Anneaux et éléments d'anneaux remarquables

Dans cette feuille, A désigne un anneau commutatif.

1 Divisibilité dans les anneaux

Définition 1.1. *Soit $a, b \in A$. On dit que a **divise** b, et on note $a \mid b$, lorsqu'il existe $c \in A$ tel que $b = ac$. On dit que a et b sont **associés** lorsque $a \mid b$ et $b \mid a$.*

Exercice 1. *Montrer que a divise b si et seulement si $(b) \subset (a)$. En particulier, a et b sont associés si et seulement $(a) = (b)$.*

Proposition 1.2. *Si A est intègre, alors a et b sont associés lorsqu'il existe $u \in A^\times$ tel que $b = ua$.*

Démonstration. Si $b = ua$ avec $u \in A^\times$ alors $a \mid b$, et comme $a = u^{-1}b$, $b \mid a$. Réciproquement, si $a \mid b$ et $b \mid a$ alors il existe $c, d \in A$ tels que $b = ca$ et $a = db$, d'où $b = cdb$. Ainsi, $b(1 - cd) = 0$. Par intégrité, ou bien $b = 0$, auquel cas $a = 0$ et on a bien $b = 1a$, ou bien $(1 - cd) = 0$, autrement dit c et d sont inversibles dans A. □

Définition 1.3. *Soit $a \in A$. On dit que a est un **diviseur de zéro** lorsque $a \in A \setminus \{0\}$ il existe $b \in A \setminus \{0\}$ tel que $ab = 0$. On dit que a est **nilpotent** lorsqu'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$. On dit que a est un **élément régulier** lorsqu'il n'est ni nul, ni un diviseur de zéro.*

Remarque 1.4. Les éléments réguliers sont exactement les éléments **simplifiables** de A, c'est-à-dire ceux tels que $ab = ac$ implique $b = c$.

Exercice 2. *Soit $n \in \mathbb{N}^*$. Déterminer les diviseurs de zéro et les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.*

Définition 1.5. *Supposons que A est intègre et soit $a \in A$ non nul. On dit que a est **premier** lorsqu'il n'est pas inversible et pour tout $b, c \in A$,*

$$a \mid bc \Rightarrow a \mid b \text{ ou } a \mid c.$$

*On dit que a est **irréductible** lorsque a n'est pas inversible et lorsque l'écriture $a = bc$ avec $b, c \in A$ implique que b ou c est inversible.*

Exercice 3. *Montrer qu'un élément premier est irréductible. Montrer que la réciproque n'est pas toujours vraie.*

Proposition 1.6. *Supposons que A est intègre et soit $a \in A$. Alors a est premier si et seulement si $a \neq 0$ et (a) est premier.*

Définition 1.7. *Soit $a, b \in A$.*

1. *On dit que a et b admettent un* ***PGCD*** *(plus grand diviseur commun) dans A lorsque l'ensemble $\{d \in A \mid d \mid a, d \mid b\}$ admet un maximum pour la divisibilité. On note* $\mathrm{PGCD}(a, b)$ *l'idéal engendré par un tel PGCD.*

2. *On dit que a et b admettent un* ***PPCM*** *(plus petit commun multiple) dans A lorsque l'ensemble $\{m \in A \mid a \mid m, b \mid m\}$ admet un minimum pour la divisibilité. On note* $\mathrm{PPCM}(a, b)$ *l'idéal engendré par un tel PPCM.*

3. *On dit que a et b sont* ***premiers entre eux*** *lorsque* 1 *est un PGCD de a et b.*

Remarque 1.8. ⚠ Un PGCD ou un PPCM n'a pas de raison d'exister en général dans un anneau, et lorsqu'il existe, il n'est unique qu'à association près, ce qui justifie que les idéaux $\mathrm{PGCD}(a, b)$ et $\mathrm{PPCM}(a, b)$ sont bien définis.

Exercice 4. *Montrer que d est un PGCD de a et b si et seulement si (d) est un élément minimal (pour l'inclusion) de $\{(c) \mid c \in A, (a) + (b) \subset (c)\}$, et que m est un PPCM de a et b si et seulement si (m) est un élément maximal de $\{(n) \mid n \in A, (n) \subset (a) \cap (b)\}$.*

2 Anneaux factoriels

Définition 2.1. *On dit que A est un anneau factoriel lorsque :*

i) A est intègre.

*ii) Tout élément non nul de A est associé à un produit d'éléments irréductibles (**Propriété E**).*

*iii) Toute factorisation en produit d'irréductibles est unique : Si $\prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$ avec $p_1, \dots, p_r, q_1, \dots, q_s \in A$ irréductibles, alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $\forall i \in \{1, \dots, r\}, \exists u_i \in A^\times, q_i = u_i p_{\sigma(i)}$ (**Propriété U**).*

Remarque 2.2. Les facteurs irréductibles d'un élément non nul d'un anneau factoriel sont donc seulement définies à multiplication par un inversible près.

Exemple 2.3.

1. $\mathbb{Z}$ est un anneau factoriel en vertu du théorème fondamental de l'arithmétique.

2. Un corps est un anneau factoriel puisque tout élément non nul y est inversible, et donc admet une décomposition comme produit vide d'irréductibles.

3. L'anneau $A[X, X^{1/2}, \dots]$ n'est pas factoriel car il ne vérifie pas la propriété E.

4. L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car il ne vérifie pas la propriété U (voir les exercices).

Proposition 2.4 (Lemme d'Euclide)**.** *Si A est factoriel, alors un élément est premier si et seulement s'il est irréductible.*

Démonstration. Un élément premier étant toujours irréductible, il s'agit de montrer la réciproque. Soit donc $p \in A$ un élément irréductible et $a, b \in A$ tels que $p \mid ab$. Il existe donc $c \in A$ tel que $pc = ab$. Puisque A est factoriel, a et b admettent une décomposition en produit d'irréductibles, qui donne une telle décomposition pour ab. L'unicité de celle-ci implique que p intervient dans la décomposition de a ou de b, d'où $p \mid a$ ou $p \mid b$, autrement dit, p est premier. □

Proposition 2.5 (Lemme de Gauss)**.** *Si A est factoriel et $a, b, c \in A$ sont tels que $a \mid bc$ et a est premier avec b, alors $a \mid c$.*

Démonstration. Par hypothèse, il existe $d \in A$ tel que $ad = bc$. Si on écrit $b = p_1 \dots p_r$ et $c = q_1 \dots q_s$ les décompositions en produits d'irréductibles de b et c alors $ad = p_1 \dots p_r q_1 \dots q_s$, qui est donc la décomposition en produit d'irréductibles de ad. Mais on peut également obtenir celle-ci à partir de celles de a et de d, et la décomposition en produit d'irréductibles de a ne contient aucun irréductible associé aux p_i puisque a et b sont premiers entre eux. L'unicité de la décomposition en produits d'irréductibles de ad donne que les facteurs irréductibles de a sont associés à des q_j, autrement dit, que $a \mid c$. □

Remarque 2.6. En fait, le lemme d'Euclide est un cas particulier du lemme de Gauss, car un irréductible ne divise pas un élément donné de A si et seulement s'il est premier avec lui.

Proposition 2.7. *Supposons que A est un anneau factoriel. Pour $a, b \in A$ non nuls, écrivons*

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}$$

et

$$b = u \prod_{i=1}^{r} p_i^{\beta_i}$$

avec les p_i irréductibles deux à deux non associés, $\alpha_i, \beta_i \in \mathbb{N}$ et $u \in A^\times$. Alors $\prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$ est un PGCD de a et b et $\prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$ en est un PPCM.

Proposition 2.8. *Si A est factoriel et $a, b \in A$ sont non nuls, alors*

$$\mathrm{PGCD}(a, b)\mathrm{PPCM}(a, b) = (ab).$$

3 Anneaux principaux

Définition 3.1. *Un idéal de A est dit **principal** lorsqu'il est engendré par un élément. L'anneau A est dit **principal** lorsqu'il est intègre et tous ses idéaux sont principaux.*

Exemple 3.2.

1. $\mathbb{Z}$ est un anneau principal puisque ses sous-groupes sont monogènes, a fortiori ses idéaux.
2. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont tous principaux (voir les exercices), mais $\mathbb{Z}/n\mathbb{Z}$ n'est pas toujours un anneau principal.
3. Un corps est un anneau principal puisqu'il est intègre et ne possède que les idéaux (0) et (1).

Exercice 5. *Montrer que $\mathbb{Z}[X]$ n'est pas principal.*

Proposition 3.3. *Si A est un anneau principal et I est un idéal non nul de A, alors I est premier si et seulement s'il est maximal, si et seulement s'il est engendré par un élément irréductible de A.*

Démonstration. En effet, un idéal premier est engendré par un élément premier, donc irréductible et le caractère principal de A donne que cet idéal est maximal. Enfin, on sait qu'un idéal maximal est premier. □

Théorème 3.4. *Si A est principal alors A est factoriel.*

Démonstration. Commençons par remarquer que A est intègre par définition. Ensuite toute suite croissante d'idéaux de A est stationnaire. En effet, si $(I_n)_{n\in\mathbb{N}}$ est une telle suite, il existe $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de A telle que pour tout $n \in \mathbb{N}, I_n = (a_n)$ et $a_{n+1} \mid a_n$. La réunion I des I_n est un idéal de A puisque la suite est croissante, qui est donc principal : $I = (a)$ pour un $a \in A$. Pour tout $n \in \mathbb{N}$, on a $(a_n) \subset (a)$ d'où $a \mid a_n$. Réciproquement, $a \in \bigcup_{n\in\mathbb{N}}(a_n)$ donc il existe $n \in \mathbb{N}$ tel que $a_n \mid a$ et alors pour tout $m \geq n$, on a $(a_n) = (a)$.

Soit maintenant $a \in A$ non nul, et montrons que a possède une décomposition en produits d'irréductibles. Si a est inversible, le produit vide convient. Sinon a admet nécessairement un diviseur irréductible. En effet, soit a lui-même est irréductible, soit $a = d_0$ n'est pas irréductible et il admet donc un diviseur d_1 qui ne lui est pas associé. Si d_1 n'est pas irréductible, on trouve un diviseur d_2 qui ne lui est pas associé, etc. On construit ainsi une suite croissante d'idéaux de A, qui stationne à partir de l'idéal engendré par un élément irréductible p. On recommence avec l'élément a/p, et à nouveau on construit une suite croissante d'idéaux (c'est-à-dire une suite décroissante de diviseurs) qui doit stationner. Cela montre que a admet une décomposition en produits d'irréductibles.

Pour montrer l'unicité d'une telle décomposition à l'ordre et à association près, il suffit de montrer que A vérifie le lemme d'Euclide. Mais si p est un élément irréductible de A alors (p) est un idéal premier de A d'après la Proposition 3.3. □

Proposition 3.5 (Relation de Bézout)**.** *Supposons que A est principal et soit $a, b \in A$ non nuls. Alors il existe $u, v \in A$ tels que $au + bv = d$, où d est un PGCD de a et b. En particulier, a et b sont premiers entre eux si et seulement si $(a) + (b) = A$.*

Démonstration. L'idéal $(a, b) = (a) + (b)$ est principal puisque A est un anneau principal, écrivons-le (d). En particulier, $a \in (d)$ et $b \in (d)$ donc d divise a et b. De plus, si c est un diviseur commun à a et b, alors c divise d puisque $d \in (a) + (b)$ est de la forme $au + bv$ avec $u, v \in A$. Ainsi, d est un diviseur commun à a et b maximal pour la relation de divisibilité, c'est donc un PGCD de a et b. □

4 Anneaux euclidiens

Définition 4.1. *On dit que A est un **anneau euclidien** lorsqu'il est intègre et qu'il existe une fonction $\varphi : A \setminus \{0\} \to \mathbb{N}$, appelée **stathme**, telle que pour tout $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que :*

i) $a = bq + r$.

ii) $r = 0$ *ou* $\varphi(r) < \varphi(b)$.

*Les éléments q et r sont appelés **quotient** et **reste** de la division euclidienne de a par b.*

Exemple 4.2.

1. L'anneau $\mathbb{Z}$ est euclidien pour le stathme valeur absolue.
2. Si K est un corps alors $K[X]$ est euclidien pour le stathme degré (voir la feuille suivante).

3. Un corps est un anneau euclidien pour n'importe quel stathme.

4. Pour $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ avec $\overline{b} \neq \overline{0}$, on peut trouver $q, r \in \mathbb{R}$ tels que $a = bq + r$ avec $r = 0$ ou $|r| < |b|$. Quitte à prendre $a, b \in \{0, \dots, n-1\}$ alors $\overline{a} = \overline{b}\overline{q} + \overline{r}$ avec $\overline{r} = \overline{0}$ ou $\varphi(\overline{r}) < \varphi(\overline{b})$, avec $\varphi(\overline{k})$ le représentant de $\overline{k}$ dans $\{0, \dots, n-1\}$. Pourtant, $\mathbb{Z}/n\mathbb{Z}$ n'est pas toujours intègre, donc ce n'est pas toujours un anneau euclidien.

Remarque 4.3. ⚠ Les quotients et restes d'une division euclidienne n'ont pas de raison d'être uniques. C'est le cas dans les anneaux $K[X]$ avec K un corps (c'en est même un caractérisation, voir les exercices), mais par exemple dans $\mathbb{Z}$ muni du stathme valeur absolue, on a $7 = 2.3+1 = 3.3-2$. Dans ce cas précis on peut retrouver l'unicité en imposant la positivité du reste, mais il n'y a pas de généralisation.

Théorème 4.4. *Si A est euclidien alors A est principal.*

Démonstration. C'est la démonstration usuelle dans $\mathbb{Z}$: on prend I un idéal non nul et on montre qu'il est engendré par un élément de stathme minimal. □

Remarque 4.5. La réciproque est fausse. Par exemple, l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal et non euclidien.

5 Autres classes d'anneaux

Dans cette section, on rassemble un peu de terminologie sur des classes plus générales d'anneaux et on discute de leurs relations.

Définition 5.1.
1. *On dit que A est **noethérien** lorsque toute suite croissante d'idéaux est stationnaire.*

2. *On dit que A est **à PGCD** lorsque tout couple d'éléments non tous nuls admet un PGCD dans A.*

3. *On dit que A est **de Bézout** lorsque pour tout $a, b \in A$, l'idéal (a, b) est principal.*

4. *On dit que A est un **atomique** lorsqu'il est intègre et vérifie la propriété E.*

On a vu qu'un anneau factoriel est à PGCD. La réciproque est fausse (considérer par exemple l'anneau des entiers algébriques, que l'on définira plus tard). De même, un anneau factoriel n'est pas nécessairement noethérien, et en particulier il n'est pas nécessairement principal.

Dans la démonstration du fait qu'un anneau principal est factoriel, on a montré qu'un anneau principal est noethérien, ce qui a permis de montrer qu'il vérifie la propriété E, autrement dit qu'il est atomique, et vérifie le lemme d'Euclide, ce qui a permis de montrer qu'il vérifie la propriété U. On a également établi qu'un anneau principal est de Bézout.

⚠ Un anneau noethérien vérifie la propriété E (procéder comme dans la démonstration du Théorème 3.4) mais n'est pas nécessairement atomique car il n'est pas forcément intègre.

6 Exercices

Exercice 6. *Déterminer les idéaux de $\mathbb{Z}/n\mathbb{Z}$, avec $n \geq 2$.*

Exercice 7. *Quels sont les éléments irréductibles de $\mathbb{Z}/n\mathbb{Z}$, pour $n \geq 2$? On pourra oublier la clause d'intégrité pour cet exercice. (Indication : Considérer le PGCD de n et a, où $\overline{a}$ est irréductible.)*

Exercice 8. *Montrer que $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un anneau et qu'il est euclidien pour le stathme $N : a + ib \mapsto a^2 + b^2$.*

Exercice 9. *Soit A l'anneau $\mathbb{Z}[i\sqrt{5}] = \{a+ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$. On définit $N : a+ib\sqrt{5} \mapsto a^2+5b^2$.*

1. *Montrer que $N(ab) = N(a)N(b)$ pour tout $a, b \in A$.*
2. *Déterminer $A^\times$.*
3. *En contemplant l'égalité $2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, montrer que A n'est pas factoriel.*

Exercice 10. *Montrer que $A = \mathbb{C}[X, Y]/(X^2 - Y^3)$ n'est pas factoriel. (Indication : Montrer que $y = \overline{Y}$ est irréductible mais pas premier. On pourra admettre que $\mathbb{C}[X, Y]$ est factoriel et utiliser que tout élément de A s'écrit sous la forme $A(y) + xB(y)$, avec $A, B \in \mathbb{C}[Y]$ et où $x = \overline{X}$.)*

Exercice 11. *Montrer que si A est un anneau intègre, $a, b \in A$ admettent un PPCM, alors ils admettent un PGCD.*

Remarque. La réciproque est fausse ! Par exemple dans $\mathbb{C}[X, Y, Z, T]/(XY - ZT)$, les éléments $\overline{X}$ et $\overline{Z}$ ont pour PGCD 1 mais n'ont pas de PPCM.

Exercice 12. *Montrer qu'un anneau atomique est factoriel si et seulement s'il vérifie le lemme d'Euclide.*

Exercice 13. *Montrer qu'un anneau factoriel de Bézout est principal.*

Exercice 14. *Montrer que $\mathcal{C}^0(I)$ n'est pas principal. (Indication : Considérer l'idéal des fonctions s'annulant en un point donné.)*

Exercice 15. *Montrer que l'anneau $\mathbb{Z}[(X_n)_{n\in\mathbb{N}}]$ n'est pas noethérien.*

Remarque. Cet anneau est cependant factoriel, comme on le verra dans la feuille suivante.

Exercice 16. *Montrer que $\mathbb{Z}[X]$ est un anneau à PGCD qui n'est pas de Bézout. (On pourra admettre que si A est factoriel alors $A[X]$ l'est.)*

Exercice 17. *Montrer qu'un anneau commutatif A est noethérien si et seulement si tous ses idéaux sont de type fini.*

Exercice 18. *Soit $P_1 = X^2 + 1 \in \mathbb{Z}[X]$ et $P_2 = 3 \in \mathbb{Z}[X]$. Montrer que pour tout $n \in \mathbb{Z}$, $P_1(n)$ et $P_2(n)$ sont premiers entre eux mais qu'il n'existe pas de polynômes $U_1, U_2 \in \mathbb{Z}[X]$ tels que $U_1P_1 + U_2P_2 = 1$.*

Exercice 19. *Soit p un nombre premier. On note $\mathbb{Z}_{(p)}$ l'ensemble*

$$\left\{ \frac{a}{p^n} \in \mathbb{Q} \mid a \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Montrer que $\mathbb{Z}_{(p)}$ est un anneau principal.

Exercice 20. *Soit A un anneau euclidien pour un stathme t.*

1. *Montrer que l'on peut supposer que $t(ab) \geq t(a)$ pour tout $a, b \in A \setminus \{0\}$, et que $t(1) = 0$.*
2. *Montrer qu'alors un élément $u \in A$ est inversible si et seulement si $t(u) = 0$.*
3. *On suppose maintenant que pour tout $a, b \in A$ avec $b \neq 0$, le couple (q, r) de la division euclidienne de a par b est unique.*
   (a) *Montrer par l'absurde que pour tout $a, b \in A \setminus \{0\}$ avec $a \neq -b$, $t(a+b) \leq \max(t(a), t(b))$.*
   (b) *En déduire que $A^\times \cup \{0\}$ est un corps.*
   (c) *Supposons que A ne soit pas un corps. Justifier qu'il existe un élément $x \in A$ tel que $t(x)$ soit strictement positif et minimal pour cette propriété.*
   (d) *Montrer que tout élément de A admet une écriture unique sous la forme $\sum_{k=0}^{n} a_k x^k$ avec les a_k inversibles dans A. (On pourra s'inspirer de la démonstration de l'existence et l'unicité de l'écriture d'un entier en base 10)*
   (e) *En déduire que A est isomorphe à un anneau de polynômes sur un corps.*