Anneaux principaux

1. Un exemple de plan (version très préliminaire)

Le titre est court : on pourrait légitimement s'attendre à trouver les mots « exemples et applications », mais alors la leçon serait nécessairement de niveau plus difficile

I-*Motivation et exemples*

a) - Considérons l'équation diophantienne $x^2 + y^2 = z^2$; on la factorise dans $\mathbb{Z}$ soit $x^2 = (z-y)(z+y)$. En utilisant la factorialité de $\mathbb{Z}$ et la notion de pgcd, on arrive alors aux solutions (x, y, z) proportionnel à $(m^2 - n^2, 2mn, m^2 + n^2)$;

- Si on veut appliquer la même technique à l'équation $x^3 = y^2 + d$ pour $d \equiv 1, 2 \mod 4$, on est amené à considérer l'anneau $\mathbb{Z}[i\sqrt{d}]$; la question est alors de savoir si cet anneau est factoriel ce qui sera le cas s'il est principal ou mieux euclidien.

Remarque : dans les anneaux de Dedekind, par exemple les anneaux d'entiers des extensions finies de $\mathbb{Q}$, la factorialité est équivalente à la principalité

b) Les exemples classiques découlent de l'implication euclidien $\Rightarrow$ principal :

- $\mathbb{Z}$, $\mathbb{Z}[i\sqrt{d}]$ avec $d = 1, 2, 3$: via la notion de pgcd on peut alors trouver les $n = x^2 + dy^2$;
- $K[X]$: notion de polynôme minimal d'un endomorphisme, d'un entier algébrique ;
- anneau des décimaux $D = \mathbb{Z}[X]/(10X - 1) = \{\frac{p}{q} \in \mathbb{Q} : \ p \wedge q = 1$ tel que $\exists a, b \in \mathbb{N}, \ q = 2^a 5^b\}$
- $K[[X]]$ (anneau séries de Laurent, de Roba...)
- les localisés

c) Quelques contre-exemples :

- $K[X]$ est principal si et seulement si K est un corps ; pour A factoriel $A[X]$ est factoriel sans être ni euclidien ni principal si A n'est pas un corps (on notera toutefois que si $Q \in A[X]$ a un coefficient dominant inversible, alors la division euclidienne de $P(X) \in A[X]$ par Q dans $Frac(A)[X]$ se passe en fait dans $A[X]$)
- $Z[i\sqrt{5}] : 9 = 3.3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ avec $3, 2 \pm i\sqrt{5}$ irréductible ; ainsi $(3, 2 + i\sqrt{5})$ est un idéal non principal.

II- *Anneaux de Dedekind*

Pour d'autres équations la factorisation nécessite en général l'introduction d'une extension finie K de $\mathbb{Q}$ dont l'anneau des entiers n'est alors plus nécessairement factoriel. Historiquement les idéaux ont été introduits par Kummer comme généralisation des nombres pour pallier à la non factorialité de l'anneau des entiers d'une extension finie de $\mathbb{Q}$. Ces « nouveaux nombres » était idéaux en ce que tout idéal s'écrit de manière unique comme produit d'idéaux premiers.

a) Un anneau de Dedekind est un anneau intègre, intégralement clos dont les idéaux premiers sont maximaux (i.e. de dimension 1) ; citons par exemple

- soit K une extension finie de $\mathbb{Q}$ et $\mathcal{O}_K$ son anneau des entiers i.e. la clôture intégrale de $\mathbb{Z}$ dans K, i.e. l'intersection de K avec l'anneau des entiers algébriques.
- l'anneau des entiers $\mathcal{O}_K$ de $K = \mathbb{Q}[\sqrt{d}]$ est $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \mod 4$ et $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \mod 4$.

b) groupe des classes d'idéaux

Définition : soient A un anneau intègre et K son corps des fractions. Un sous-module $\mathfrak{A}$ non nul de K est un **idéal fractionnaire** de A s'il existe $0 \neq \alpha \in A$ tel que $\alpha\mathfrak{A} \subset A$.

Tout idéal fractionnaire $\mathfrak{A}$ de A s'écrit d'une façon et d'une seule sous la forme $\prod_{\mathfrak{P}\in\mathcal{P}} \mathfrak{P}^{n_{\mathfrak{P}}(\mathfrak{A})}$ où les $n_{\mathfrak{P}}(\mathfrak{A})$ sont des entiers relatifs presque tous nuls.

Les idéaux fractionnaires d'un anneau de Dedekind A forment un groupe abélien $I(A)$ d'élément neutre A. Les idéaux fractionnaires principaux, i.e. de la forme Aa pour $a \in K^\times$, en forment un sous-groupe $F(A)$ et le groupe quotient $C(A) = I(A)/F(A)$ s'appelle **le groupe des classes d'idéaux de** A.

Le résultat principal sur le sujet est *la finitude* de $C(A)$ dont on note h_A son cardinal ; la preuve repose sur le fait qu'un idéal $\mathfrak{A}$ non nul de $\mathcal{O}_K$ contient un élément non nul x tel que

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |D_K|^{1/2} N(\mathfrak{A})$$

où $D_K \in \mathbb{N}$ est le discriminant de $\mathcal{O}_K$, i.e. $\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}} = (D_K)$.

Remarque : les corps quadratiques imaginaires $\mathbb{Q}(i\sqrt{d})$ ont un anneau des entiers principal si et seulement si $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

c) Retour sur la principalité : un idéal $\mathfrak{A}$ de $\mathcal{O}_K$ où K est une extension finie de $\mathbb{Q}$ peut être engendré par 2 éléments ; précisément pour $0 \neq a \in \mathfrak{A}$ arbitraire, il existe $\alpha \in \mathfrak{A}$ tel que $\mathfrak{A} = a\mathcal{O}_K + \alpha\mathcal{O}_K$.

Remarque : dans un anneau de Dedekind, principal est équivalent à factoriel ; par contre principal n'implique pas euclidien comme le montre l'exemple de $\mathcal{O}_K$ pour $K = \mathbb{Q}[i\sqrt{19}]$.

d) Retour sur la factorialité : nous avons vu que dans un anneau de Dedekind la factorialité était équivalente à la principalité ; le **théorème de Carlitz** affirme que si A est un anneau de Dedekind tel que $Cl(A)$ est fini et tel que toute classe non nulle contienne des idéaux premiers (par exemple si A est l'anneau des entiers d'un corps de nombres) alors A est semi-factoriel (i.e. toutes les factorisations en irréductibles de $a \in A$ ont la même longueur) si et seulement si $|Cl(A)| \leq 2$.

e) Comment rendre un idéal principal :

- Une première méthode pour rendre $\mathfrak{A}$ principal est de localiser $\mathcal{O}_K$ en un idéal premier $\mathfrak{P}$.
- Une autre technique est de considérer une extension finie K' de K. En effet soit h le nombre de classes de $\mathcal{O}_K$ de sorte que $\mathfrak{A}^h = (a)$ et soit $L = K(\alpha)$ avec $\alpha = a^{1/h}$. Dans $\mathcal{O}_K$, $\mathfrak{A}^h$ est principal et dans $\mathcal{O}_L$ on a $(\mathfrak{A}\mathcal{O}_L)^h = (\alpha)^h$ et donc d'après l'unicité de la décomposition en produits d'idéaux premiers, on a $\mathfrak{A}\mathcal{O}_L = (\alpha)$. L'inclusion $\mathfrak{A} \subset (\alpha) \cap \mathcal{O}_K$ est triviale, réciproquement soit $x \in (\alpha) \cap \mathcal{O}_K$ de sorte que $x = \lambda\alpha$ avec $\lambda \in \mathcal{O}_L$. On a $x^h = \lambda^h a$ et donc $\lambda^h \in \mathcal{O}_K$. En passant aux idéaux, on obtient dans $\mathcal{O}_K$, $(x)^h = (\lambda^h)\mathfrak{A}^h$ et donc $(\lambda^h) = \mathfrak{B}^h$ de sorte que $(x) = \mathfrak{B}\mathfrak{A}$ soit $x \in \mathfrak{A}$.

  On peut alors construire une extension L de K dans laquelle pour tout idéal $\mathfrak{A}$ de $\mathcal{O}_K$, $\mathfrak{A}\mathcal{O}_L$ est principal. En effet si $\mathfrak{A}$ et $\mathfrak{B}$ sont des idéaux dans la même classe, alors $\mathfrak{A}\mathcal{O}_L$ est principal si et seulement si $\mathfrak{B}\mathcal{O}_L$ l'est. Soit alors $\mathfrak{A}_1, \cdots, \mathfrak{A}_h$ un système de représentants du groupe des classes d'idéaux et soit $L = K(\alpha_1, \cdots, \alpha_h)$ avec les α_i comme précédemment. Ainsi pour tout $1 \leq i \leq h$, $\mathfrak{A}_i\mathcal{O}_L$ est principal d'où le résultat.

Remarque : le corps de classe de Hilbert (c'est l'extension abélienne non ramifiée maximale) vérifie aussi la propriété que tout idéal premier de K y devient principal.

Remarque : à partir de $K \subset L$ comme ci-dessus, il est aisé de comprendre la non factorialité de $\mathcal{O}_K$. Soit $a \in \mathcal{O}_K$ et $a = p_1 \cdots p_r$ "**la**" factorisation en irréductibles de $a \in \mathcal{O}_L$. On écrit dans $\mathcal{O}_K$, $(a) = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ avec d'après (3), $\mathfrak{P}_i\mathcal{O}_L = (p_i)$. Étant donnée une factorisation dans $\mathcal{O}_K$, $a = a_1 \cdots a_s$, en passant aux idéaux, on en déduit l'existence de σ tel que $(a_i) = \mathfrak{P}_{\sigma(n_{i-1}+1)} \cdots \mathfrak{P}_{\sigma(n_i)}$ de sorte que toute factorisation $a = a_1 \cdots a_s$ dans $\mathcal{O}_K$ s'obtient en

regroupant des orbites de l'action du groupe de Galois de L/K sur les p_i, i.e. il existe $\sigma \in \mathfrak{S}_r$ tel que pour tout $1 \leq i \leq s$, a_i et $p_{\sigma(n_{i-1}+1)} \cdots p_{\sigma(n_i)}$ sont associés dans OC_K.

III- *Modules sur les anneaux principaux*

a) classes d'équivalence des matrices à coefficients dans un anneau principal : facteurs invariants

b) applications :

– théorème de la base adaptée ;
– classification des groupes abéliens de type fini ;
– invariants de similitude d'un endomorphisme.

c) localisation lemme de Nakayama

...

1.1. Développements. —

– résolution de $p = x^2 + 2y^2$ pour p premier via l'étude de $\mathbb{Z}[i\sqrt{2}]$;
– étude de $\mathbb{Z}[i\sqrt{5}]$ qui n'est pas factoriel ; des exemples de couple d'éléments sans pgcd ; il vérifie la condition de Carlitz de sorte que toute décomposition en facteurs irréductibles a la même longueur ;
– Construction du groupe de classes d'idéaux et sa finitude...
– théorème de la base adaptée et applications à la classification des groupes abéliens de type fini ;
– localisation et lemme de Nakayama ; quelques applications...

2. Questions

Exercice 2.1. — *Décrivez* $\mathbb{Z}[X]/(2X-1)$.

Exercice 2.2. — *Montrez qu'un anneau est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal.*

Exercice 2.3. — *Soit A un anneau local d'idéal maximal $\mathcal{M}$.*

(i) Soient $f_1, \cdots, f_n \in A$ tels que $1 = \sum_{i=1}^n f_i$. Montrez que l'un des f_i est inversible.

(ii) Soient I et J deux idéaux de A et $a \in A$ un élément non diviseur de 0 tel que $IJ = (a)$. Montrez qu'il existe $x \in I$ et $y \in J$ tels que $xy = a$. En déduire que $I = (x)$ et $J = (y)$.

Exercice 2.4. — *Calculer les localisés $(\mathbb{Z}/n\mathbb{Z})_{(p)}$ et en déduire que l'application naturelle*

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \bigoplus_p (\mathbb{Z}/n\mathbb{Z})_{(p)}$$

est un isomorphisme de groupes.

Exercice 2.5. — *Soit A un anneau, prouvez ou donnez des contre-exemples aux implications suivantes :*

(i) ($\forall \mathcal{M}$ maximal, $A_{\mathcal{M}}$ est intègre) $\Rightarrow$ (A est intègre) ;
(ii) ($\forall \mathcal{M}$ maximal, $A_{\mathcal{M}}$ est principal) $\Rightarrow$ (A est principal) ;
(iii) ($\forall \mathcal{M}$ maximal, $A_{\mathcal{M}}$ est factoriel) $\Rightarrow$ (A est factoriel) ;
(iv) ($\forall \mathcal{M}$ maximal, $A_{\mathcal{M}}$ est réduit) $\Rightarrow$ (A est réduit) ;

Exercice 2.6. — *Soit M un A-module et $N \subset M$ un sous-A-module. Montrez que* $\mathrm{Ass}M \subset \mathrm{Ass}N \cup \mathrm{Ass}(M/N)$ *et que l'inclusion peut être stricte.*

Exercice 2.7. — *Soient A un anneau intègre et M un A-module, on note M_{tor} son sous-module des éléments de torsion. Montrez que pour toute partie S multiplicativement stable de A, on a $(S^{-1}M)_{tor} = S^{-1}M_{tor}$ puis montrez que les énoncés suivants sont équivalents :*
(i) M est sans torsion ;
(ii) pour tout idéal $\mathfrak{P}$ premier, $M_{\mathfrak{P}}$ est sans torsion ;
(iii) pour tout idéal $\mathcal{M}$ maximal, $M_{\mathcal{M}}$ est sans torsion.

3. Solutions

2.1 Il s'agit du sous-anneau de $\mathbb{Q}$ constitué des fractions p/q écrites sous forme irréductible avec q une puissance de 2 ; i.e. X est formellement l'inverse de 2...

2.2 Supposons A local d'idéal maximal $\mathcal{M}$ et soit $x \in A^\times$ inversible ; si x appartenait à $\mathcal{M}$ on aurait $\mathcal{M} = A$ ce qui n'est pas. Si $x \in A$ n'est pas inversible, d'après le lemme de Zorn, il appartient à un idéal maximal et donc à $\mathcal{M}$.

Réciproquement soit A un anneau tel que l'ensemble de ses éléments non inversibles est un idéal noté $\mathcal{M} \subsetneq A$. Soit alors $\mathcal{M}'$ un idéal maximal ; ses élément ne sont pas inversibles de sorte que $\mathcal{M}' \subset \mathcal{M}$ et par maximalité de $\mathcal{M}'$ on a $\mathcal{M}' = \mathcal{M}$.

2.3 (i) Si aucun des f_i est inversible alors d'après l'exercice précédent ils appartiennent tous à $\mathcal{M}$ et donc $1 \in \mathcal{M}$ ce qui n'est pas.

(ii) On a $a = \sum_i x_i y_i$ avec $x_i \in I$ et $y_i \in J$. Comme $x_i y_i \in IJ = (a)$, il existe $f_i \in A$ tel que $x_i y_i = a f_i$ ce qui donne $a = \sum_i a f_i$ et comme a n'est pas un diviseur de 0, on a $1 = \sum_i f_i$. D'après (i), il existe i tel que f_i est inversible de sorte que $a = f_i^{-1} x_i y_i$ soit $a = xy$ en posant $x = f_i x_i^{-1} \in I$ et $y = y_i$.

Soit $b \in A$ tel que $bx = 0$ et donc $ba = bxy = 0$ ce qui donne $b = 0$. Ainsi x et y ne sont pas des diviseurs de 0. Soit alors $z \in I$, comme $zy \in IJ = (a)$, on a $zy = ba = bxy$ et comme y n'est pas un diviseur de 0, on a $z = bx \in (x)$ de sorte que $I \subset (x)$. L'inclusion inverse est immédiate et donc $I = (x)$. Le cas de J se traite de manière similaire.

2.4 Si p ne divise pas n alors n est un élément inversible de $\mathbb{Z}_{(p)}$ de sorte que $n\mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}$ et donc $(\mathbb{Z}/n\mathbb{Z})_{(p)} \simeq \mathbb{Z}_{(p)}/n\mathbb{Z}_{(p)} = 0$.

Si $n = p^a m$ avec p ne divisant pas m, montrons que $(\mathbb{Z}/n\mathbb{Z})_{(p)} \simeq \mathbb{Z}/p^a\mathbb{Z}$. Considérons l'application naturelle $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})_{(p)}$: celle-ci est surjective. En effet pour $y/s \in \mathbb{Z}_{(p)}$ avec $s \notin (p)$, il existe $u, v \in \mathbb{Z}$ tels que $us + vp^a = 1$ de sorte que pour $x = uy$, on a $m(sx - y) = m(suy - y) = nvy$ et donc, comme $m \notin (p)$, l'image de $y/s \in \mathbb{Z}_{(p)}/n\mathbb{Z}_{(p)}$ est égale à $\pi(x)$.

Le noyau de π contient $p^a\mathbb{Z}$; réciproquement si $x \in \operatorname{Ker}\pi$, il existe alors $s \notin (p)$ tel que n divise sx. Comme s et p sont premiers entre eux on en déduit alors que p^a divise x, soit $x \in p^a\mathbb{Z}$.

L'isomorphisme de l'énoncé découle alors du lemme chinois.

2.5 (i) C'est faux, voici un contre-exemple : soit $A = A_1 \times A_2$ le produit de deux anneaux intègres. Les idéaux maximaux de A sont de la forme $\mathcal{M}_1 \times A_2$ ou $A_1 \times \mathcal{M}_2$ avec $\mathcal{M}_1$ et $\mathcal{M}_2$ des idéaux maximaux de A_1 et A_2 respectivement. Les localisés sont donc $A_{\mathcal{M}_1 \times A_2} \simeq (A_1)_{\mathcal{M}_1}$ et $A_{A_1 \times \mathcal{M}_2} \simeq (A_2)_{\mathcal{M}_2}$: en effet soit $A_{\mathcal{M}_1 \times A_2} \to (A_1)_{\mathcal{M}_1}$ qui à $(a_1, a_2)/(s_1, s_2)$ associe a_1/s_1. Ce morphisme est bien défini car si $(a_1', a_2')/(s_1', s_2')$ est un autre représentant de $(a_1, a_2)/(s_1, s_2)$ alors son image $a_1'/s_1' = a_1/s_1$. Ce morphisme est évidemment surjectif car $(a_1, 1_{A_2})/(s_1, 1_{A_2})$ est un antécédent de a_1/s_1. Si $(a_1, a_2)/(s_1, s_2)$ est dans le noyau alors $a_1/s_1 = 0$ de sorte qu'il

existe $s \notin \mathcal{M}_1$ tel que $s(a_1 - s_1) = 0$ mais alors $(s, 0_{A_2}) \notin \mathcal{M}_1 \times A_2$ et $(s, 0_{A_2})\Big((a_1, a_2) - (s_1, s_2)\Big) = s(a_1 - s_1) = 0$ ce qui signifie que $(a_1, a_2)/(s_1, s_2) = 0$ dans $A_{\mathcal{M}_1 \times A_2}$.

Ainsi les localisés de A par un idéal maximal quelconque sont intègres alors que visiblement A ne l'est pas.

(ii) C'est encore faux ; on reprend l'exemple précédent avec A_1 et A_2 principaux de sorte que tous leurs localisés sont principaux. Ainsi tous les localisés $A_{\mathcal{M}}$ sont principaux alors que A n'est même pas intègre.

(iii) C'est toujours faux ; le même exemple donne que pour A_1 et A_2 factoriel que tous les localisés $A_{\mathcal{M}}$ sont factoriel alors que A n'est même pas intègre.

Remarque : pour un contre-exemple avec A intègre, considérez $A = \mathbb{C}[X, Y]/(Y^2 - X^3 + X)$.

(iv) C'est vrai ! Soit a un élément nilpotent de A, il est encore nilpotent dans tout localisé de A. Comme $A_{\mathcal{M}}$ est réduit on a alors $a/1 = 0$ dans $A_{\mathcal{M}}$ pour tout idéal maximal $\mathcal{M}$, ce qui signifie que pour tout $\mathcal{M}$, il existe $s_{\mathcal{M}} \notin \mathcal{M}$ tel que $s_{\mathcal{M}} a = 0$. Ainsi l'annulateur $I_a := (0 : a)$ de a dans A n'est contenu dans aucun idéal maximal de sorte que $I = A$ et donc $1 \in I$ soit $1.a = a = 0$ et A est réduit.

2.6 Soit $0 \neq x \in M$ tel que $P = \mathrm{Ann}x$ soit premier ; si $Ax \cap N = 0$ alors tout élément y de l'intersection est tel que $\mathrm{Ann}y = P$ et donc $P \in \mathrm{Ass}N$. Si $Ax \cap N = 0$ alors l'application naturelle $A/P \hookrightarrow M \twoheadrightarrow M/N$ est injective et donc $P \in \mathrm{Ass}(M/N)$.

Pour le contre exemple, on peut prendre $2\mathbb{Z} \subset \mathbb{Z}$ avec $\mathrm{Ass}\mathbb{Z} = \{(0)\}$ alors que $\mathrm{Ass}(\mathbb{Z}/2\mathbb{Z}) = \{(2)\}$.

2.7 Si $0 \in S$ alors tous les localisés sont nuls, il n'y a donc rien à prouver, supposons donc $0 \notin S$ et soit $m \in M_{tor}$: $a \in A$ tel que $am = 0$. Pour tout $s \in S$, m/s est de torsion puisque $a/1.m/s = 0$ avec $a/1 \neq 0$ car A est intègre et $0 \notin S$. Ainsi $S^{-1}M_{tor} \subset (S^{-1}M)_{tor}$.

Réciproquement si $m/s \in (S^{-1}M)_{tor}$ il existe alors $a/t \in S^{-1}A$ non nul tel que $a/t.m/s = 0$, i.e. il existe $s' \in S$ tel que $s'am = 0$ et comme A est intègre et que $0 \notin S$, on a $s'a \neq 0$ et donc $m \in M_{tor}$.

L'implication $(i) \Rightarrow (ii)$ en découle directement ; $(ii) \Rightarrow (iii)$ étant évidente car maximal implique premier, il suffit de montrer $(iii) \Rightarrow (i)$. Soit $m \in M_{tor}$ et $I = \mathrm{Ann}(m)$. L'image de m dans $M_{\mathcal{M}}$ pour tout idéal maximal $\mathcal{M}$ est de torsion et comme $(M_{\mathcal{M}})_{tor} = (0)$, il existe $s \notin \mathcal{M}$ tel que $sm = 0$. Ainsi on a $I \not\subset \mathcal{M}$ pour tout idéal maximal $\mathcal{M}$ de A ce qui implique $I = A$ et donc $1.m = 0$ d'où le résultat.

Références