Université de Rennes

Arithmétique des anneaux

Le but de ce texte est de résumer les caractéristiques usuelles des anneaux et leurs relations. Les anneaux considérés sont tous unitaires et commutatifs.

Références principales

[B] Texte de David Bourqui
[C] Texte de Gaëtan Chennevier
[M] Marie-Paule Malliavin (*Algèbre commutative*)
[P] Daniel Perrin (*Cours d'algèbre*)

1. Propriétés de base

On cherche à décomposer chaque élément d'un anneau en briques élémentaires.

Définitions 1. *Deux éléments a et b d'un anneau sont dits* associés *si a divise b et b divise a.*
Un élément a d'un anneau A est dit

- inversible *s'il existe un élément b de A tel que $ab = 1_A$.*
- irréductible *s'il est non nul, non inversible et non produit de deux éléments non inversibles.*
- premier *s'il est non inversible et si pour tout $(b, c) \in A^2$, $(a \mid bc \implies a \mid b \text{ ou } a \mid c)$*

Proposition 1. *Soit A un anneau intègre.*

- *Deux élément a et b de A sont associés s'il existe un inversible u de A tel que $a = ub$ i.e. $(a) = (b)$.*
- *Un élément a est* irréductible *s'il est non nul, non inversible et si pour tout $(b, c) \in A^2$, $(a = bc \implies a \mid b \text{ ou } a \mid c)$ i. e. ses seuls diviseurs sont inversibles ou associés à a.*

Ces définitions ont des contreparties en termes (de grande taille) d'idéaux.

Définitions 2. *Un idéal $\mathcal{I}$ d'un anneau A est dit*

- premier *s'il est strictement contenu dans A et si pour tout $(b, c) \in A^2$, $(bc \in \mathcal{I} \implies b \in \mathcal{I} \text{ ou } c \in \mathcal{I})$*
- maximal *s'il est strictement contenu dans A et si tout idéal $\mathcal{J}$ de A vérifie $(\mathcal{I} \subset \mathcal{J} \subset A \implies \mathcal{J} = \mathcal{I} \text{ ou } \mathcal{J} = A)$.*

Les propriétés précédentes se caractérisent par la

Proposition 2. *Soit a un élément d'un anneau A et $\mathcal{I}$ un idéal.*

- *a est inversible $\iff (a) = A$.*
- *a est irréductible $\iff (a)$ est maximal parmi les idéaux principaux.*
- *$\mathcal{I}$ est premier $\iff A/\mathcal{I}$ est intègre.*
- *$\mathcal{I}$ est maximal $\iff A/\mathcal{I}$ est un corps.*

On dispose aussi des implications

Proposition 3. *Soit a un élément non nul et non inversible d'un anneau A et $\mathcal{I}$ un idéal. Alors,*
$\mathcal{I}$ maximal $\implies \mathcal{I}$ premier.
Si A est intègre, a premier $\implies a$ irréductible.

2. Recherche de diviseurs communs

La recherche des diviseurs communs à deux éléments conduit aux

Définitions 3. *Soit A un anneau. Deux éléments a et b de A sont dits*

— premiers entre eux *si tous leurs diviseurs communs sont inversibles i.e. si le seul idéal principal qui contient $(a) + (b)$ est A.*

— étrangers *si $(a) + (b) = A$.*

Définitions 4. *(Voir [B]) On dit qu'un anneau A intègre vérifie*

— le lemme d'Euclide *si ses éléments irréductibles sont premiers i.e. pour tout $(a, b, c) \in A^3$, si a est irréductible et $a \not| b$ alors $(a \mid bc \implies a \mid c)$.*

— le lemme de Gauss *si pour tout $(a, b, c) \in A^3$, si a et b sont premiers entre eux alors $(a \mid bc \implies a \mid c)$.*

— le théorème de Bézout *si ses éléments premiers entre eux sont étrangers.*

Proposition 4. *On a les implications :*

$$\text{Le théorème de Bezout} \implies \text{Le lemme de Gauss} \implies \text{Le lemme d'Euclide.}$$

3. Décomposition en produits d'irréductibles

Définitions 5. *Un anneau A est dit*

— noethérien *si chacun de ses idéaux $\mathcal{I}$ est engendré par un nombre fini d'éléments de $\mathcal{I}$ i.e. est de type fini.*

— atomique *s'il est intègre et si tout élément de A non nul et non inversible s'écrit comme produit d'irréductibles.*

— factoriel *s'il est intègre et si tout élément de A non nul et non inversible s'écrit comme produit d'irréductibles, de façon unique à l'ordre et à association près.*

— principal *s'il est intègre et si chacun de ses idéaux est principal. (Il suffit en fait de tester ses idéaux premiers. voir [M] page 38)*

— Euclidien *s'il est intègre et s'il existe une fonction $\nu : A - \{0\} \to \mathbb{N}$ telle que pour tout couple $(a, d) \in A \times (A - \{0\})$ il existe un couple $(q, r) \in A^2$ tel que $a = qd + r$ et $r = 0$ ou $\nu(r) < \nu(d)$.*

— intégralement clos *s'il est intègre et si tout élément de son corps de fractions, entier sur A, est en fait dans A.*

Proposition 5. — *Dans un anneau principal, les idéaux premiers non nuls sont maximaux.*

— *Dans un anneau factoriel, un élément irréductible engendre un idéal premier.*

— *Dans un anneau principal, un élément irréductible engendre un idéal maximal.*

Cette proposition est à comparer avec les implications de la proposition 3.

Proposition 6. *On a les implications suivantes*

$$\begin{tikzcd}
 & & \substack{A \text{ noethérien} \\ \text{et intègre}} \arrow[r, Rightarrow] & A \text{ atomique} \\
A \text{ Euclidien} \arrow[r, Rightarrow] & A \text{ principal} \arrow[r, Rightarrow] \arrow[ur, Rightarrow] \arrow[d, Rightarrow] & A \text{ factoriel} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] \arrow[d, Rightarrow] & \\
 & \text{Théorème de Bezout} \arrow[r, Rightarrow] & \text{Lemme de Gauss} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{Lemme d'Euclide} \\
 & & A \text{ intégralement clos} &
\end{tikzcd}$$

Plus précisément,

Théorème 1.

— *Un anneau atomique est factoriel si et seulement si il vérifie le lemme d'Euclide.*

— *Un anneau atomique est principal si et seulement si il vérifie le théorème de Bezout.*

Pour le premier item, on constate que le lemme d'Euclide assure l'unicité des décompositions en produit d'irréductibles. Pour le second item, un anneau atomique qui vérifie le théorème de Bezout est factoriel. L'existence du pgcd et le théorème de Bezout permettent de montrer d'abord que tout idéal de type fini est principal (On dit que A est un anneau de Bezout). On montre ensuite que dans un anneau factoriel toute suite croissante d'idéaux PRINCIPAUX est stationnaire. (Voir [B])

4. Autour de la notion de $pgcd$

Définitions 6. *Un* $pgcd$ *de deux éléments* a *et* b *d'un anneau* A *est un élément maximal (pour la relation de divisibilité) de l'ensemble des diviseurs communs de* a *et de* b.

Il résulte de la définition que deux $pgcd$ d'un même couple sont associés.

Proposition 7.

— *Dans un anneau factoriel, tout couple d'éléments admet un* $pgcd$ *construit à l'aide des valuations associées à chaque classe d'irréductibles modulo association.*

— *Dans un anneau principal, tout couple d'éléments* (a, b) *admet un* $pgcd$ *choisi comme générateur de* $(a) + (b)$.

5. Autour de la notion de dimension de Krull

Définitions 7.

— *Un anneau est dit* de dimension 0 *si ses idéaux premiers sont maximaux.*

— *Un anneau est dit* de dimension inférieure à 1 *si ses idéaux premiers non nuls sont maximaux.*

— *Un anneau est dit* Artinien *s'il est noethérien est de dimension 0.*

— *Un anneau est dit* de Dedekind *s'il est intègre, intégralement clos et de dimension inférieure à 1.*

Théorème 2.

— *Les anneaux principaux sont de Dedekind.*

— *Un anneau atomique est principal si et seulement si il est de dimension inférieure à 1.*

Pour montrer qu'un anneau atomique de dimension inférieure à 1 est principal, on montre en prenant un irréductible dans la décomposition d'un élément non nul et non inversible que les idéaux maximaux d'un anneau factoriel sont principaux. On considère ensuite grâce au lemme de Zorn un élément maximal de l'ensemble supposé non vide des idéaux non principaux et on montre qu'il est strictement inclus dans un idéal maximal, principal, et en travaillant dans le corps des fractions qu'il est principal. (voir [M] page 37)

6. Exemples d'anneaux

L'intégrité ne se conserve pas par passage au quotient.

La noethérianité se conserve par passage au quotient, par localisation et par passage de l'anneau A à l'anneau de polynômes $A[X_1, \cdots, X_n]$ en un nombre fini de variables.

Les exemples classiques d'anneaux euclidiens incluent l'anneau des entiers relatifs $\mathbb{Z}$; l'anneau des entiers de Gauss $\mathbb{Z}[i]$ et les anneaux de polynômes $k[X]$ en une variable à coefficients dans un corps k.

La factorialité se conserve par localisation et par passage à l'anneau $A[X_1, \cdots, X_n]$ en un nombre fini de variables et même à l'anneau $A[X_i]_{i \in \mathbb{N}}$. L'exemple $\mathbb{C}[X, Y, Z]/(X^2 - YZ)$ montre que la factorialité ne se conserve pas par quotient. Un analogue arithmétique : à l'aide de l'application norme $z = a + bi\sqrt{5} \mapsto z\overline{z} = a^2 + 5b^2$ multiplicative sur l'anneau intègre $\mathbb{Z}[i\sqrt{5}] = \frac{\mathbb{Z}[X]}{(X^2+5)}$ permet de montrer que ses inversibles sont 1 et -1, que 2 est irréductible. L'égalité $(1+i\sqrt{5})(1-i\sqrt{5}) = 2 \times 3$ montre alors que l'élément irréductible 2 n'est pas premier. L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est donc pas factoriel. Mais, comme c'est l'anneau des entiers de $\mathbb{Q}(i\sqrt{5})$ il est intégralement clos.

L'anneau $\mathbb{Z}[X]$ est factoriel, non principal : ses éléments premiers entre eux 2 et X ne sont pas étrangers. Il est par contre intègre et noethérien.

L'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos, car le nombre d'or $\frac{1+\sqrt{5}}{2}$ est solution de l'équation $X^2 - X - 1$. Il est par contre intègre et noethérien.