu que $A/0A = A$ qui est intègre.Des lors (III) $\Leftrightarrow$ (II) car pour $p = 0$ (III) est vraie alors que (II) est fausse.Et même si on ajoutait à (III) $pA \neq \{0\}$ l'équivalence avec (II) serait encore fausse.

(II) $\Leftrightarrow pA$ est un idéal premier non nul.

On peut s'en convaincre avec l'acui $\mathbb{Z}(i\sqrt{5})$.Il est facile de montrer qu'avec $p = 3$ (II) est vraie.
En posant $N(a + i\sqrt{5}b) = a^2 + 5b^2$ il est immédiat que $N(zz') = N(z)N(z')$ d'où si $zz' = 1$ avec $z = a + i\sqrt{5}b \quad N(z) = a^2 + 5b^2 = 1$ ce qui entraîne $b = 0$,$a = (^+/_-)1$.Les inversibles de $\mathbb{Z}(i\sqrt{5})$ sont donc 1 et -1 soit $\mathcal{U} = \{1, -1\}$.
$p = 3 \neq 0$ et $p = 3 \notin \mathcal{U} = \{1, -1\}$
De plus $a + i\sqrt{5}b \in \mathcal{D}_3 \Longrightarrow \underline{(a + i\sqrt{5}b)(x + i\sqrt{5}y) = 3} \Longrightarrow$
$N(3) = 9 = (a^2 + 5b^2)(x^2 + 5y^2) \Longrightarrow a^2 + 5b^2 \in \mathcal{D}_9 = \{1,3,9\}$
Or $a^2 + 5b^2 = 1 \Longrightarrow b = 0$ et $a = (^+/_-)1 \Longrightarrow a + i\sqrt{5}b = (^+/_-)1 \in \mathcal{U}$
et $a^2 + 5b^2 = 3 \Longrightarrow b = 0$ et $a^2 = 3$ ce qui est impossible dans $\mathbb{Z}$.
Enfin $a^2 + 5b^2 = 9 \Longrightarrow x^2 + 5y^2 = 1 \Longrightarrow y = 0$ et $x = (^+/_-)1$ d'où avec l'égalité souslignée $a + i\sqrt{5}b = (^+/_-)3 \in 3\mathcal{U}$
On a donc prouvé l'inclusion:$\mathcal{D}_3 \subset \mathcal{U} \bigcup 3\mathcal{U}$ et comme l'inclusion contraire est immédiate (II) est bien vraie avec p=3.
Pourtant $3\mathbb{Z}(i\sqrt{5})$ est un idéal non nul qui n'est pas premier vu que
$(2 - i\sqrt{5})(2 + i\sqrt{5}) = 9 \in 3\mathbb{Z}(i\sqrt{5})$ bien que ni$(2 - i\sqrt{5})$,ni $(2 + i\sqrt{5}) \in 3\mathbb{Z}(i\sqrt{5})$ compte tenu que $2 - i\sqrt{5} = 3(a + i\sqrt{5}b) \Longrightarrow 2 = 3a$ ce qui est impossible dans $\mathbb{Z}$ et idem avec $2 + i\sqrt{5}$.
Le but recherché étant de trouver une définition générale d'un élément premier valable aussi bien pour les entiers naturels que pour les éléments d'un acui quelconque il reste la proposition (II) et on remarque qu'elle est équivalente à la proposition (I) proposée dans l'introduction.
$p \neq 0$ et $p \notin \mathcal{U}$ et $\mathcal{D}_p = \mathcal{U} \bigcup p\mathcal{U}$ (II)
$\forall (a,b) \in A^2 \quad p = ab \Longrightarrow (a,b) \notin \mathcal{U}^2 \bigcup (A \backslash \mathcal{U})^2$ (I)
Montrons que (II) $\Longleftrightarrow$ (I)
(II)$\Longrightarrow$?(I)
$p = ab \Longrightarrow a$ et $b \in \mathcal{D}_p = \mathcal{U} \bigcup p\mathcal{U}$
alors $\underline{(a,b) \notin \mathcal{U}^2}$.Sinon on aurait $p = ab \in \mathcal{U}$ ce qui contredirait (II)
On a aussi $\underline{(a,b) \notin (A \backslash \mathcal{U})^2}$.Sinon a et $b \notin \mathcal{U}$ et comme a et $b \in \mathcal{D}_p = \mathcal{U} \bigcup p\mathcal{U}$ on aurait donc a et $b \in p\mathcal{U}$ soit $a = p\epsilon, b = p\theta$ puis $ab = p = p^2\epsilon\theta$ et $p(1 - p\epsilon\theta) = 0$ enfin

comme A est intègre et $p \neq 0 \quad 1 = p\epsilon\theta$
On aurait donc $p \in \mathcal{U}$ ce qui contredirait (II).
Finalement (I) est vérifiée.
(I)$\Longrightarrow$?(II)
$p \neq 0$ sinon $p = 0.0$ avec $(0,0) \in (A\backslash\mathcal{U})^2$ ce qui contredirait (I).
$p \notin \mathcal{U}$ sinon $p = p.1$ avec $(p,1) \in \mathcal{U}^2$ ce qui contredirait (II).
$\mathcal{D}_p \subset \mathcal{U} \bigcup p\mathcal{U}$
En effet $a \in \mathcal{D}_p \Longrightarrow p = ab$ d'où d'après (I) $(a,b) \notin \mathcal{U}^2 \bigcup (A\backslash\mathcal{U})^2$.
D'autre part on a l'alternative:
ou bien $a \in \mathcal{U}$ et alors $a \in \mathcal{U} \bigcup p\mathcal{U}$
ou bien $a \notin \mathcal{U}$ et alors $b \in \mathcal{U}$ sinon $(a,b) \in (A\backslash\mathcal{U})^2$ ce qui contredirait (I).
Donc il existe $c \in A$ tel que $bc = 1$ d'où $p = ab \Longrightarrow pc = abc = a.1 = a$
et $a \in p\mathcal{U}$ vu que $c \in \mathcal{U}$.Par conséquent $a \in \mathcal{U} \bigcup p\mathcal{U}$
Finalement l'inclusion annoncée est prouvée et comme l'inclusion contraire est immédiate on a montré que (II) est vérifiée ce qui termine la preuve de l'équivalence annoncée.
Malgré l'équivalence des propositions (II) et (I) dans un acui,où l'intégrité a été utilisée, on peut remarquer que (II) fait référence à la structure d'anneau à cause de 0 qui y figure alors que ce n'est pas le cas de (I) qui se réfère seulement à un demi-groupe abélien multiplicatif.
On pourrait aussi définir un élément premier ,hors intégrité ,dans un acu grâce à (I) mais on perdrait la règle des degrés deg(PQ)=deg(P)+deg(Q) pour P et Q non nuls qui découle de l'intégrité or cette règle est fondamentale pour l'arithmétique dans les anneaux de polynômes $A[X_1,X_2,...X_n]$.
Il semble dès lors raisonnable de définir un élément premier dans un acui avec la proposition (II) ou la (I) c'est le choix fait dans ce qui suit.
Montrons qu'avec la proposition (I) on retrouve les caractérisations usuelles des éléments premiers dans $\mathbb{N}$ *et dans les demi-groupes multiplicatifs d'anneaux(acui) classiques comme* $\mathbb{Z}$*, et* $A[X_1,X_2...X_n] \quad$ *avec* $n \geq 1$ *et* A *un acui , éventuellement un corps.*
Ici je préfère dire polynôme premier que polynôme irréductible qui pourrait faire référence à la notion d'élément irréductible d'un acui dont je préfère ne pas parler ici , même si ,pour $p \neq 0$ les 2 notions coïncident sur un acui factoriel([2] page 50).

premiers dans $\mathbb{N}$

Dans $\mathbb{N}$ il n'y a qu'un inversible:1 donc $\mathcal{U} = \{1\}$.
La définition élémentaire pour qu'un entier p soit premier est:$card(\mathcal{D}_p) = 2$.
Montrons que pour $p \in \mathbb{N}$
$card(\mathcal{D}_p) = 2 \iff \forall (a,b) \in \mathbb{N}^2 \quad p = ab \implies a$ ou bien b est inversible i.e. a ou bien b est égal à 1
$(\Longrightarrow ?)$
On a $card(\mathcal{D}_p) = 2$ d'où $\mathcal{D}_p = \{1,p\}$ et donc $p \neq 1$.
Si on a $p = ab$ alors a et $b \in \mathcal{D}_p = \{1,p\}$
ou $a = 1$ et alors $b = p \neq 1$ par conséquent a ou bien b est bien inversible.
ou $b = 1$ et alors $a = p$ ensuite même raisonnement.
$(\Longleftarrow ?)$
Si $a \in \mathcal{D}_p$ alors il existe b tel que $p = ab$ d'où a ou bien b est inversible i.e. a ou bien b est égal à 1.
Soit $a = 1$ et $b = p$ soit $b = 1$ et $a = p$.Les seuls diviseurs de p sont donc:1 et p et comme $p \neq 1$(sinon $p = 1.1$,p serait produit de 2 inversibles)on a bien $card(\mathcal{D}_p) = 2$.

premiers dans $\mathbb{Z}$

Il est facile de montrer que $p \in \mathcal{P}(\mathbb{Z}) \iff |p| \in \mathcal{P}(\mathbb{N})$

Les premiers dans $A[X_1,X_2....X_n]$

Pour simplifier , $A[X_1,X_2....X_n]$ sera noté $A[X_i]$, c'est l'anneau des polynômes à coéfficients dans un acui A en les indéterminées $X_1,X_2,...X_n$ où $n \geq 1$
Avec la règle des degrés il est immédiat que les inversibles de $A[X_i]$ sont les inversibles de A.
On rappelle qu'un polynôme de $A[X_i]$ sera dit primitif si et seulement si ses coéfficients ne sont divisibles que par les inversibles de A avec la convention que le polynôme nul n'a que le coéfficient 0.Par conséquent le polynôme nul n'est pas primitif car $o|o$ et o n'est pas inversible.
Il est clair qu'un polynôme dont l'un des coéfficients est inversible comme 1 ou -1 est primitif.
Il est aussi clair qu'un polynôme non nul à coéfficients dans un corps est primitif car il admet un coéfficient $a_k \neq 0$ et un diviseur d de ce polynôme divisera a_k donc $d \neq 0$ et par suite d est inversible.

6.5 Les premiers de $A[X_i]$ sont:

soit les polynômes constants quand la constante est un élément premier de A.
Soit les polynômes non constants,primitifs et ne pouvant s'écrire comme produit de 2 polynômes non constants.

$$P \in \mathcal{P}(A[X_i]) \Leftrightarrow \left| \begin{array}{l} deg(P) = 0 \quad \text{et } P \in \mathcal{P}(A) \\ \text{ou bien} \\ deq(P) \geq 1 \text{ , } P \text{ est primitif et } P = QR \Rightarrow \text{deg(Q) ou bien deg(R)=0} \end{array} \right.$$

$(\Longrightarrow ?)$

P étant premier,$P \neq 0$ et donc P admet un degré.
Si $deg(P) = 0$ alors $P \in A$ et si on a $P = QR$ dans A comme $A \subset A[X_i]$ on a aussi $P = QR$ dans $A[X_i]$ or $P \in \mathcal{P}(A[X_i])$ donc Q ou bien R est inversible dans $A[X_i]$ et par suite dans A ce qui assure la primalité de P dans A.
Si $deg(P) \geq 1$ alors P est primitif.En effet soit $D \in A$ un diviseur de P.On a alors $P = DQ$ dans $A[X_i]$ avec $deg(Q) = deg(P) \geq 1$ d'où Q n'est pas inversible et par conséquent D est inversible sinon P serait produit de 2 non inversibles ce qui contredirait sa primalité.
De plus si on a $P = QR$ dans $A[X_i]$ et comme $P \in \mathcal{P}(A[X_i])$ Q ou bien R est inversible donc $deg(Q)$ ou bien $deg(R) = 0$

$(\Longleftarrow ?)$

Si $deg(P) = 0$ et $P \in \mathcal{P}(A)$ on a $P \neq 0$
soit $P = QR$ dans $A[X_i]$ alors $Q \neq 0$ et $R \neq 0$ d'où Q et R ont un degré et comme $deg(P) = deg(Q) + deg(R)$ on a $deg(Q) = deg(R) = 0$ et donc Q et $R \in A$.Or $P \in \mathcal{P}(A)$ d'où Q ou bien R est inversible dans A et donc dans $A[X_i]$ ainsi on a bien $P \in \mathcal{P}(A[X_i]$.
Si $deg(P) \geq 1$, P est primitif et $P = QR \Longrightarrow deg(Q)$ ou bien $deg(R) = 0$
soit $P = QR$ dans $A[X_i]$ on a par hypothèse $deg(Q)$ ou bien deg(R)=0
par exemple $deg(Q) = 0$ d'où $deg(R) \geq 1$ et ainsi R n'est pas inversible.De plus la constante Q divise le polynôme primitif P donc Q est inversible ce qui prouve bien que $P \in \mathcal{P}(A[X_i])$.
Exemples:les polynômes primitifs de degré 1 sont premiers(c'est clair)comme:
$P = -3X + 5Y + 2Z$ avec $A = \mathbb{Z}$
Par contre $P = 5X - 10Y + 15Z$ est de degré 1 mais n'est pas premier car il n'est pas primitif vu que $5|P$ et 5 n'est pas inversible dans $\mathbb{Z}$.

Traitons maintenant le cas particulier des polynômes à coéfficients dans un corps commutatif K.
Un élément de K est soit 0 donc non premier soit inversible donc non premier aussi et par conséquent $\mathcal{P}(K) = \emptyset$.
De plus $\forall P \in K[X_i]$ avec $deg(P) \geq 1$ Pest primitif d'où l'équivalence précédente devient:

$$P \in \mathcal{P}(K[X_i]) \Longleftrightarrow deg(P) \geq 1 \quad \text{et } P = QR \Longrightarrow deg(Q) \text{ ou bien } deg(R) = 0$$

Exemples:les polynômes de degré 1 à une ou plusieurs indéterminées et à coéfficients dans un corps sont premiers.

Comme application de la classification des éléments d'un demi-groupe abélien multiplicatif et pour terminer donnons une caractérisation des corps parmi les acui nœthériens:
"pour qu' un acui nœthérien soit un corps il faut et il suffit qu'il n'ait pas d'élément premier."
Autrement dit pour un acui nœthérien A:

$$\text{A est un corps} \Longleftrightarrow \mathcal{P}(A) = \emptyset$$

On a déjà remarqué que si A est un corps alors $\mathcal{P}(A) = \emptyset$. Il reste donc à montrer que si A est un acui nœthérien et $\mathcal{P}(A) = \emptyset$ alors A est un corps.
A est intègre donc par définition $A \neq \{0\}$ dès lors on peut choisir un élément non nul $a_0 \in A$ et en raisonnant par l'absurde on va montrer que a_0 est inversible.
En effet si a_0 n'était pas inversible comme il n'est pas premier ($\mathcal{P}(A) = \emptyset$) il serait composé donc il s'écrirait $a_0 = a_1 b_1$ avec a_1 etb_1 non inversibles d'où $a_0 A \subset a_1 A$.
on pourrait alors recommencer avec a_1 à la place de a_0
soit $a_1 = a_2 b_2$ avec a_2 etb_2 non inversibles d'où $a_1 A \subset a_2 A$ etc...
A chaque étape on obtiendrait un élément a_k non inversible et non premier donc il serait composé et pourrait s'écrire $a_k = a_{k+1} b_{k+1}$ avec a_{k+1} et b_{k+1} non inversibles et bien sûr $a_k A \subset a_{k+1} A$.
On construirait ainsi une suite croissante d'idéaux qui serait stationnaire à partir d'un certain rang n vu que A est nœthérien; par conséquent
$a_n A = a_{n+1} A$ d'où il existerait $x \in A$ tel que $a_{n+1} = a_n x$ et comme par construction $a_n = a_{n+1} b_{n+1}$ on aurait

$$a_n = a_n x b_{n+1} \quad \text{puis}$$
$$a_n(1 - x b_{n+1}) = 0$$

De plus comme on aurait $a_0 A \subset a_k A$ pour tout entier k on aurait $a_n \neq 0$ (sinon $a_0 A \subset 0A = \{0\}$ et donc $a_0 = 0$ et la contradiction) or A est intègre d'où $1 - x b_{n+1} = 0$ et enfin $1 = x b_{n+1}$ d'où b_{n+1} serait inversible et la contradiction .Finalement A est bien un corps.
Par conséquent un acui nœthérien autre qu'un corps admet au moins un élément premier.On peut alors montrer que tout élément ni nul ni inversible admet une décomposition primaire qui n'est pas unique en général en s'inspirant de de la méthode précédente.
La propriété précédente permet aussi de prouver qu'un acui n'est pas nœtherien.En effet un acui autre qu'un corps qui n'a pas d'élément premier n'est pas nœtherien.
Exemple: l'anneau $\widehat{\mathbb{Z}}$ des entiers algébriques sur $\mathbb{C}$.
Preuve:
D'abord $\widehat{\mathbb{Z}}$ est un acui(bien connu) mais ce n'est pas un corps, sinon ,comme l'intersection de 2 corps est un corps on aurait $\widehat{\mathbb{Z}} \bigcap \mathbb{Q}$ qui serait un corps or $\widehat{\mathbb{Z}} \bigcap \mathbb{Q} = \mathbb{Z}$.
En effet soit la fraction irréductible $\frac{p}{q} \in \widehat{\mathbb{Z}} \bigcap \mathbb{Q}$.Il existe donc un polynôme unitaire $P \in \mathbb{Z}[X]$ de degré ≥ 1 tel que $P(\frac{p}{q}) = 0$.
D'où,avec des notations évidentes
$a_0 + a_1 \frac{p}{q} + a_2(\frac{p}{q})^2 + ... + a_{n-1}(\frac{p}{q})^{n-1} + (\frac{p}{q})^n = 0$.Après multiplication par q^n on obtient:
$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + ... a_{n-1} p^{n-1} q + p^n = 0$
Dès lors q divise p^n et en appliquant le théorème de GAUSS à répétition
comme $p \wedge q = 1$ on a $q|p^n \Longrightarrow q|p^{n-1} \Longrightarrow q|p^{n-2} ... \Longrightarrow q|p \Longrightarrow \frac{p}{q} \in \mathbb{Z}$ ce qui prouve une inclusion,l'autre étant évidente.
$\widehat{\mathbb{Z}}$ n'est donc pas un corps.
De plus $\mathcal{P}(\widehat{\mathbb{Z}}) = \emptyset$ sinon soit $p \in \mathcal{P}(\widehat{\mathbb{Z}})$ comme $p \in \widehat{\mathbb{Z}}$ il existerait $P \in \mathbb{Z}[X]$ unitaire

et de degré ≥ 1 tel que $P(p) = 0$ d'où avec les notations précédentes $a_0 + a_1 p + a_2 p^2 + ...a_{n-1}p^{n-1} + p^n = 0$.
Or dans $\mathbb{C}$ tout complexe est un carré d'où $p = q^2$ avec $q \in \mathbb{C}$.
On aurait donc $a_0 + a_1 q^2 + a_2 q^4 + ...a_{n-1}q^{2n-2} + q^{2n} = 0$ par conséquent $q \in \widehat{\mathbb{Z}}$ et finalement p serait un carré dans $\widehat{\mathbb{Z}}$ donc ne pourrait être premier d'où la contradiction.
$\widehat{\mathbb{Z}}$ est un bon exemple d'acui sans éléments premiers qui n'est ni nœthérien ni bien sûr factoriel.

J'espère avoir convaincu le lecteur de l'intérêt d'utiliser la proposition (I) pour définir les éléments premiers et de l'intérêt de la classification des éléments d'un demi-groupe abélien multplicatif qui s'y rapporte car ce sont des facteurs de clarté et de simplification des preuves en arithmétique élémentaire ou plus élaborée.
Pour me contacter $\rightsquigarrow$ guyphilippe@les-mathematiques.net

Bibliographie

[1] S.MACLANE et G.BIRKHOFF Algèbre 1/structures fondamentales GAUTHIER-VILLARS 1970 p171

[2] J-M.ARNAUDIES et J.BERTIN Groupes,algèbres et géométrie T1 ELLIPSES 1993 p 48

[3] A.BOUVIER , M.GEORGE ET F.LE LIONNAIS Dictionnaire des mathématiques PUF 1996 p670

[4] D.DUVERNEY Théorie des nombres DUNOD 1998 p53

Chapitre 7

Arithmétique factorielle

Guy PHILIPPE

PRELIMINAIRES ET OBJECTIF

DEMI-GROUPES FACTORIELS
(Cours d'arithmétique factorielle)

ANNEAUX FACTORIELS
(Théorème de permanence de la factorialité,de Gauss)

CRITERE D'EISENSTEIN

RECAPITULATIF

(des propositions et théorèmes)

Guy PHILIPPE

PRELIMINAIRES ET OBJECTIF

Ce travail est la suite logique de l'article intitulé "la quintessence de la primalité n'est-elle pas l'inversibilité?"où j'ai essayé de convaincre le lecteur du bien-fondé de définir un élément premier dans un demi-groupe multiplicatif abélien E et non pas dans un anneau, comme c'est l'usage, grâce à la définition: p **élément de** E **sera dit premier si et seulement si** $p = ab$ **n'est possible qu'avec** a **ou bien** b **inversible("ou bien" désignant le "ou" exclusif).** Dès lors il devenait naturel de développer l'arithmétique factorielle(celle qui est "calée" uniquement sur la décomposition primaire unique) dans un demi-groupe où il existe une décomposition primaire unique qui est appelé pour cela demi-groupe factoriel.La suite est donc un cours d'arithmétique factorielle developpé à partir de la structure de demi-groupe factoriel où l'on retrouve bien sûr toutes les propriétés traditionnelles d'un anneau factoriel après quoi pour rejoindre l'arithmétique polynômiale qui elle nécessite la structure d'anneau on définit un anneau factoriel comme un anneau commutatif unitaire intègre dont le demi-groupe multiplicatif est factoriel ce qui est équivalent à la définition traditionnelle d'un anneau factoriel.On poursuit avec le théorème de permanence de la factorialité de Gauss et on termine avec le critère d 'Eisenstein dans plusieurs versions qui permet de détecter les polynômes premiers à une ou plusieurs indéterminées.
La lecture de l'article cité plus haut est conseillée pour tirer un profit optimal de ce travail.

Notations , définitions et rappels

acui est une abréviation pour anneau commutatif unitaire intègre.
A étant un acui, A* désignera l'ensemble des éléments inversibles de A.On sait qu'alors $A[X_i]$ où $i = 1$ à $n \quad (n \geq 1)$ est aussi un acui et il est remarquable et très utile de savoir que $(A[X_i])^* = A^*$(à cause de la règle des degrés) d'où avec $A[Y_j]$ à la place de A on aura aussi $(A[Y_j][X_i])^* = (A[Y_j])^* = A^*$
Dans un anneau polynômial $A[X_i]$ A désignera l'anneau des coéfficients(ou des scalaires) et X_i les indéterminées.$P \in A[X_i]$ sera dit primitif (sur A) si ses coéfficients n'ont pour diviseurs communs que les inversibles de A.
On notera Q_A le corps des fractions de A. $\mathcal{P}(A)$ désignera l'ensemble des premiers de A et $\mathcal{P}(A[X_i])$ l'ensemble des polynômes premiers de $A[X_i]$;on dira aussi polynômes premiers sur A ou polynômes A-premiers.
On utilisera pour définition des éléments premiers d'un anneau commutatif unitaire intègre(acui) la suivante, pour montrer sa facilité d'usage, à savoir:
$p \in \mathcal{P}(A) \iff \forall (a,b) \in A^2 \quad p = ab \Longrightarrow a$ ou bien $b \in A^*$ qui est encore équivalente à $p \neq 0$ et $p \notin A^*$ et $\mathcal{D}_p = A^* \bigcup pA^*$(cf l'article cité au début).
On rappelle que "ou bien" signifie ou exclusif.
On rappelle aussi le **théorème de caractérisation des polynômes premiers de** $A[X_i]$ **où** A **est un acui**(preuve dans l'article cité au début).
Les polynômes premiers de $A[X_i]$ sont:
1• les polynômes CONSTANTS quand cette constante est un premier de A.
2• les polynômes P de degré≥ 1 et primitifs qui ne peuvent s'écrire $P = QR$ dans $A[X_i]$ avec $deg(Q) \geq 1$ et $deg(R) \geq 1$.
Cas particulier: si A est un corps:P est premier dans $A[X_i] \iff deg(P) \geq 1$ et P ne peut s'écrire $P = QR$ dans $A[X_i]$ avec $deg(Q) \geq 1$ et $deg(R) \geq 1$.

Polymorphie des polynômes à plusieurs indéterminées

A étant un acui et n un entier supérieur ou égal à 2 on notera $A[X_i]$ l'anneau $A[X_1,X_2,...X_n]$ des polynômes à coéfficients dans A et à n indéterminées.

Soit P un polynôme de $A[X_i]$.On entend par polymorphie le fait que l'on puisse alors considérer par exemple P comme un polynôme en les indéterminées X_1,...X_p , à coéfficients dans $A[X_{p+1},...X_n]$ si $p = 1$ à $n-1$ ou à coéfficients dans A si $p = n$.

P peut donc être interprété comme un polynôme de $2^n - 1$ façons c'est à dire d'autant de façons qu'il y a de choix de parties non vides dans l'ensemble des indéterminées $\{X_1...X_n\}$.

Au choix de la partie $\{X_2,X_3\}$ pour les indéterminées principales correspond l'interprétation de P comme polynôme de $A[X_1,X_4,...X_n][X_2,X_3]$.

Exemple (en mettant entre parenthèses les coéfficients autres que 1 et -1):

1 $P = X + (5)X^2Y - X^3Z^7 + Y^2 \in \mathbb{Z}[X,Y,Z]$

2 $P = (X + 5X^2Y + Y^2) + (-X^3)Z^7 \in \mathbb{Z}[X,Y][Z]$

3 $P = (X - X^3Z^7) + (5X^2)Y + Y^2 \in \mathbb{Z}[X,Z][Y]$

4 $P = (Y^2) + X + (5Y)X^2 + (-Z^7)X^3 \in \mathbb{Z}[Y,Z][X]$

5 $P = (X) + (5X^2)Y + (-X^3)Z^7 + Y^2 \in \mathbb{Z}[X][Y,Z]$

6 $P = (Y^2) + X + (5Y)X^2 - X^3Z^7 \in \mathbb{Z}[Y][X,Z]$

7 $P = (-Z^7)X^3 + Y^2 + X + (5)YX^2 \in \mathbb{Z}[Z][X,Y]$

Ici il y a 3 indéterminées:X,Y,Z soit n=3;on a bien $2^3 - 1 = 7$ interpétations possibles pour P.

L'intérêt de cette polymorphie est que si P est premier pour une des interprétations possibles il l'est aussi pour toutes les autres(cf théorème 1).

Ceci permettra d'envisager P comme un polynôme à une seule indéterminée X_i et de pouvoir éventuellement lui appliquer le critère d'EISENSTEIN(traité dans la suite).

Par contre un polynôme $P \in A[X_i]$ pourra être primitif pour une interprétation et pas primitif pour une autre:

$P = X^2 + XY + X^3Y^2 \in \mathbb{Z}[X,Y]$; P est primitif sur $\mathbb{Z}$ alors que

$P = (X^2) + (X)Y + (X^3)Y^2 \in \mathbb{Z}[X][Y]$ n'est pas primitif sur $\mathbb{Z}[X]$.

Choisissons une partie E non vide de {1,2,3,...n} et soit S sa complémentaire de façon à ce que les X_e pour $e \in E$ désignent les indéterminées principales et les X_s pour $s \in S$ les secondaires en convenant que pour $S = \emptyset$ $A[X_s] = A$.

Théorème 1 $P \in \mathcal{P}(A[X_i]) \iff P \in \mathcal{P}(A[X_s][X_e])$

Démonstration si $S = \emptyset$ l'équivalence est triviale sinon:

($\Longrightarrow$?)

Soit P=QR dans $A[X_s][X_e]$ .Q et R sont aussi des polynômes de $A[X_i]$ donc on a P=QR dans $A[X_i]$ et comme $P \in \mathcal{P}(A[X_i])$ on a Q ou bien R $\in (A[X_i])^* = A^* = (A[X_s][X_e])^*$ d'où $P \in \mathcal{P}(A[X_s][X_e])$ et idem pour la réciproque.

Autre aspect de la polymorphie: tout polynôme P à n indéterminées de $A[X_i]$ peut aussi être considéré comme un polynôme à n+1 indéterminées $X_1,X_2,..X_n,T$ ou plus.

Et la primalité du premier polynôme entraîne la primalité du deuxième.

Théorème 2 $P \in \mathcal{P}(A[X_i]) \Longrightarrow P \in \mathcal{P}(A[X_i,T])$

Démonstration Soit $P = QR$ dans $A[X_i,T]$.Comme $P \in \mathcal{P}(A[X_i])$ $P \neq 0$ donc P

a un degré donc aussi un degré en T d'où $deg_{|_T}(P) = deg_{|_T}(Q) + deg_{|_T}(R) = 0$ et par suite $deg_{|_T}(Q) = deg_{|_T}(R) = 0$ i.e. Q et $R \in A[X_i]$, on a donc $P = QR$ dans $A[X_i]$ et comme $P \in \mathcal{P}(A[X_i])$ on aura Q ou bien $R \in (A[X_i])^* = A^* = (A[X_i,T])^*$ ce qui prouve bien que $P \in \mathcal{P}(A[X_i,T])$.

Remarque:soit $P \in \mathcal{P}(A[X_i,T])$ si on spécialise l'indéterminée T par $T = t \in A$ on obtient un nouveau polynôme $P_t \in A[X_i]$ mais en général $P_t \notin \mathcal{P}(A[X_i])$.Exemple: $P = X^2 - T \in \mathcal{P}(A[X,T])$ vu que P en tant que polynôme de $A[X][T]$ est de degré 1 et primitif sur $A[X]$(cf théorème de caractérisation des premiers de $A[X_i]$ où A est un acui),pourtant avec $T = 1$ on a $P_1 = X^2 - 1 = (X+1)(X-1)$ donc $P_1 \notin \mathcal{P}(A[X])$.

Dans la suite **"demi-groupe" voudra dire demi-groupe abélien multiplicatif.**

Relation d'association dans un demi-groupe
Soit un demi-groupe E et la relation d'association,notée $\sim$, définie par
$a \sim b \iff \exists \epsilon \in E^* \quad a = \epsilon b$.
Il est clair que c'est un relation d'équivalence.
Cette relation est compatible avec la multiplication et ainsi la structure de demi-groupe multiplicatif abélien de E passe au quotient dans $E/\sim$
En effet $a \sim b$ et $x \sim y \Longrightarrow \exists \epsilon$ et $\theta \in E^* \quad a = \epsilon b$ et $x = \theta y$ d'où $ax = (\epsilon\theta)by$ or $\epsilon\theta \in E^*$ donc $ax \sim by$
remarque: $\forall p \in \mathcal{P}(E) \qquad \forall \epsilon \in E^* \qquad \epsilon p \in \mathcal{P}(E)$ i.e.
"l'associé d' un premier est premier"
En effet soit $\epsilon p = ab$ dans E on a $p = \epsilon^{-1}ab = (\epsilon^{-1}a)b$ et comme $p \in \mathcal{P}(E)$ on a $\epsilon^{-1}a$ ou bien $b \in E^*$ i.e. a ou bien $b \in E^*$ d'où $\epsilon p \in \mathcal{P}(E)$.
*Par contre si E est le demi-groupe multiplicatif d'un acui cette relation n'est pas compatible en général avec l'addition.*Ce que l'on peut vérifier avec $E = \mathbb{Z}$ d'où $E^* = \{-1,1\}$
$5 \sim 5$ et $-3 \sim 3$ pourtant $5 + (-3) \not\sim 5 + 3$

Dans le demi-groupe multiplicatif $E/\sim$ les éléments(classes) premiers sont les classes des éléments premiers de E(preuve dans le théorème 3).
La primalité étant "calée" sur l'inversibilité précisons les inversibles de $(E/\sim)$. Ce sont les classes des inversibles de E.
En effet $\overline{a}$ inversible dans $E/\sim \iff \exists \overline{b} \in E/\sim \quad \overline{a}\,\overline{b} = \overline{1}$ autrement dit ab et 1 sont associés d'où il existe $\epsilon \in E^*$ tel que $ab = \epsilon 1 = \epsilon \in E^*$ ce qui entraîne a est inversible dans E.

Réciproquement a inversible dans $E \Longrightarrow \exists b \in E \quad ab = 1 \Longrightarrow \overline{ab} = \overline{1} \Longrightarrow \overline{a}\,\overline{b} = \overline{1} \Longrightarrow \overline{a}$ est inversible dans $E/\sim$.

Théorème 3 "La relation $\sim$ respecte la primalité"
$\overline{p} \in \mathcal{P}(E/\sim) \iff p \in \mathcal{P}(E)$
$\overline{p}$ désigne bien sûr la classe de p où $p \in E$

Démonstration $(\Longrightarrow ?)$
Soit $\overline{p} \in \mathcal{P}(E/\sim)$, si on écrit p sous la forme $p = qr$ dans E en passant aux classes on aura $\overline{p} = \overline{qr}$ soit grâce à la définition de la multiplication dans $E/\sim \qquad \overline{p} = \overline{q}\,\overline{r}$ et comme $\overline{p} \in \mathcal{P}(E/\sim)$ on aura $\overline{q}$ ou bien $\overline{r} \in (E/\sim)^*$ c'est à dire q ou bien $r \in E^*$ car les inversibles de $E/\sim$ sont les classes des inversibles de E comme il a été vu précédemment.
Donc , si on écrit $p = qr$ dans E alors q ou bien $r \in E^*$ i.e.que $p \in \mathcal{P}(E)$
$(\Longleftarrow ?)$
Soit $p \in \mathcal{P}(E)$, si on écrit dans $E/\sim \quad \overline{p} = \overline{q}\,\overline{r}$ alors $\overline{p} = \overline{qr}$ c'est à dire $p = \epsilon(qr)$ avec $\epsilon \in E^*$ soit aussi $p = (\epsilon q)r$ et comme $p \in \mathcal{P}(E)$ on en déduit que ϵq ou bien $r \in E^*$ ce qui revient à $\overline{\epsilon q} = \overline{q}$ ou bien $\overline{r} \in (E/\sim)^*$ vu que $\overline{\epsilon} = \overline{1}$.
En résumé pour $p \in \mathcal{P}(E)$ si on écrit dans $E/\sim \quad \overline{p} = \overline{q}\,\overline{r}$ on a $\overline{q}$ ou bien $\overline{r} \in (E/\sim)^*$ donc $\overline{p} \in \mathcal{P}(E/\sim)$ et ceci achève la preuve du théorème 3.

Théorème 4 A étant un acui ayant des éléments premiers$(\mathcal{P}(A) \neq \emptyset)$
$\forall p \in \mathcal{P}(A) \quad \forall a \in A$ on a l'alternative $p|a$ ou bien p est premier avec a(i.e.tout diviseur de p et a est inversible)

Démonstration En effet:
Si $p|a$ cqfd.
Et si $p \not| a$ comme $\mathcal{D}_p = A^* \bigcup pA^*$(cf les rappels) un diviseur d de p et a est forcément inversible sinon d serait un associé de p qui diviserait a et par conséquent p diviserait aussi a d'où une contradiction.

Théorème 5 A étant un acui ayant des éléments premiers$(\mathcal{P}(A) \neq \emptyset)$
"Dans un acui 2 premiers non associés sont premiers entre eux"
Soient p_1,$p_2 \in \mathcal{P}(A)$ avec $p_1 \not\sim p_2$ alors p_1 est premier avec p_2
En effet $\mathcal{D}_{p_1} = A^* \bigcup p_1 A^*$ et idem pour p_2 d'où si d divise p_1 et p_2 alors d est forcément inversible sinon ,comme $d|p_1 \quad d$ serait un associé de p_1 soit $d = \epsilon p_1$ qui diviserait p_2.On aurait alors :
• soit $\epsilon p_1 \in A^*$ et alors p_1 serait inversible d'où une contradiction
• soit $\epsilon p_1 \in p_2 A^*$ et alors p_1 et p_2 serait associés d'où encore une contradiction.

DEMI-GROUPES FACTORIELS

On sait combien est fondamentale l'UNICITE de la décomposition primaire dans le demi-groupe $(\mathbb{N}$,x) mais en général ce n'est pas le cas dans un demi-goupe quelconque.Exemple dans $(\mathbb{Z}$,x) on a $-15 = (-3).5 = 3.(-5)$ or si on convient d'utiliser uniquement les premiers positifs on récupèrera
l'unicité: $-15 = (-1).3.5$; -1 étant un facteur inversible.
Aussi comme la classe des associés d'un premier p n'est formée que de premiers on va choisir dans chacune de ces classes un représentant et on obtient ainsi un ensemble S appelé système représentatif des premiers de E.

Définition *(en s'inspirant de* $\mathbb{N}$*):*
On dira qu'un demi-groupe $(E$,x) est factoriel si et seulement s'il admet un élément absorbant noté 0, des premiers($\mathcal{P}(E) \neq \emptyset$) et si tout élément NON NUL de E admet une décomposition primaire unique après choix d'un système représentatif des éléments premiers de E.Autrement dit l'application:
E^*x$\mathbb{N}^{(S)} \ni (\epsilon,(\alpha_p)_{p\in S}) \mapsto \epsilon \prod_{p\in S} p^{\alpha_p} \in E \setminus \{0\}$ est une bijection où $\mathbb{N}^{(S)}$ désigne l'ensemble des familles d'entiers $(\alpha_p)_{p\in S}$ indexées par $p \in S$ dont tous les termes sont nuls sauf un nombre fini.
Tout élément $a \in E$ NON NUL s'écrit donc de manière unique sous la forme

(1) $\quad a = \epsilon_a \prod_{p\in S} p^{\alpha_p}$(c'est la décomposition primaire de a)

On notera que la décomposition primaire d'un élément inversible est réduite à lui-même avec $\forall p \in S \quad \alpha_p = 0$.On dira que ϵ_a est le facteur inversible de a puis que α_p est la valuation de a relative à p que l'on notera $val_p(a)$.

Exemples:
•$(\mathbb{N}$,x) est un demi-groupe factoriel.
$\mathbb{N}$ n'a qu'un seul inversible:1 donc on n'a pas le choix, le seul système représentatif des premiers possible est $S = \mathcal{P}(\mathbb{N})$.
L'existence et l'unicité de la décomposition primaire sont bien connues et se justifient en utilisant la relation d'ordre total:$\leq$ dans $\mathbb{N}$.
La décomposition de 1 étant 1 lui-même.
•$(\mathbb{Z}$,x) est un demi-groupe factoriel.On sait que $\mathbb{Z}^* = \{-1,1\}$ et que pour la relation $\sim$ la classe du premier p est $\overline{p} = \{p, -p\}$. Dès lors on peut choisir pour chaque classe le premier> 0 soit $|p|$ on obtient ainsi un système reprèsentatif des premiers de $\mathbb{Z}$ noté S et $S = \mathcal{P}(\mathbb{N})$.Dès lors l'application de $\mathbb{Z}^*$x$\mathbb{N}^{(S)} \longrightarrow \mathbb{Z} \setminus \{0\}$ définie par $(\epsilon,(\alpha_p)_{p\in S}) \longmapsto \epsilon \prod_{p\in S} p^{\alpha_p}$ est bijective.
Donc $\forall a(non\, nul) \in \mathbb{Z}$ a s'écrit de manière unique sous la forme:

$$a = \epsilon_a \prod_{p\in S} p^{\alpha_p}$$

On remarque que 1 et -1 ont pour décompositions primaires eux-mêmes
Quelques décomposition primaires:
$-150 = (-1).2.3.5^2 \qquad 1 = 1 \qquad 63 = (+1).3^2.7 \qquad -1 = -1$
On appelle **arithmétique factorielle** la partie de l'arithmétique qui est "calée" sur la **décomposition primaire unique** et dont le cadre naturel est le demi-groupe factoriel.
Ce qui suit est un cours d'arithmétique factorielle.

Arithmétique dans un demi-groupe factoriel $(A,\mathbf{x})$

Proposition *0:* *"tout élément non nul est simplifiable"*
$\forall(a,b,c) \in A^3 \quad a \neq 0$ et $ab = ac \Longrightarrow b = c$

Démonstration Si $b = 0$ il est clair que $c = 0$ et on a bien $b = c$.Idem si $c = 0$.
Si b et c ne sont pas nuls alors a,b,c admettent des décompositions primaires d'où avec des notations évidentes les décompositions primaires de ab et ac donnent

$$\epsilon_a\epsilon_b \sum_{p\in S} p^{\alpha_p+\beta_p} = \epsilon_a\epsilon_c \sum_{p\in S} p^{\alpha_p+\gamma_p}$$

d'où grâce à l'unicité de la décomposition primaire on a $\epsilon_a\epsilon_b = \epsilon_a\epsilon_c$ soit $\epsilon_b = \epsilon_c$ et aussi $\alpha_p + \beta_p = \alpha_p + \gamma_p$ soit $\beta_p = \gamma_p$ et donc $b = c$.

Proposition *1:*
a et b étant non nuls on aura: $a = \epsilon_a \prod_{p\in S} p^{\alpha_p}$ et $b = \epsilon_b \prod_{p\in S} p^{\beta_p}$ alors
$a|b \iff \forall p \in S \qquad \alpha_p \leq \beta_p \iff \forall p \in S \qquad val_p(a) \leq val_p(b)$

Démonstration C'est clair avec l'unicité de la décomposition primaire.
Alors il est immédiat que $\forall(a,b) \in A^2 \quad a|b$ et $b|a \iff \quad a \sim b$
En effet l'implication $(\Longleftarrow)$ est immédiate vu que 2 éléments associés se divisent mutuellement et réciproquement $a = bq$ et $b = ar \Longrightarrow ab = abqr$ or $ab \neq 0$ donc ab est simplifiable d'où $1 = qr$ et ainsi q et r sont inversibles.

Proposition *2:*
"Tout élément non inversible $a \in A$ admet un diviseur premier."

Démonstration Si $a = 0$ c'est clair car tout premier $p|0$
Si $a \neq 0$ alors a admet une décomposition primaire comme (1) alors
$\prod_{p\in S} p^{\alpha_p} \neq 1$ sinon $a = \epsilon_a \in A^*$ et une contradiction d'où un α_p au moins n'est pas nul et $p|a$.
Soit $\varphi : A \setminus \{0\} \mapsto A^*$ définie par $\varphi(a) = \epsilon_a$ le facteur inversible de a dans (1).

Proposition *3:*
$\forall(a,b) \in (A \setminus \{0\})^2 \qquad \forall\theta \in A^*$ on a:
$\varphi(ab) = \varphi(a)\varphi(b)$ à cause de l'unicité de la décomposition primaire
$\varphi(\theta) = \theta$

Démonstration c'est clair.

Définition On appellera "élément simple" tout élément a non nul de A tel que $\varphi(a) = 1$. Les éléments simples de A sont :1 et les produits finis de premiers de S.
Exemple:dans $\mathbb{Z}$ les éléments simples sont les entiers positifs si $S = \mathcal{P}(\mathbb{N})$.

Proposition *4:*
"Toute classe des associés d'un élément a non nul contient un élément simple."

Démonstration En effet $\overline{a} = \{\epsilon a \setminus \epsilon \in A^*\}$ alors si $\epsilon = \varphi(a)^{-1}$ on a ϵa qui est un élément simple de A vu que $\varphi(\epsilon a) = \varphi(\epsilon)\varphi(a) = \epsilon\varphi(a) = 1$.

Exemple:1 est l'élément simple de $A^* = \overline{1}$.

On pose $I_n = \{1,2,3,...,n\}$

Définition *: (un)pgcd et (le)PGCD*
Soit $a_1,a_2,a_3,....a_n$ des éléments de $A(n \geq 1)$;on dira que d est un plus grand commun diviseur des a_i si et seulement si d divise tous les a_i et si tout diviseur des a_i divise d.On notera alors $d = (un)pgcd(a_i)$ ou $d = pgcd(a_i)$.

Existence dans tous les cas d'un $pgcd(a_i)$

Si tous les $a_i = 0$ alors $pgcd(a_i) = 0$ et réciproquement.C'est facile à vérifier.
S'il existe au moins un $a_i \neq 0$,soit $I = \{i \in I_n / a_i \neq 0\}$ et $\forall i \in I \quad a_i = \epsilon_{a_i} \prod_{p \in S} p^{\alpha_p^i}$.
Posons $D = \prod_{p \in S} p^{\alpha_p}$ où $\alpha_p = Min_{i \in I}(\alpha_p^i)$ alors D est un $pgcd(a_i)$ car D divise bien sûr les $a_i = 0$ mais aussi les autres, vu que
$\forall i \in I \quad \forall p \in S \quad \alpha_p \leq \alpha_p^i$ (proposition 1).De plus tout diviseur d des a_i divise les $a_i \neq 0$ d'où $d \neq 0$ et si $d = \epsilon_d \prod_{p \in S} p^{\delta_p}$ on aura
$\forall i \in I \quad \forall p \in S \quad \delta_p \leq \alpha_p^i$ et par conséquent $\forall p \in S \quad \delta_p \leq \alpha_p$ soit $d|D$
On peut remarquer que D est simple donc $\varphi(D) = 1$.

Proposition *5:* "Deux $pgcd(a_i)$ sont associés."

Démonstration En effet si d et d' sont deux $pgcd(a_i)$ alors d divise les a_i donc d divise d' qui est un $pgcd(a_i)$ et de manière symétrique d' divise d et finalement d et d' sont associés.Dès lors si un des a_i au moins n'est pas nul chaque $pgcd(a_i) \neq 0$ donc la classe des associés de $pgcd(a_i)$ admet un élément simple qu'on appellera le plus grand commun diviseur des a_i et que l'on notera $PGCD(a_i)$ et qui n'est autre que le D précédent vu que $\varphi(D) = 1$.
$PGCD(a_i) = \prod_{p \in S} p^{Min_{i \in I}(\alpha_p^i)}$ où $I = \{i = 1$ à $n / a_i \neq 0\}$ avec $I \neq \emptyset$.

Définition *:*
On dira que des éléments $a_1,a_2,...a_n (n \geq 2)$ de A sont premiers entre eux si et seulement si les seuls diviseurs communs des a_i sont les inversibles de A.

Proposition *6:*
$a_1,a_2,...a_n$ sont premiers entre eux $\Leftrightarrow (un)pgcd(a_i) \in A^* \Leftrightarrow PGCD(a_i) = 1$

Démonstration La $2^{ième}$ équivalence étant évidente montrons la $1^{ière}$. Si les a_i sont premiers entre eux comme un $pgcd(a_i)$ est un diviseur des a_i nécessairement chaque $pgcd(a_i)$ est inversible. réciproquement si un $pgcd(a_i)$ est inversible comme tout diviseur commun des a_i divise ce $pgcd(a_i)$ donc ce diviseur commun est inversible aussi et les a_i sont bien premiers entre eux.

Proposition *7:*
Si les a_i ne sont pas tous nuls et que $PGCD(a_i) = D$ alors $D \neq 0$ et les $\frac{a_i}{D}$ sont premiers entre eux i.e. que $PGCD(\frac{a_i}{D}) = 1$.

Démonstration En effet comme D divise les a_i posons $a_i = Dq_i$ .Soit d un diviseur

des $\frac{a_i}{D} = q_i$ alors $q_i = dk_i$ d'où $a_i = Dq_i = Ddk_i$ donc Dd divise les a_i et par conséquent aussi $PGCD(a_i) = D$ soit $D = Ddr$;on simplifie par $D \neq 0$ (proposition 0) et l'on obtient $dr = 1$ d'où d est inversible i.e. les $\frac{a_i}{D}$ sont premiers entre eux.

Proposition *8:*
Si tous les a_i ne sont pas nuls et $m \neq 0$ alors $PGCD(m.a_i) = \epsilon_m^{-1}.m.PGCD(a_i)$

Démonstration Toujours avec $I = \{i \in I_n / a_i \neq 0\}$ et des notations évidentes on a
$\forall i \in I \quad ma_i = \epsilon_m \epsilon_{a_i} \prod_{p\in S} p^{\mu_p+\alpha_p^i}$ d'où $PGCD(ma_i) = \prod_{p\in S} p^{\alpha_p}$ où
$\forall p \in S \quad \alpha_p = Min_{i\in I}(\mu_p + \alpha_p^i) = \mu_p + Min_{i\in I}(\alpha_p^i)$
D'où $PGCD(ma_i) = \prod_{p\in S} p^{\mu_p+Min_{i\in I}(\alpha_p^i)} = \prod_{p\in S} p^{\mu_p} \prod_{p\in S} p^{Min_{i\in I}(\alpha_p^i)} = (\epsilon_m^{-1})m.PGCD(a_i)$ cqfd.

En particulier si m est simple i.e. $\epsilon_m = 1$ alors $PGCD(m.a_i) = m.PGCD(a_i)$
De plus il est clair que $(un)pgcd(m.a_i)$ et $(un)pgcd(a_i).m$ sont toujours associés ce qui est encore vrai si $m = 0$ ou si tous les $a_i = 0$ vu que $0 \sim 0$.

Définition *:(un)ppcm et (le)PPCM*
Avec les notations qui précèdent on dit que $M \in A$ est un plus petit commun multiple des a_i si et seulement si M est un multiple des a_i et si tout multiple commun m des a_i est multiple de M.On notera $M = (un)ppcm(a_i)$

Proposition *9:* "Existence dans tous les cas d'un $ppcm(a_i)$"

Démonstration •Si un des a_i est 0, tout multiple de 0 étant 0, alors seul 0 peut être $ppcm(a_i)$. On vérifie facilement que dans ce cas 0 est bien un $ppcm(a_i)$. Réciproquement si $ppcm(a_i) = 0$ alors un des a_i est 0.Sinon $a_1a_2...a_n$ serait un multiple non nul des a_i donc un multiple de $ppcm(a_i) = 0$ d'où une contradiction.
•Sinon tous les a_i sont non nuls et admettent donc une décomposition primaire unique $a_i = \epsilon_{a_i} \prod_{p\in S} p^{\alpha_p^i}$.Soit $M = \prod_{p\in S} p^{Max_{i\in I_n}(\alpha_p^i)}$ alors M est un $ppcm(a_i)$. En effet M est bien multiple des a_i car
$\forall p \in S \quad \forall i \in I_n \quad Max_{i\in I_n}(\alpha_p^i) \geq \alpha_p^i$ donc $\forall i \in I_n \quad a_i|M$(proposition 1).
De plus si m est un multiple des a_i alors ou $m = 0$ et $M|m$
ou bien $m \neq 0$ et comme $m = \epsilon_m \prod_{p\in S} p^{\mu_p}$ est multiple de chacun des a_i on a $\forall p \in S \quad \forall i \in I_n \quad \mu_p \geq \alpha_p^i$ et donc $\forall p \in S \quad \mu_p \geq Max_{i\in I_n}(\alpha_p^i)$ soit $M|m$.

Proposition *10:*
Deux $ppcm(a_i)$ sont associés.

Démonstration En effet soit m et m' deux $ppcm(a_i)$.
$m = (un)ppcm(a_i)$ donc m estun multiple des a_i donc il sera multiple de m' qui est aussi $(un)ppcm(a_i)$ donc $m'|m$ et par symétrie du rôle de m et m' on aura $m|m'$ et finalement m et m' sont associés.Dès lors si aucun des a_i n'est nul la classe des associés d'un $ppcm(a_i)$ contient un élément simple qu'on appellera le plus petit commun multiple des a_i, on le notera $PPCM(a_i)$,c'est le M précédent soit $M = \prod_{p\in S} p^{Max_{i\in I_n}(\alpha_p^i)}$ vu que $\varphi(\prod_{p\in S} p^{Max_{i\in I_n}(\alpha_p^i)}) = 1$.

La clé de voûte de l'arithmétique factorielle est la décomposition primaire unique et ses conséquences comme les théorèmes de Gauss et d'Euclide.

Théorème de Gauss:

$\forall(a,b,c) \in A^3$ a est premier avec b et $a|bc \Longrightarrow a|c$
Comme a est premier avec b alors a et b ne sont pas tous les deux nuls.
$a|bc \iff \exists d \in A \quad bc = ad$
Si $a = 0$ alors $bc = 0$ et comme $b \neq 0$ on a $c = 0$ et donc $a|c$
Si $b = 0$ comme a est premier avec b alors $a \neq 0$ et a est inversible(sinon a, d'après la proposition 2,admettrait un diviseur premier qui diviserait aussi $0 = b$ d'où une contradiction).Donc $a|c$ vu que $c = a(ca^{-1})$
Si $c = 0$ alors $a|c$
Si enfin a,b et c sont non nuls alors bc et ad ont la même décomposition primaire d'où après simplification des facteurs inversibles et avec des notations évidentes

$$\prod_{p\in S} p^{\beta_p} \prod_{p\in S} p^{\gamma_p} = \prod_{p\in S} p^{\alpha_p} \prod_{p\in S} p^{\delta_p}$$

d'où
$\beta_p + \gamma_p = \alpha_p + \delta_p$ ce qui implique $\forall p \in S \quad \alpha_p \leq \gamma_p$ sinon
il existerait $p \in S$ tel que $\alpha_p > \gamma_p \geq 0$ d'où $\alpha_p > 0$ et alors $p|a$ et puis $\beta_p = (\alpha_p - \gamma_p) + \delta_p \geq \alpha_p - \gamma_p > 0$ soit $\beta_p > 0$ et alors $p|b$.
On aurait alors p premier donc non inversible qui diviserait a et b d'où une contradiction.
Finalement on a bien $\forall p \in S \quad \alpha_p \leq \gamma_p$ ce qui implique $a|c$ d'après la proposition 1.

Théorème d'Euclide:

$\forall(a,b) \in A^2 \quad \forall p \in \mathcal{P}(A) \quad p|ab \Longrightarrow p|a$ ou $p|b$

En effet si a ou $b = 0$ c'est clair car $p|0$.Sinon,si a et $b \neq 0$ alors
p ne divise pas $a \Longrightarrow val_p(a) = 0$ et alors $p|ab \Longrightarrow val_p(ab) = val_p(a) + val_p(b) = 0 + val_p(b) = val_p(b) \geq 1 \Longrightarrow p|b$.

Voici quelques résultats classiques d'arithmétique factorielle dans un demi-groupe factoriel,en plus des précédents, sous forme de propositions concernant des éléments b_1,b_2,...,b_n de A tous non nuls.On posera $B = b_1b_2...b_n$.

proposition 11:
b_1,b_2,...,b_n premiers entre eux $\iff \forall p \in S \quad \exists i \in I_n = \{1,2,3...n\} \quad val_p(b_i) = 0$

($\Longrightarrow$?)
Sinon $\exists p \in S \quad \forall i \in I_n \quad val_p(b_i) \neq 0$ et alors p diviserait les b_i d'où p serait inversible ce qui est contradictoire.
($\Longleftarrow$?)
Sinon il existerait un diviseur non inversible des b_i donc aussi un diviseur premier

p(proposition 2) d'où on aurait $\forall i \in I_n \quad val_p(b_i) \neq 0$ et une contradiction.

Proposition *12:*
$\forall i \in I_n \quad a$ est premier avec $b_i \quad \Longrightarrow a$ est premier avec $b_1 b_2 ... b_n$

Démonstration Sinon il existerait un diviseur premier p de a et $b_1 b_2 .. b_n$ or $p | b_1 b_2 ... b_n$ $\Longrightarrow val_p(b_1 b_2 .. b_n) = val_p(b_1) + val_p(b_2) + ... + val_p(b_n) \geq val_p(p) = 1 \Longrightarrow \exists i \in I_n \quad val_p(b_i) \geq 1 \Longrightarrow p | b_i$ mais alors p diviserait a et b_i d'où une contradiction.

Proposition *13:*
Si les b_i sont premiers deux à deux alors $(un) ppcm(b_i) = b_1 b_2 ... b_n$.

Démonstration $\forall i \in I_n \quad b_i \neq 0$ donc b_i admet la décomposition primaire: $b_i = \epsilon_{b_i} \prod_{p \in S} p^{\beta_p^i}$
alors $\forall p \in S$ les β_p^i sont soit <u>tous nuls</u> soit <u>tous nuls sauf un</u>. sinon
$\exists (i,j) \in I_n^2 \quad i \neq j$ et $\beta_p^i > 0$ et $\beta_p^j > 0$ d'où on aurait $p | b_i$ et $p | b_j$ ce qui contredirait l'hypothèse.D'où avec des notations évidentes et pour tout p dans S on a $\sum_{i=1}^n \beta_p^i = 0$ ou bien $\sum_{i=1}^n \beta_p^i = \beta_p^{i_0} > 0$.
Alors $B = b_1 b_2 ... b_n$ est un $ppcm(b_i)$ i.e.B est un multiple des b_i ce qui est clair et tout multiple a des b_i est un multiple de B.
En effet si $a = 0$ alors $B | a$ et si $a \neq 0$ alors $a = \epsilon_a \prod_{p \in S} p^{\alpha_p}$
et $\forall i \in I_n \quad b_i | a \Longrightarrow \forall p \in S \quad \forall i \in I_n \quad \beta_p^i \leq \alpha_p$
Dès lors $\sum_{i=1}^n \beta_p^i$ soit est égal à 0 et alors $\sum_{i=1}^n \beta_p^i \leq \alpha_p$ soit $\sum_{i=1}^n \beta_p^i = \beta_p^{i_0}$ et là encore $\sum_{i=1}^n \beta_p^i = \beta_p^{i_0} \leq \alpha_p$
Finalement $\forall p \in S \quad \sum_{i=1}^n \beta_p^i \leq \alpha_p \Longrightarrow B | a$ car $val_p(B) = val_p(b_1 b_2 .. b_n) = \sum_{i=1}^n \beta_p^i \leq \alpha_p = val_p(a)$

Proposition *14:*
Si les b_i sont premiers deux à deux alors les $\frac{B}{b_i}$ sont premiers entre eux.

Démonstration En utilisant les notations précédentes on a

$$\forall i \in I_n \quad \frac{B}{b_i} = \prod_{j \neq i} b_j = (\prod_{j \neq i} \epsilon_{b_j}) \prod_{j \neq i} (\prod_{p \in S} p^{\beta_p^j}) = (\prod_{j \neq i} \epsilon_{b_j}) \prod_{p \in S} p^{\gamma_p^i}$$

avec $\gamma_p^i = \sum_{j \neq i} \beta_p^j$
Si d est un diviseur des $\frac{B}{b_i} \quad d$ n'est pas nul,il s'écrit $d = \delta \prod_{p \in S} p^{\delta_p}$ et alors $\forall p \in S \quad \forall i \in I_n \quad \delta_p \leq \gamma_p^i \, (2)$
Comme les b_i sont premiers deux à deux on a vu dans la proposition 13 que $\forall p \in S \quad \sum_{i=1}^n \beta_p^i = 0$ ou bien $\sum_{i=1}^n \beta_p^i = \beta_p^{i_0}$.
• si $\sum_{i=1}^n \beta_p^i = 0$ les β_p^i sont tous nuls d'où $\gamma_p^i = \sum_{j \neq i}^n \beta_p^j = 0$ et donc d'après $(2) \quad \delta_p = 0$
• si $\sum_{i=1}^n \beta_p^i = \beta_p^{i_0}$ alors $\forall j \neq i_0 \quad \beta_p^j = 0$ d'où $\gamma_p^{i_0} = \sum_{j \neq i_0} \beta_p^j = 0$ et donc d'après (2) avec $i = i_0 \qquad \delta_p = 0$
Finalement $\forall p \in S \quad \delta_p = 0$ c'est à dire que d est inversible et donc que les $\frac{B}{b_i}$ sont premiers entre eux.

Cette proposition 14 est utilisée dans un théorème fondamental d'algèbre linéaire:le théorème de décomposition des noyaux.

Proposition *15:*
$b = (un)ppcm(b_i) \iff \forall i \in I_n \quad b_i|b$ et les $\frac{b}{b_i}$ sont premiers entre eux.

Démonstration $(\Longrightarrow ?)$
$b = ppcm(b_i)$ donc par définition b est un multiple des b_i i.e. que $\forall i \in I_n \quad b_i|b$ et donc $\forall i \in I_n \quad \forall p \in S \quad \beta_p^i \leq \beta_p$ si on pose $b = \epsilon_b \prod_{p\in S} p^{\beta_p}$ vu que $b \neq 0$.
Par l'absurde,si les $\frac{b}{b_i}$ n'étaient pas premiers ils admettraient un diviseur non inversible donc un diviseur premier p(proposition 2) d'où on aurait $\forall i \in I_n \quad p|\frac{b}{b_i} \Longrightarrow val_p(p) \leq val_p(\frac{b}{b_i})$ soit $1 \leq \beta_p - \beta_p^i$
Or $b = (un)ppcm(b_i)$ est un associé de $PPCM(b_i)$ et par construction de $PPCM(b_i)$ on a $\beta_p = max_{i\in I_n}\beta_p^i = \beta_p^{i_0}$ d'où on aurait $\beta_p - \beta_p^{i_0} = 0$ ce qui contredirait l'inégalité précédente pour $i = i_0$. Finalement les $\frac{b}{b_i}$ sont bien premiers entre eux.
$(\Longleftarrow ?)$
$\forall i \in I_n \quad b_i|b$ donc b est bien un multiple des b_i.Il reste à montrer que tout multiple m des b_i est un multiple de b.
Si $m = 0$ alors m est bien multiple de b.
Si $m \neq 0$ alors posons $m = \epsilon_m \prod_{p\in S} p^{\mu_p}$.Comme les b_i divisent m on a $\forall i \in I_n \quad \forall p \in S \quad \beta_p^i \leq \mu_p$
De plus les $\frac{b}{b_i}$ sont premiers entre eux d'où d'après la proposition 11
$\forall p \in S \quad \exists i_0 \in I_n \quad val_p(\frac{b}{b_{i_0}}) = val_p(b) - val_p(b_{i_0}) = \beta_p - \beta_p^{i_0} = 0$
Donc $\forall p \in S \quad \exists i_0 \in I_n \quad \beta_p = \beta_p^{i_0} \leq \mu_p$ d'où $b|m$ i.e. que m est bien multiple de b.

ANNEAUX FACTORIELS

ANNEAUX FACTORIELS

On appellera anneau factoriel tout acui A dont le demi-groupe $(A$,x) est factoriel i.e. un acui ayant des premiers($\mathcal{P}(A) \neq \emptyset$) et pour lequel il existe une décomposition primaire unique pour tout élément non nul de A après choix(axiome du choix) d'un système représentatif S des premiers de A.
Autrement dit l'application de A^*x$\mathbb{N}^{(S)}$ dans $A \setminus \{0\}$ définie par
$(\epsilon,(\alpha_p)_{p\in S}) \longmapsto \epsilon \prod_{p\in S} p^{\alpha_p}$ est bijective.
Tout élément a non nul de A s'écrira de manière unique sous la forme $a = \epsilon_a \prod_{p\in S} p^{\alpha_p}$.
Dans ce chapitre,sauf avis contraire, A désignera un anneau factoriel.

LES PROPRIETES PRECEDENTES D'UN DEMI-GROUPE FACTORIEL SONT BIEN SUR VALABLES DANS UN ANNEAU FACTORIEL. ELLES CONSTITUENT L'ARITHMETIQUE FACTORIELLE.

Proposition *16:*
"caractérisation des éléments premiers d'un anneau factoriel grâce aux idéaux"
$p \in \mathcal{P}(A) \iff pA$ est un idéal premier non nul(i.e. A/pA est un anneau intègre et $pA \neq 0$).

Démonstration $(\Longrightarrow ?)$
D'abord $pA \neq 0$ car $p.1 = p \in pA$ et $p \neq 0$ vu qu'il est premier.
Ensuite $ab \in pA \Longrightarrow p|ab$ d'où comme A est factoriel $p|a$ ou $p|b$(théorème d'Euclide) soit $a \in pA$ ou $b \in pA$ et ainsi A/pA est bien intègre.

$(\Longleftarrow ?)$ Cette implication est vraie hors factorialité de l'anneau.
Soit $p = qr$ dans A alors $qr \in pA$ d'où $q \in pA$ ou $r \in pA$
•Si $q \in pA$ alors $q = pa$ et $p = par$ puis $p(1 - ar) = 0$ et comme $p \neq 0$ (sinon $pA = 0$) on a $ar = 1$ et donc $r \in A^*$ alors que $q \notin A^*$(sinon comme $q = pa$ et $a \in A^*$ on aurait $p \in A^*$ d'où $pA = A$ et A/pA serait l'anneau nul ce qui contredirait l'intégrité de A/pA) .En résumé on a q ou bien $r \in A^*$ i.e. $p \in \mathcal{P}(A)$.
•Si $r \in pA$ on procède de manière analogue.
Proposition *17: "écriture simplifiée des éléments de Q_A"*
Tout élément de Q_A s'écrit de manière unique sous la forme $\frac{a}{b}$ où b est un élément simple et $PGCD(a,b) = 1$.

Démonstration • Si $\frac{N}{D}(\neq 0) \in Q_A$ alors N et D ont une décomposition primaire qui permet de simplifier les facteurs premiers de S communs aux 2 décompositions et d'obtenir $\frac{n}{d}$.On peut écrire en décomposant n et d:

$$\frac{n}{d} = \frac{\epsilon_n \prod_{p\in S} p^{\nu_p}}{\epsilon_d \prod_{p\in S} p^{\delta_p}} = \frac{a}{b}$$

où $a = (\epsilon_n.\epsilon_d^{-1}) \prod_{p\in S} p^{\nu_p}$ et $b = \prod_{p\in S} p^{\delta_p}$; b est bien simple et il est clair que $PGCD(a,b) = 1$ vu que a et b n'ont aucun diviseur premier commun.
Prouvons maintenant l'unicité.
Si $\frac{a}{b} = \frac{a'}{b'}$ avec b et b' simples ainsi que $PGCD(a,b) = PGCD(a',b') = 1$ alors $ab' = a'b$ d'où $a|a'b$ et comme a est premier avec b on a $a|a'$(théorème de Gauss) et de même on a $a'|a$,finalement a et a' sont associés i.e. qu'il existe $\epsilon \in A^*$ tel que $a' = \epsilon a$.
Or $ab' = a'b \Longrightarrow \varphi(ab') = \varphi(a'b) \Longrightarrow \varphi(a)\varphi(b') = \varphi(a')\varphi(b)$ or $\varphi(b) = \varphi(b') = 1$ vu que b et b' sont simples d'où $\varphi(a) = \varphi(a') = \varphi(\epsilon a) = \varphi(\epsilon)\varphi(a) = \epsilon\varphi(a)$ soit $\varphi(a) = \epsilon\varphi(a)$ et enfin $\epsilon = 1$ vu que $\varphi(a)$ est inversible.
On a donc $a = a'$ d'où $ab' = ab$ et comme $a \neq 0$ a est simplifiable en vertu de la proposition 0;par conséquent $b = b'$ et on a bien l'unicité annoncée.
• Si $\frac{N}{D} = 0$ alors on convient de l'écrire $0 = \frac{0}{1}$ où l'on constate bien que 1 est un élément simple et $PGCD(0,1) = 1$.
Finalement on a bien l'unicité de l'écriture simplifiée des éléments de Q_A.

Remarque: tout élément a de A est aussi dans Q_A et à ce titre son écriture simplifiée sera $a = \frac{a}{1}$ le 1 étant bien un élément simple et $PGCD(a,1) = 1$

Exemple:avec $A = \mathbb{Z}$ on a $Q_A = \mathbb{Q}$ et les éléments simples de $\mathbb{Z}$ sont les entiers positifs(Si $S = \mathcal{P}(\mathbb{N})$).
L'écriture simplifiée de $\frac{1400}{-2750} = \frac{2^3.5^2.7}{-2.5^3.11} = \frac{2^2.7}{-5.11}$ sera donc $\frac{-28}{55}$.

Théorème de permanence de la factorialité(Gauss)

A est un anneau factoriel $\Longrightarrow$ $A[X]$ est un anneau factoriel.
(En fait Gauss a montré que $\mathbb{Z}[X]$ était factoriel.)

On adoptera pour les polynômes non nuls de $A[X]$ la notation:
$P = p_0 + p_1X + p_2X^2 + ...p_nX^n$ et $Q = q_0 + q_1X + q_2X^2 + ...q_kX^k$ etc...
Ces écritures supposent que $p_n \neq 0$ et $q_k \neq 0$ donc tous les coéfficients de P ne sont pas nuls et ainsi $PGCD(p_i)$ existe même si certains des p_i sont nuls.

Définition *:*
$P \in A[X]$ sera dit primitif si et seulement si les seuls diviseurs des coéfficients de P sont les inversibles de A ce qui revient à $P \neq 0$ et $PGCD(p_i) = 1$
c'est immédiat avec la proposition 6.

Lemme *de Gauss:*
P et Q primitifs $\Longrightarrow$ PQ est primitif.

Démonstration • Si P ou Q est constant, par exemple P, alors P constant et primitif implique P est inversible sinon P serait non inversible,il admettrait donc un diviseur premier(proposition 2)qui bien sûr ne serait pas inversible d'où une contradiction. P étant inversible on a $\epsilon_P = \varphi(P) = P$.De plus comme P est primitif on a $P \neq 0$ et idem pour Q donc $PQ \neq 0$ d'où d'après la proposition 8 $PGCD(Pq_i) = \epsilon_P^{-1}.P.PGCD(q_i) \Longrightarrow PGCD(Pq_i) = P^{-1}P = 1$ i.e. PQ est primitif.
• Si P et Q ne sont pas constants
Par l'absurde,si PQ n'était pas primitif ses coéfficients admettraient un diviseur non inversible qui admettrait lui-même en vertu de la proposition 2 un diviseur premier p;dès lors A/pA serait intègre(proposition 16) ainsi que $(A/pA)[Y]$ Soit ϕ l'application définie par
$A[X] \ni P = p_0 + p_1X + ..p_nX^n \quad \mapsto \quad \overline{p_0} + \overline{p_1}Y + ...\overline{p_n}Y^n \in (A/pA)[Y]$
C'est clair que $\phi(PQ) = \phi(P)\phi(Q)$.
On aurait $\phi(PQ) = \overline{0}$ car p diviserait tous les coéfficients de PQ or $\phi(P) \neq \overline{0}$ et $\phi(Q) \neq \overline{0}$ car p ne divise ni tous les coéfficients de P ni tous ceux de Q car P et Q sont primitifs d'où la contradiction, vu l'intégrité de $(A/pA)[Y]$.

Définition *:contenu d'un polynôme*
On rappelle que Q_A désigne le corps des fractions de A.On notera conformément à l'usage $\frac{a}{b}$ pour $cl(\frac{a}{b})$.
Si un polynôme $P \in Q_A[X]$ peut s'écrire sous la forme $P = \frac{a}{b}P'$ avec
$\frac{a}{b} \in Q_A \setminus \{0\}$ et $P' \in A[X]$ primitif on dira que$\frac{a}{b}$ est un contenu de P et alors nécessairement $P \neq 0$ car P' est primitif donc $P' \neq 0$.Le polynôme nul n'a donc pas de contenu et un contenu n'est pas nul par définition.

Proposition *18:*
"Deux contenus d'un polynôme non nul de $Q_A[X]$ sont associés sur A"

Démonstration $P = \frac{a}{b}P' = \frac{c}{d}P'' \Longrightarrow \exists \epsilon \in A^* \qquad \frac{a}{b} = \epsilon\frac{c}{d}$
Si on note p'_i les coéfficients de P' et p''_i ceux de P'' comme a,b,c,d sont tous non nuls les adp'_i ne sont pas tous nuls ainsi que les bcp''_i.On peut alors appliquer la proposition 8 et $adP' = bcP'' \Longrightarrow PGCD(adp'_i) = PGCD(bcp''_i)$ puis $\epsilon_{ad}^{-1}.ad.PGCD(p'_i) =$

$\epsilon_{bc}^{-1}.bc.PGCD(p_i'')$ soit $\epsilon_{ad}^{-1}.ad = \epsilon_{bc}^{-1}.bc$ CQFD.

On va montrer que tout polynôme non nul $P \in Q_A[X]$ admet un contenu.
Posons $P = p_0 + p_1X + ... + p_nX^n \in Q_A[X]$.D'après la proposition 17 tout p_i peut s'écrire de manière unique sous la forme $p_i = \frac{a_i}{b_i}$ avec $PGCD(a_i,b_i) = 1$ et b_i qui est simple.Comme tous les b_i sont non nuls on a $M = PPCM(b_i) \neq 0$ et si on pose$M = b_ic_i$ alors $p_i = \frac{a_i}{b_i} = \frac{a_ic_i}{b_ic_i} = \frac{a_ic_i}{M}$ d'où
$P = \frac{a_0c_0}{M} + \frac{a_1c_1}{M}X + ... + \frac{a_nc_n}{M}X^n = \frac{1}{M}(a_0c_0 + a_1c_1X + ... + a_nc_nX^n)$
Posons $D = PGCD(a_ic_i)$ d'où $PGCD(\frac{a_ic_i}{D}) = 1$(proposition 7) et
$P = \frac{D}{M}(\frac{a_0c_0}{D} + \frac{a_1c_1}{D}X + ... + \frac{a_nc_n}{D}X^n) = \frac{D}{M}P'$ avec $P' \in A[X]$ primitif.
Quant à $\frac{D}{M}$ on dira que c'est LE contenu de P et on le notera C_P.
D et M étant simples on aura $\varphi(D) = \varphi(M) = 1$.
Si $P \in A[X]$ est primitif alors $C_P = 1$ car pour $i = 1$ à $n \quad b_i = 1$ donc

$$M = PPCM(b_i) = 1$$

et $D = PGCD(a_ic_i) = PGCD(p_i) = 1$ car $p_i = \frac{a_i}{1} = a_i = a_ic_i$ vu que $M = b_ic_i$ donne $1 = 1c_i$ soit $c_i = 1$.

Théorème des contenus:

Pour tous polynômes P et Q NON NULS de $Q_A[X]$ on a $C_{PQ} = C_PC_Q$

En effet posons $C_P = \frac{a}{b}$,$C_Q = \frac{c}{d}$ et $C_{PQ} = \frac{e}{f}$ avec $P = C_PP'$,$Q = C_QQ'$ et $PQ = C_{PQ}R'$ où P',Q',R' sont primitifs dans $A[X]$.
On a $PQ = C_{PQ}R' = C_PP'C_QQ'$ ou $C_{PQ}R' = C_PC_QP'Q'$ d'où d'après le lemme Gauss et la proposition 18 $\exists \epsilon \in A^* \quad C_{PQ} = \epsilon C_PC_Q$ ce qui donne
$\frac{e}{f} = \epsilon\frac{a}{b}\frac{c}{d}$ d'où $ebd = \epsilon acf$ et vu que a,b,c,d,e,f sont simples
$\varphi(ebd) = \varphi(\epsilon acf)$ soit $\varphi(e)\varphi(b)\varphi(d) = \varphi(\epsilon)\varphi(a)\varphi(c)\varphi(f)$ puis $1 = \varphi(\epsilon)$ et enfin $\epsilon = 1$ d'où le résultat annoncé qui se généralise bien sûr pour 3 polynômes ou plus.

Proposition *19:valable dans un acui A quelconque, hors factorialité.*
"Les premiers constants de $A[X_i]$ sont les premiers de A"
$P \in \mathcal{P}(A[X_i])$ et $deg(P) = 0 \iff P \in \mathcal{P}(A)$

Démonstration $(\Leftarrow ?)$
En effet soit $P \in \mathcal{P}(A)$ et $P = QR$ dans $A[X_i]$.Comme $P \neq 0$ on a $Q \neq 0$ et $R \neq 0$ d'où $deg(P) = deg(Q) + deg(R) = 0 \Longrightarrow Q$ et $R \in A$
or $P \in \mathcal{P}(A)$ et par conséquent Q ou bien $R \in A^* = (A[X_i])^*$ soit $P \in \mathcal{P}(A[X_i])$.
$(\Longrightarrow ?)$
Soit $P \in \mathcal{P}(A[X_i])$ et $deg(P) = 0$ donc $P \in A$.Soit $P = QR$ dans A donc dans $A[X_i]$ comme $P \in \mathcal{P}(A[X_i])$ on en déduit que Q ou bien $R \in A[X_i]^* = A^*$ donc on a bien $P \in \mathcal{P}(A)$.

Proposition *20:*"Pour tout polynôme non constant et primitif de $A[X]$ la primalité sur A revient à la primalité sur Q_A."
Pour tout polynôme P primitif de $A[X]$ avec $deg(P) \geq 1$ on a

$P \in \mathcal{P}(A[X]) \iff P \in \mathcal{P}(Q_A[X])$

Démonstration $(\Longrightarrow ?)$
Soit $P = QR$ dans $Q_A[X]$.On a $C_P = C_Q C_R = 1$ car P est primitif. d'où $P = C_Q C_R Q'R' = Q'R'$ avec Q' et$R' \in A[X]$ or $P \in \mathcal{P}(A[X])$ d'où Q' ou bien $R' \in (A[X])^* = A^*$ par exemple $Q' \in A^*$ donc $Q = C_Q Q'$ est un élémént non nul de Q_A donc un inversible de Q_A et de $Q_A[X]$ alors que $deg(R') = deg(R) \geq 1$ vu que $deg(P) \geq 1$ d'où R n'est pas inversible dans $Q_A[X]$ et finalement $P \in \mathcal{P}(Q_A[X])$.
$(\Longleftarrow ?)$
Soit $P = QR$ dans $A[X]$ donc aussi dans $Q_A[X]$.Comme $P \in \mathcal{P}(Q_A[X])$ on a Q ou bien $R \in (Q_A[X])^* = Q_A \setminus \{0\}$ par exemple $Q \in Q_A \setminus \{0\}$ donc $deg(Q) = 0$ soit $Q \in A$ mais alors la constante Q divise P qui est primitif donc $Q \in A^* = (A[X])^*$ i.e. Q est inversible dans $A[X]$ alors que $deg(R) \geq 1$ vu que $deg(P) \geq 1$ d'où R n'est pas inversible dans $A[X]$ et finalement $P \in \mathcal{P}(A[X])$.

Pour prouver que $A[X]$ est un anneau factoriel définissons un système représentatif des premiers de $A[X]$.On prend d'abord pour représentants des polynômes premiers constants ceux de S,et pour les autres polynômes P avec $deg(P) \geq 1$, on choisit dans la classe $\overline{P}$ des associés de P le polynôme ayant son coéfficient dominant simple.On obtient ainsi un ensemble T et alors $S \cup T$ est le système désiré.

Existence d'une décomposition primaire dans $A[X]$.

Soit un polynôme NON NUL $P \in A[X]$.On a donc $P \in Q_A[X]$ qui est un anneau euclidien vu que Q_A est un corps et donc un anneau principal(bien connu) dont le système représentatif des premiers est formé des polynômes premiers UNITAIRES.Ainsi P admet la décomposition primaire unique $P = KP_1P_2...P_n$ dans $Q_A[X]$ où $K \in Q_A \setminus \{0\}$ et les P_i sont premiers unitaires avec $deg(P_i) \geq 1$.Or $P_i = C_{P_i}P'_i$ avec $P'_i \in A[X]$ primitif et donc $P'_i \in \mathcal{P}(Q_A[X])$ vu que $C_{P_i} \neq 0$ et $P_i \in \mathcal{P}(Q_A[X])$ implique $\frac{1}{C_{P_i}}P_i = P'_i \in \mathcal{P}(Q_A[X])$ d'où en vertu de la proposition 20 $P'_i \in \mathcal{P}(A[X])$.
On a donc $C_P P' = KC_{P_1}C_{P_2}...C_{P_n}P'_1P'_2...P'_n$ d'où d'après la proposition 18 il existe $\theta \in A^*$ tel que $\theta C_P = KC_{P_1}C_{P_2}...C_{P_n}$ avec $C_P \in A$ vu que $P \in A[X]$.D'où $P = \theta C_P P'_1P'_2...P'_n$. Or pour tout $i = 1$ à n il existe $\epsilon_i \in A^*$ tel que si on multiplie le coéfficient dominant de P'_i par ϵ_i on obtient un élément simple soit $\epsilon_i P'_i = P''_i \in T$.D'où $P = \theta C_P(\prod_{i=1}^n \epsilon_i^{-1})P''_1P''_2...P''_n$. En posant $a = \theta C_P(\prod_{i=1}^n \epsilon_i^{-1}) \in A$ et en décomposant a dans A on obtient $a = \epsilon_a \prod_{p\in S} p^{\alpha_p}$ et alors $P = \epsilon_a(\prod_{p\in S} p^{\alpha_p})P''_1P''_2...P_n$ ce qui constitue une décomposition primaire de P relative à $S \cup T$.

Unicité de la décomposition primaire dans $A[X]$.

Soit deux décompositions d'un même polynôme NON NUL de $A[X]$

$$\epsilon \prod_{p\in S} p^{\alpha_p} \prod_{P\in T} P^{\beta_P} = \epsilon' \prod_{p\in S} p^{\alpha'_p} \prod_{P\in T} P^{\beta'_P} (2)$$

Comme $P \in T$ il premier dans $A[X]$,avec $deg(P) \geq 1$ et son coéfficient dominant a_P est simple alors P est primitif(théorème de caractérisation des premiers de $A[X_i]$ où A est un acui).D'après la proposition 20 on en déduit que $P \in \mathcal{P}(Q_A[X])$ ainsi que $\frac{1}{a_P} P \in \mathcal{P}(Q_A[X])$ qui est est unitaire et qui est donc élément du système représentatif des premiers de $Q_A[X]$.
En remplaçant partout P par $a_P(\frac{1}{a_P} P)$ dans (2) on obtient:

$\epsilon \prod_{p\in S} p^{\alpha_p} \prod_{P\in T} a_P^{\beta_P} (\frac{1}{a_P} P)^{\beta_P} = \epsilon' \prod_{p\in S} p^{\alpha'_p} \prod_{P\in T} a_P^{\beta'_P} (\frac{1}{a_P} P)^{\beta'_P}$ puis

$[\epsilon \prod_{p\in S} p^{\alpha_p} \prod_{P\in T} a_P^{\beta_P}] \prod_{P\in T} (\frac{1}{a_P} P)^{\beta_P} = [\epsilon' \prod_{p\in S} p^{\alpha'_p} \prod_{P\in T} a_P^{\beta'_P}] \prod_{P\in T} (\frac{1}{a_P} P)^{\beta'_P}$

et compte tenu de l'unicité de la décomposition primaire dans $Q_A[X]$ on tire que les 2 scalaires entre crochets sont égaux et que $\forall P \in T \quad \beta_P = \beta'_P$ soit:

$$\epsilon \prod_{p\in S} p^{\alpha_p} \prod_{P\in T} a_P^{\beta_P} = \epsilon' \prod_{p\in S} p^{\alpha'_p} \prod_{P\in T} a_P^{\beta_P}$$

Après simplification on obtient $\epsilon \prod_{p\in S} p^{\alpha_p} = \epsilon' \prod_{p\in S} p^{\alpha'_p}$ et vu l'unicité de la décomposition dans A on en tire $\forall p \in S \quad \alpha_p = \alpha'_p$ et $\epsilon = \epsilon'$.
Finalement on a bien l'unicité de la décomposition primaire dans $A[X]$
relative à $S \cup T$.L'application
$A^* \text{x} \mathbb{N}^{(S)} \text{x} \mathbb{N}^{(T)} \ni (\epsilon,(\alpha_p)_{p\in S},(\beta_P)_{P\in T}) \mapsto \epsilon \prod_{p\in S} p^{\alpha_p} \prod_{P\in S} P^{\beta_P} \in A[X] \setminus \{0\}$
est bijective.

Exemples:
•$\mathbb{Z}$ est un anneau factoriel et même plus car il est euclidien donc principal.
$\mathbb{Z}^* = \{-1,1\}$ donc les classes d'associés ont 2 éléments opposés sauf
la classe de 0.On choisira comme système S représentatif des premiers de $\mathbb{Z}$ les positifs soit $S = \mathcal{P}(\mathbb{N})$.Il est clair que l'application:
$\mathbb{Z}^* \text{x} \mathbb{N}^{(S)} \ni (\epsilon,(\alpha_p)_{p\in S}) \quad \mapsto \quad \epsilon \prod_{p\in S} p^{\alpha_p} \in \mathbb{Z} \setminus \{0\}$ est bijective.
Preuve en s'appuyant sur la décomposition primaire unique dans $\mathbb{N}$.
Les éléments simples de $\mathbb{Z}$ sont les positifs.
$PGCD(0,0,-75,45,-60,0) = PGCD(0,0,-3.5^2,3^2.5,-2^2.3.5,0) =$
$3^{Min(1,2,1)}.5^{Min(2,1,1)} = 3.5 = 15$
$PPCM(39,-54,0,128) = 0$
$PPCM(-75,45,-60) = 2^{Max(0,0,2)}.3^{Max(1,2,1)}.5^{Max(2,1,1)} = 4.9.25 = 900$
•$\mathbb{Z}[X]$ est le "prototype" d'un anneau factoriel car il n'est pas principal.
$(\mathbb{Z}[X])^* = \mathbb{Z}^* = \{-1,1\}$ donc les classes d'associés ont 2 éléments opposés sauf la classe de 0. On choisira comme système représentatif des premiers de $\mathbb{Z}[X]$ l'ensemble $S \cup T$ où S est le système repésentatif des premiers de $\mathbb{Z}$ soit $S = \mathcal{P}(\mathbb{N})$et T est formé des premiers non constants dont le coéfficient dominant est simple i.e. positif.
Les éléments simples de $\mathbb{Z}[X]$ sont les polynômes à coéfficient dominant > 0

Exemple de décomposition primaire dans $\mathbb{Z}[X]$:
$P = -50x^3 + 70x^2 - 150x + 210 = (-1)2.5(5x-7)(x^2+3)$.$P$ n'est pas simple.

Il est très remarquable que la factorialité d'un acui A se transmette à l'anneau $A[X]$ des polynômes à une indéterminée sur A. D'où de proche en proche si A est factoriel $A[X_1]$ est factoriel puis $A[X_1,X_2]$ identifié à $A[X_1][X_2]$ l'est aussi ...etc $A[X_1,X_2,...X_n]$ est factoriel.
De plus,si A est un corps commutatif on sait que $A[X]$ est un anneau euclidien donc principal et enfin factoriel(théorèmes classiques).
Ainsi tout anneau de polynômes $A[X_i]$ à une ou plusieurs indéterminées et à coéfficients dans un anneau factoriel ou un corps commutatif A est un anneau factoriel qui,on va le voir dans le théorème 6, ne pourra être un anneau principal que si A est un corps et s'il n'y a qu'une seule indéterminée.

Théorème 6 A désignant un anneau factoriel ou un corps et $X_1,X_2...X_n$ des indéterminées $(n \geq 1)$
$A[X_i]$ est principal $\Longleftrightarrow$ A est un corps et n=1.

Démonstration $(\Longrightarrow ?)$
D'abord $n = 1$ sinon soit 2 indéterminées X_1 et X_2 qui sont aussi 2 polynômes premiers dans $A[X_i]$ vu qu'ils sont primitifs et de degré 1;de plus ils ne sont pas associés donc ils sont premiers entre eux(théorème 5) d'où d'après le théorème de Bézout il existerait 2 polynômes P et Q de $A[X_i]$ tels que $X_1P + X_2Q = 1$ ce qui est impossible car $X_1P + X_2Q$ n'a pas de terme constant donc on a bien $n = 1$.
Il reste à montrer que si $A[X]$ est un anneau principal alors A est un corps.
En effet soit $a \in A$ et $a \neq 0$ alors a et X sont premiers entre eux car un polynôme qui les divise est constant vu qu'il divise a et cette constante est inversible vu qu'elle divise X.En appliquant Bézout il existe donc P et $Q \in A[X]$ tels que $aP + XQ = 1$ or XQ n'a pas de terme constant d'où si $P = p_0 + p_1X + ...$ on a $ap_0 = 1$ donc a est inversible.CQFD
$(\Longleftarrow ?)$
Pour un corps K il est bien connu que $K[X]$ est un anneau euclidien
montrons qu'alors il est principal. Soit I un idéal de $K[X]$.
Il y a 3 cas à étudier:
1. I admet un polynome non constant (donc dans le cas contraire I ne sera formé que de polynômes constants d'où les cas 2. et 3.)
2. I n'a que le polynôme constant nul donc c'est bien un idéal principal
3. I contient un polynôme constant non nul:p alors $\frac{1}{p} \in K$ et $p.\frac{1}{p} = 1 \in I$ d'où $I = 1.K[X]$ et I est bien un idéal principal.
Etude du cas 1.
Notons $P \in I$ un polynôme non constant de degré minimum.
Alors $\forall M \in I \quad \exists (Q,R) \in (K[X])^2 \qquad M = PQ+R$ avec $R = 0$ ou $\deg(R) < \deg(P)$.
C'est la division d'Euclide de M par P d'où on tire $R = 0$ (sinon $R = M - PQ \in I$ ce qui contredirait la minimalité du degré de P.)
Par conséquent $M = PQ$ et donc $I \subset P.K[X]$. L'inclusion contraire étant évidente on en tire que $K[X]$ est bien principal.CQFD

Le théorème de permanence de la factorialité,de Gauss,en le répètant éventuellement plusieurs fois, nous permet d'affirmer que si A est un anneau factoriel alors
$A[X_1,X_2,...,X_n]$ est aussi factoriel pour tout $n \geq 1$ d'où il existe un système représentatif des premiers(srdp en abrégé) de $A[X_i]$ pour lequel il y a décomposition primaire unique.
Dès lors il est clair que pour tout autre srdp de $A[X_i]$ il y aura encore décomposition primaire unique vu que 2 premiers représentatifs d'une même classe d'association sont associés.
Par conséquent sur $A[X_i]$ on peut choisir pour srdp $S \bigcup T$ où S est un srdp de A qui représente les polynômes premiers constants et où T est formé en choisissant dans chaque classe des associés d'un polynôme premier non constant celui dont le dtol admet un coéfficient simple.

Lemme *Lemme ^{bis} de Gauss*(c'est le lemme de Gauss avec plusieurs indéterminées)
P et $Q \in A[X_i]$ sont primitifs $\Longrightarrow$ PQ est primitif.

Démonstration Un polynôme non nul comme P admet une décomposition primaire $P = \epsilon_P \prod_{p\in S} p^{\alpha_p} \prod_{P\in T} P^{\beta_P}$ alors
dire que P est primitif revient à $\forall p \in S \quad \alpha_p = 0$ c'est clair.
Alors,si $Q = \epsilon_Q \prod_{p\in S} p^{\alpha'_p} \prod_{P\in T} P^{\beta'_P}$ on aura aussi $\forall p \in S \quad \alpha'_p = 0$
d'où $PQ = \epsilon_P\epsilon_Q \prod_{P\in T} P^{(\beta_P+\beta'_P)}$ et PQ est bien primitif.

Proposition *20 ^{bis}* (c'est la proposition 20 valable aussi pour les polynômes à plusieurs indéterminées et à coéfficients dans un anneau factoriel A)

"Pour les polynômes primitifs et non constants de $A[X_i]$ la primalité sur A revient à la primalité sur Q_A."
$\forall P \in A[X_i]\, avec\, deg(P) \geq 1\, et\, P\, primitif : P \in \mathcal{P}(A[X_i]) \iff P \in \mathcal{P}(Q_A[X_i])$

On peut définir le contenu C_P d'un polynôme $P \in \mathcal{P}(Q_A[X_i])$ de la même façon que cela a déjà été fait pour un polynôme à une indéterminée puisque seuls les coéfficients sont pris en compte.
On a vu dans le $lemme^{bis}$ de Gauss que le produit de 2 polynômes primitifs de $A[X_i]$ est encore primitif.

Démonstration $(\Longrightarrow ?)$
Soit $P = QR$ dans $Q_A[X_i]$.Comme $Q = C_Q Q'$ et $R = C_R R'(Q' et R' \in A[X_i]$ étant primitifs) on a
$P = C_Q C_R Q'R' = \frac{a}{b} Q'R'$ en posant $C_Q C_R = \frac{a}{b}$ d'où $bP = aQ'R'$ or P et $Q'R'$ sont primitifs d'où en notant m_i les coéfficients de $Q'R'$ on a $PGCD(p_i) = PGCD(m_i) = 1$ puis comme $bP = aQ'R'$ avec a et b non nuls, de $PGCD(bp_i) = PGCD(am_i)$ on tire d'après la proposition 8 $\epsilon_b^{-1} bPGCD(p_i) = \epsilon_a^{-1} aPGCD(m_i)$ soit $\epsilon_b^{-1} b = \epsilon_a^{-1} a$ et enfin $\frac{a}{b} = \frac{\epsilon_a}{\epsilon_b} = \alpha \in A^*$. Dès lors $P = \alpha Q'R' = (\alpha Q')R'$ dans $A[X_i]$ et comme $P \in \mathcal{P}(A[X_i])$
on en déduit que $\alpha Q'$ ou bien $R' \in (A[X_i])^* = A^*$;celui qui est dans A^* n'est pas nul donc il est dans $Q_A \setminus \{0\} = (Q_A)^* = (Q_A[X_i])^*$ et l'autre est de degré≥ 1 (sinon P serait constant ce qui contredirait l'hypothèse) donc il n'est pas dans $Q_A \setminus \{0\} = (Q_A)^* = (Q_A[X_i])^*$. Or $\alpha Q'$ et Q' ont le même degré vu que $\alpha \neq 0$ donc on a Q' ou bien $R' \in (Q_A[X_i])^*$ et aussi $Q = C_Q Q'$ ou bien $R = C_R R' \in (Q_A[X_i])^* =$

$Q_A \setminus \{0\}$ vu qu'un contenu n'est pas nul,ce qui prouve bien que $P \in \mathcal{P}(Q_A[X_i])$.
($\Longleftarrow$?)
Par l'absurde.Comme $P \in A[X_i]$ est primitif de degré≥ 1 s'il n'était pas premier sur A d'après le "théorème de caractérisation..." on pourrait écrire $P = QR$ dans $A[X_i]$ donc dans $Q_A[X_i]$ avec $deg(Q)$ et $deg(R) \geq 1$ et cela contredirait la primalité de P sur Q_A qui est un corps.

Exemple:
$P = XY + 2X - 3Y \in \mathcal{P}(\mathbb{Z}[X,Y])$ car $P = (2X) + (X-3)Y$ en tant que polynôme en Y sur $\mathbb{Z}[X]$ est du premier degré et primitif vu que les diviseurs dans $\mathbb{Z}[X]$ de 2X sont -2,2,-X,X et aucun de ces derniers ne divise $X-3$.Donc $P \in \mathcal{P}(\mathbb{Z}[X][Y])$ d'après le "théorème de caractérisation..." et $P = XY + 2X - 3Y \in \mathcal{P}(\mathbb{Z}[X,Y])$ par polymorphie(théorème 1).
De plus P est primitif sur $\mathbb{Z}$ vu que le coéfficient de XY est 1 et P n'est pas constant d'où d'après la proposition 20 ^{bis} on a $P \in \mathcal{P}(\mathbb{Q}[X,Y])$.

EISENSTEIN

CRITERE D'EISENSTEIN

Désormais on est prêt à se lancer dans la détection des polynômes
premiers de $A[X_i]$ où A est un anneau factoriel.Le critère d'EISENSTEIN est un outil important de détection.
Ce critère d'EISENSTEIN est formé de conditions suffisantes pour qu'un
polynôme non constant à coéfficients dans un anneau factoriel et à une seule
indéterminée soit premier.Il y a plusieurs versions et même une valable dans un acui quelconque, i.e.hors factorialité, que voici:

EISENSTEIN I(version la plus générale)

Théorème (d'Eisenstein) A étant un acui: si

- $\exists p \in A$ tel que pA est un idéal premier non nul
- $P \in A[X]$ avec $P = a_0 + a_1X + ... + a_kX^k$ primitif et $deg(P) = k \geq 1$ $\Big\} \Longrightarrow$
- $p|a_0$,$p|a_1$,...,$p|a_{k-1}$ et $p^2 \not| a_0$

alors $P \in \mathcal{P}(A[X])$

Démonstration
D'abord pA étant un idéal premier non nul on a par définition A/pA est intègre et par conséquent $(A/pA)[Y]$ est aussi intègre on pourra donc utiliser le règle des degrés dans $(A/pA)[Y]$ .De plus p est premier d'après l'implication ($\Longleftarrow$?) de la proposition 16.
L'application f définie par :
$A[X] \ni M = m_0 + m_1X + ... + m_nX^n \quad \mapsto f(M) = \overline{m_0} + \overline{m_1}Y + ... + \overline{m_n}Y^n \in (A/pA)[Y]$ est clairement un morphisme d'anneaux.
Il est aussi clair que $\forall M \in A[X]$ et si $f(M) \neq 0 \quad deg(f(M)) \leq deg(M)$.
P est de degré≥ 1 et primitif d'où en vertu du théorème de caractérisation des premiers de $A[X_i]$ quand A est un acui, si P n'était pas premier on aurait:
$P = RS$ dans $A[X]$ avec $deg(R) \geq 1$ et $deg(S) \geq 1$ (I)
D'où $f(P) = f(RS) = f(R)f(S) = \overline{a_k}Y^k$ et $\overline{a_k} \neq \overline{0}$ (sinon on aurait $p|a_k$ et comme p divise les a_i pour $i = 1$ à $k-1$ alors on aurait le premier p qui diviserait les coéfficients du polynôme primitif P d'où une contradiction).
Par conséquent $deg(f(P)) = deg(P) = k$.
Comme $f(P) \neq \overline{0}$ on aurait $f(R) \neq \overline{0}$ et $f(S) \neq \overline{0}$ d'où $f(R)$,$f(S)$ auraient un degré et alors on aurait $deg(f(R)) \geq 1$ et $deg(f(S)) \geq 1$
[sinon par exemple on aurait $deg(f(R)) = 0$ et $deg(f(S)) = k$(règle des degrés dans $(A/pA)[Y]$ à partir de $f(P) = f(R)f(S)$ et vu que $deg(f(P)) = k$) or $deg(S) \geq deg(f(S)) = k \Longrightarrow deg(S) = k$ et donc $deg(R) = 0$ ce qui contredirait (I)].
Donc,toujours sous l'hypothèse d'absurde (I), on aurait bien $deg(f(R)) \geq 1$ et $deg(f(R)) \geq 1$
$f(R)f(S) = \overline{a_k}Y^k \Longrightarrow f(R)$,$f(S)$ seraient des monômes en Y.
En effet, en posant provisoirement et pour simplifier $f(R) = R'$, $f(S) = S'$ et $val(R')$ désignant la valuation du polynôme R',si R' n'était pas un monôme alors on aurait $val(R') < deg(R')$ et comme on a toujours $val(S') \leq deg(S')$ on aurait $val(R').val(S') < deg(R').deg(S')$ ou encore $val(R'S') < deg(R'S')$ et alors $R'S'$

ne serait pas un monôme d'où une contradiction.Finalement R' est bien un monôme et le même raisonnement avec S' à la place de R' montrerait que S' est aussi un monôme.De plus comme $R' = f(R)$ et $S' = f(S)$ seraient des monômes de degrés ≥ 1 leurs termes constants seraient nuls d'où si on posait $R = r_0 + r_1X + ...$ et $S = s_0 + s_1X + ...$ on aurait $\overline{r_0} = \overline{0}$ et $\overline{s_0} = \overline{0}$ i.e. $p|r_0$ et $p|s_0$ d'où $p^2|r_0s_0$ or $P = a_0 + a_1X + ... = RS = r_0s_0 + ...$ d'où $r_0s_0 = a_0$ et alors p^2 diviserait a_0 ce qui contredirait une des hypothèses. Finalement on a bien $P \in \mathcal{P}(A[X])$.c.q.f.d.
Comme on a $deg(P) \geq 1$ et que P est primitif on déduit de la proposition 20 que l'on a aussi $P \in \mathcal{P}(Q_A[X])$.

Remarque:on a mis l'hypothèse "$deg(P) = k \geq 1$" car les polynômes constants premiers on les connaît,ce sont les premiers de A(proposition 19).

EISENSTEIN II(version usuelle)

Théorème (d'Eisenstein)A étant un acui factoriel, si:

- $\exists p \in \mathcal{P}(A)$
- $P \in A[X]$ avec $P = a_0 + a_1X + ... + a_kX^k$ primitif et $deg(P) = k \geq 1$ $\Big\} \Longrightarrow$
- $p|a_0$,$p|a_1$,...,$p|a_{k-1}$ et $p^2 \not| a_0$

alors $P \in \mathcal{P}(A[X])$

Démonstration
Comme $p \in \mathcal{P}(A)$ et que A est factoriel,d'après la proposition 16, on a pA est un idéal premier non nul donc on peut appliquer l'énoncé précédent.

Exemple:$P = X + 5X^2Y - X^3Z^7 + Y^2 \in \mathcal{P}(\mathbb{Z}[X,Y,Z])$ car en interprétant P comme un polynôme de $\mathbb{Z}[X,Z][Y]$ i.e.un polynôme à une seule indéterminée Y et à coéfficients dans l'anneau factoriel $\mathbb{Z}[X,Z]$ soit
$P = (X - X^3Z) + (5X^2)Y + Y^2$ les conditions de EISENSTEIN II sont vérifiées car P est primitif vu que le coéfficient de Y^2 est 1 et de plus $p = X \in \mathcal{P}(\mathbb{Z}[X,Z])$ vu que X est primitif et du 1er degré(théorème de caractérisation des premiers de $A[X_i]$ où A est un acui). on a bien $X|(X - X^3Z^7)$,$X|5X^2$ et $X^2 \not|(X - X^3Z^7)$.Doù $P \in \mathbb{Z}[X,Z][Y]$
Dès lors on en déduit que les 7 interprétations de P par polymorphie sont premières sur leurs anneaux de scalaires respectifs(théorème 1).

EISENSTEIN III(autre version usuelle)

Théorème (d'Eisenstein)A étant un acui factoriel, si :

- $\exists p \in \mathcal{P}(A)$
- $P \in A[X]$ avec $P = a_0 + a_1X + ... + a_kX^k$ et $deg(P) = k \geq 1$ $\Big\} \Longrightarrow$
- $p|a_0$,$p|a_1$,...,$p|a_{k-1}$, $p \not| a_k$ et $p^2 \not| a_0$

alors $P \in \mathcal{P}(Q_A[X])$

Démonstration Par l'absurde.Si P n'appartenait pas à $\mathcal{P}(Q_A[X])$ comme Q_A est un corps,on pourrait écrire $P = QR$ dans $Q_A[X]$ avec $deg(Q) \geq 1$ et $deg(R) \geq 1$ en vertu du théorème de caractérisation des premiers de $A[X_i]$ où A est un acui.
Montrons qu'il existe $\lambda \in Q_A$ tel que $P = (\lambda Q)(\frac{1}{\lambda}R)$ avec λQ et $\frac{1}{\lambda}R \in A[X]$.
Il suffit de poser $\lambda = \frac{1}{C_Q}$ car P,Q,R sont non nuls donc on a $Q = C_Q Q'$ et $R = C_R R'$ avec Q',$R' \in A[X]$ et $C_{QR} = C_Q C_R$ d'où $\lambda Q = \frac{1}{C_Q}Q = Q' \in A[X]$ et $\frac{1}{\lambda}R = C_Q R = C_Q C_R R' = C_{QR}R' = C_P R' \in A[X]$ vu que $C_P \in A$ compte tenu de $P \in A[X]$ Dès lors on considèrera que $P = QR$ avec Q,$R \in A[X]$.
Posons $Q = b_0 + b_1 X + ... + b_m X^m$ et $R = c_0 + c_1 X + ... + c_l X^l$ où $m \geq 1$, $l \geq 1$ et $m + l = k$.Il est clair que $m < k$.
Comme $p|a_0 = b_0 c_0$ et que A est factoriel on a par exemple $p|b_0$(théorème d'Euclide) et p ne divise pas c_0 (sinon on aurait $p^2|a_0$ et une contradiction).
De plus p ne divise pas b_m vu que $b_m c_l = a_k$ et que p ne divise pas a_k donc il existe $m_1 \leq m$ tel que $p|b_0$,b_1...,b_{m_1-1} et $p \not| b_{m_1}$.De plus $1 \leq m_1$ car $p|b_0$. Il en résulte que p ne divise pas a_{m_1} (sinon comme $a_{m_1} = b_0 c_{m_1} + b_1 c_{m_1-1} + ... + b_{m_1-1}c_1 + b_{m_1}c_0$ et $p|b_0$,b_1,...,b_{m_1-1} on aurait $p|b_{m_1}c_0$ et donc $p|b_{m_1}$ ou $p|c_0$ d'où une contradiction).
Donc $p \not| a_{m_1}$ ce qui est contradictoire car $m_1 \leq m < k \Longrightarrow m_1 \leq k-1$ or par hypothèse on a $p|a_0$,a_1...,a_{k-1}
Finalement P est bien premier sur le corps Q_A des fractions de A.
Si en plus P est primitif on a aussi $P \in \mathcal{P}(A[X])$ (proposition 20)

Exemple:$P = -3Y + 6XZ^2 - 9X^2YZ + 5X^3 \in \mathbb{Z}[X,Y,Z]$
On peut considérer que $P \in A[X]$ où $A = \mathbb{Z}[Y,Z]$ est bien factoriel soit $P = (-3Y) + (6Z^2)X + (-9YZ)X^2 + (5)X^3$.
On peut appliquer EISENSTEIN III avec $p = 3 \in \mathcal{P}(\mathbb{Z})$ d'où en vertu de la proposition 19 on a $p = 3 \in \mathcal{P}(\mathbb{Z}[Y,Z])$.
On a aussi $deg|_X(P) = 3 \geq 1$ et enfin
$3|-3Y$; $3|6Z^2$; $3|-9YZ$; $3 \not| 5$ et $3^2 \not| -3Y$. D'où $P \in \mathcal{P}(Q_A[X])$
De plus P est primitif sur $A = \mathbb{Z}[Y,Z]$ vu qu'un diviseur $d \in \mathbb{Z}[Y,Z]$ des coéfficients de P divise 5 et par conséquent d=1,-1,5ou-5 or ni 5 ni -5 ne divisent -3Y donc d=1 ou -1 et P est bien primitif sur A. Comme $deg|_X(P) \geq 1$ on a aussi $P \in \mathcal{P}(A[X])$ en vertu de la proposition 20.Donc $P \in \mathcal{P}(\mathbb{Z}[Y,Z][X])$ et enfin par polymorphie $P \in \mathcal{P}(\mathbb{Z}[X,Y,Z])$.
Par contre on a bien $10P = -30Y + 60XZ^2 - 90X^2YZ + 50X^3 \in \mathcal{P}(Q_A[X])$ car $10P$ est associé de $P \in \mathcal{P}(Q_A[X])$ mais $10P \notin \mathcal{P}(\mathbb{Z}[X,Y,Z])$ car $10P$ n'est pas primitif vu que $5|10P$ et 5 n'est pas inversible puisqu'il est premier dans $\mathbb{Z}$ donc dans $\mathbb{Z}[Y,Z]$. La décomposition primaire de $10P$ dans $\mathbb{Z}[X,Y,Z]$ est: $10P = 2.5(-3Y + 6XZ^2 - 9X^2YZ + 5X^3)$ où l'on a choisi comme représentant d'un polynôme premier non constant celui dont le dtol(dernier terme dans l'ordre lexicographique) admet pour coéfficient un élément positif(i.e.simple dans $\mathbb{Z}$).En effet on a $dtol(10P) = 5X^3$ et $5 > 0$.

RECAPITULATIF DES PROPOSITIONS ET THEOREMES

RECAPITULATIF DES PROPOSITIONS ET THEOREMES

N'hésitez pas à me contacter $\rightsquigarrow$ guyphilippe2@aol.com.

Vos avis et remarques seront les bienvenus.