Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 7 – Propriétés d'anneaux

On fixe A un anneau commutatif unitaire et intègre.

1 Propriétés d'anneaux

Nous avons vu que la notion d'anneau est calquée sur les propriétés algèbriques de $(\mathbb{Z}, +, \cdot)$, ce dernier exemple vérifie cependant un certain nombre de propriétés supplémentaires, que l'on peut éventuellement demander à un anneau. Nous introduisons maintenant certaines de ces notions, de la plus générale à la plus restrictive. Cette partie du cours sera de fait sensiblement plus abstraite que les autres sections. Le cas échéant, elle pourra donc ne faire l'objet d'une lecture que plus tard, lorsque vous aurez acquis une meilleure intuition des anneaux dans leur généralité.

1.1 Anneaux factoriels

Un des éléments centraux de l'étude des nombres entiers est l'unique décomposition en facteurs premiers. Nous avons retrouver ce phénomène dans le cadre des polynômes. Le lecteur attentif aura toutefois remarqué que dans un cas, celui des entiers, on décomposait chaque élément en produit de facteurs *premiers*, tandis que dans l'autre, celui des polynômes, les facteurs étaient *irréductibles*. Nous commencerons donc par clarifier la distinction entre ces deux notions, pour nous placer ensuite dans un cadre où ces deux notions coïncident.

Remarque 1.1.1. Les éléments premiers ou irréductibles ayant vocation à être les facteurs d'uniques décompositions, on pourra se convaincre que ces deux notions concernent ni 0, qui est absorbant, ni les inversibles, qui peuvent toujours être rajoutés artificiellement en facteur.

Définition 1.1.2. Soit $a \in A^* \setminus A^\times$.

- On dit que a est *irréductible* s'il n'est pas le produit de deux éléments non inversibles. Cela revient à dire que si $a = b.c$ avec $b, c \in A$, alors b ou c est inversible.
- On dit que a est *premier* si, pour tout $b_1, b_2 \in A$ tels que $b_1.b_2 \in (a)$, on a $b_1 \in (a)$ ou $b_2 \in (a)$. Cela revient à dire que a vérifie le critère d'Euclide, à savoir que si un produit est un multiple de a, alors l'un des facteur au moins est un multiple de a.

Exemples 1.1.3.

- Dans $\mathbb{Z}$, les éléments premiers et les éléments irréductibles sont les mêmes, et ils correspondent aux nombres premiers et leurs opposés.
- Dans $\mathbb{C}[X]$, les éléments premiers et les éléments irréductibles sont les mêmes, et ils correspondent aux polynômes de degré 1. Dans $\mathbb{R}[X]$ également, mais il faut alors rajouter les polynômes de degré 2 dont le discriminant est strictement négatif.
- Dans $\mathbb{Z}[i\sqrt{3}] := \{a + ib\sqrt{3} \mid a, b \in \mathbb{Z}\}$, on peut montrer que 2 est irréductible mais il n'est pas premier car $(1 + i\sqrt{3}).(1 - i\sqrt{3}) = 4 \in (2)$ mais $(1 + i\sqrt{3}), (1 - i\sqrt{3}) \notin (2)$.

Ces notions de primalité et d'irréductibilité ne sont pas étrangère l'une à l'autre :

Proposition 1.1.4. Tout élément premier est irréductible.

Démonstration. Soit $a \in A^* \setminus A^\times$ un élément premier. Suposons que $a = b_1.b_2$ avec $b_1, b_2 \in A$. Alors $b_1.b_2 \in (a)$ donc par primalité, et quitte à échanger b_1 et b_2, on a $b_2 \in (a)$, c'est-à-dire $b_2 = c.a$ avec $c \in A$. Mais alors $a = b_1.c.a$ et par intégrité de A, a étant non nul, $1 = b_1.c$. On en déduit que b_1 est inversible. □

Remarque 1.1.5. L'hypothèse d'intégrité de A est ici essentielle. En effet, dans $\mathbb{Z}/6\mathbb{Z}$, 2 n'est pas irréductible car $2 = 2.4$ avec 2 et 4 non inversibles, mais 2 est premier car $(2) = \{0, 2, 4\}$ et un produit d'éléments dans $\mathbb{Z}/6\mathbb{Z} \setminus (2) = \{1, 3, 5\}$ restera dans $\{1, 3, 5\}$ par un argument de parité.

Nous pouvons maintenant donner une première définition d'un anneau factoriel.

Définition 1.1.6. On dit que A est factoriel si tout élément $a \in A^* \setminus A^\times$ est un produit d'éléments premiers.

Sous cette hypothèse, les notions d'élements premiers et irréductibles coïncident.

Proposition 1.1.7. Si A est factoriel, alors un élément $a \in A^* \setminus A^\times$ est premier si et seulement si il est irréductible.

Démonstration. On a déjà vu que tout élément premier est irréductible, il suffit donc de montrer la réciproque. Soit donc $a \in A^* \setminus A^\times$ irréductible. Par factorialité de A, il existe des éléments $p_1, \dots, p_k \in A^* \setminus A^\times$ premiers tels que $a = p_1 \dots p_k$. Supposons par l'absurde que $k > 1$. Puisque p_1 est non inversible, on sait que $p_2 \dots p_k$ l'est par irréducibilité de a. Il existe donc $c \in A$ tel que $p_2 \dots p_k.c = 1$. Mais alors p_2 est inversible ce qui contredit sa primalité. On en déduit que $k = 1$ et $a = p_1$ est donc premier. □

Remarque 1.1.8. La proposition 1.1.7 n'est pas une équivalence. Il existe en effet des anneaux non factoriels pour lesquels les notions d'éléments premiers et irréductibles coïncident. On pourra citer l'anneaux des fonctions holomorphes sur $\mathbb{C}$ (fonctions $f : \mathbb{C} \to \mathbb{C}$ dérivables au sens complexe) ou l'anneaux des entiers algébriques (racines réelles d'un polynôme unitaire à coefficients dans $\mathbb{Z}$), mais le vérifier dépasserait de loin le programme de L2.

Nous allons maintenant exprimer la factorialité de A en terme d'uniques factorisations de ses éléments. Mais afin d'énoncer proprement le caractère unique, nous devons d'abord introduire une notion d'équivalence entre éléments.

Définition 1.1.9. Deux éléments $a_1, a_2 \in A$ sont *associés* s'il existe $b \in A^\times$ tel que $a_2 = b.a_1$. On parle alors d'*association* entre a_1 et a_2.

Proposition 1.1.10.

- L'association est une relation d'équivalence.
- Deux éléments $a_1, a_2 \in A$ sont associés si et seulement si $(a_1) = (a_2)$.
- Deux éléments associés sont simultanément irréductibles ou non, et simultanément premiers ou non.

Démonstration. Le premier point est clair.

Concernant le second point, supposons d'abord que a_1 et a_2 sont associés. Il existe alors $b \in A^\times$ tel que $a_1 = b.a_2$ et on a alors d'une part $a_1 = b.a_2 \in (a_2)$ et donc $(a_1) \subset (a_2)$, et d'autre part $a_2 = b^{-1}.a_1 \in (a_1)$ et donc $(a_2) \subset (a_1)$. Réciproquement, on suppose $(a_1) = (a_2)$. On a alors d'une part $a_1 \in (a_2)$ et il existe donc $b \in A$ tel que $a_1 = b.a_2$, et d'autre part $a_2 \in (a_1)$ et il existe donc $c \in A$ tel que $a_2 = c.a_1$. On en déduit que $a_1 = b.a_2 = b.c.a_1$ et, par intégrité de A, que $1 = b.c$. L'élément b est donc inversible ; les éléments a_1 et a_2 sont donc associés.

Enfin, pour le dernier point, l'affirmation est claire concernant la primalité car la définition de cette dernière ne fait intervenir que l'idéal engendré par l'élément en question. Et concernant l'irréductibilité,

supposons que a_1 et a_2 soient associés. Il existe donc $b \in A^\times$ tel que $a_2 = b.a_1$. Alors toute décomposition $a_1 = c_1.c_2$ avec c_1 et c_2 non inversibles induit une décomposition $a_2 = (b.c_1).c_2$ avec $b.c_1$ et c_2 non inversibles. En effet, si $b.c_1$ était inversible, alors $c_1 = b^{-1}.b.c_1$ le serait aussi. On en déduit que a_1 irréductible implique a_2 irréductible et, par symétrie des rôles de a_1 et a_2, que a_2 irréductible implique a_1 irréductible. □

Proposition 1.1.11. L'anneau A est *factoriel* ssi

- pour tout $a \in A^* \setminus A^\times$ il existe $p_1, p_2, \cdots, p_k$ des éléments irréductibles de A tels que $a = p_1.\cdots.p_k$;
- si $p_1.\cdots.p_k = p'_1.\cdots.p'_{k'}$ avec tous les $p_i, p'_i \in A$ irréductibles, alors $k = k'$ et il existe $\sigma \in \mathfrak{S}_k$ tels que p'_i et $p_{\sigma(i)}$ sont associés pour tout $i \in [\![1, k]\!]$.

Autrement dit, A est factoriel si tout élément non nul et non inversible admet une unique décomposition en facteurs irréductibles, à ordre et association près des facteurs.

Remarque 1.1.12. La proposition 1.1.11 est une équivalence et elle est d'ailleurs prise dans bon nombre de livres comme définition d'un anneau d'un anneau factoriel. Dans ce cours, nous avons toutefois préféré utiliser la définition 1.1.6 car, d'une part, celle-ci nécessite moins de notions préliminaires et, d'autre part, elle semble plus simple à vérifier directement puisqu'il suffit de montrer l'existence d'une décomposition mais pas son unicité.

Démonstration. Supposons que A est factoriel. Alors tout élément non nul et non inversible s'écrit comme produit d'éléments premiers et donc comme produit d'éléments irréductibles. On montre le second point par récurrence sur k, en supposant, quitte à échanger les rôles des p_i et des p'_i, que $k \leq k'$. Pour $k = 1$, le résultat est clair si $k' = 1$. Supposons donc par l'absurde que $k' > 1$, alors on a $p'_1.\cdots.p'_{k'} \in (p_1)$ et donc, par application successive de la primalité de p_1, il existe $j \in [\![1, k']\!]$ tel que $p'_j \in (p_1)$. Par commutativité de A et quitte à réindexer les p'_i, on peut supposer que $j = 1$. Il existe donc $b \in A$ tel que $p'_1 = p_1.b$, et donc $p_1 = p_1.b.p'_2.\cdots.p'_{k'}$. Par intégrité de A, on obtient $1 = b.p'_2.\cdots.p'_{k'}$ et donc $p'_{k'}$ inversible ce qui contredit sa primalité/son irréducibilité.

Supposons maintenant le résultat vrai pour $k-1$. De l'égalité $p_1.p_2.\cdots.p_k = p'_1.p'_2.\cdots.p'_{k'}$, on en déduit que $p'_1.p'_2.\cdots.p'_{k'} \in (p_1)$ et donc, par application successive de la primalité de p_1, qu'il existe $j \in [\![1, k']\!]$ tel que $p'_j \in (p_1)$. Par commutativité de A et quitte à réindexer les p'_i, on peut supposer que $j = 1$. Il existe donc $b \in A$ tel que $p'_1 = p_1.b$. Par irréducibilité de p'_1 l'un des facteurs b ou p_1 est inversible, et par primalité/irréducibilité de p_1, ça ne peut être que b. On en déduit que p_1 et p'_1 sont associés. De plus, par intégrité de A, on a $p_2.\cdots.p_k = (b.p'_2).p'_3.\cdots.p'_{k'}$ avec $(b.p'_2), p'_3, \ldots, p'_{k'}$ irréductibles et on conclut par hypothèse de récurrence.

Réciproquement, supposons maintenant les deux points vérifiés et montrons que A est factoriel. Pour tout $a \in A^* \setminus A^\times$, le premier point donne une factorisation de a en produits d'éléments irréductibles. Il suffit de montrer que chacun de ces facteur est en fait premier. Supposons donc par l'absurde qu'il existe $p \in A^* \setminus A^\times$ irréductible mais non premier. Il existe alors $b_1, b_2 \in A$ tels que $b_1.b_2 \in (p)$ mais $b_1, b_2 \notin (p)$. On a alors $b_1, b_2 \neq 0$, car $0 \in (p)$, et $b_1, b_2 \notin A^\times$ car si, par exemple $b_2 \in A^\times$, alors $b_1 = b_1.b_2.b_2^{-1} \in (p)$. Par hypothèse, il existe donc des éléments irréductibles $p_1, \ldots, p_k$ et $q_1, \ldots, q_l$ de A tels que $b_1 = p_1.\cdots.p_k$ et $b_2 = q_1.\cdots.q_l$. Mais alors $p = p_1.\cdots.p_k.q_1.\cdots.q_l$, ce qui viole le second point car $k + l > 1$. □

Exemples 1.1.13.

- L'ensemble des entiers $\mathbb{Z}$ est factoriel.
- L'ensemble des entiers de Gauss $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ est factoriel.
- L'ensemble $\mathbb{Z}[i\sqrt{3}] := \{a + ib\sqrt{3} \mid a, b \in \mathbb{Z}\}$ n'est pas factoriel car $4 = 2.2 = (1 + i\sqrt{3}).(1 - i\sqrt{3})$ or on peut montrer que 2, $1 + i\sqrt{3}$ et $1 - i\sqrt{3}$ sont irréductibles et non associés.
- Les ensembles de polynômes $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont factoriels.

Afin de simplifier l'unicité de la décomposition en facteurs irréductibles, on fixe parfois un système de représentants d'éléments irréductibles dans chaque classe d'association. Par exemple, dans $\mathbb{Z}$, il existe dans chaque classe d'association un unique représentant positif : cela conduit à l'ensemble $\mathcal{P}$ des nombres premiers usuels et le théorème d'unique décomposition en facteurs premiers devient donc

$$n = \varepsilon.p_1.\cdots.p_k$$

avec $\varepsilon \in \mathbb{Z}^\times = \{\pm 1\}$ et $p_i \in \mathcal{P}$, les p_i étant uniques à ordre près.

Dans $\mathbb{C}[X]$, il existe dans chaque classe d'association un unique représentant unitaire, c'est-à-dire dont le coefficient dominant vaut 1 : cela conduit au théorème d'unique décomposition en facteurs premiers suivant

$$P = \alpha.P_1.\cdots.P_k$$

avec $\alpha \in \mathbb{C}^*$ et $P_i := X - \beta_i$ avec $\beta_i \in \mathbb{C}$, les P_i étant uniques à ordre près. De même, dans $\mathbb{R}[X]$, on peut écrire de manière unique tout polynôme non nul sous la forme

$$P = \alpha.P_1.\cdots.P_k$$

avec $\alpha \in \mathbb{R}^*$ et $P_i = X - \beta_i$ pour un certain $\beta_i \in \mathbb{R}$ ou $P_i = X^2 + \beta_i X + \gamma_i$ pour certains $\beta_i, \gamma_i \in \mathbb{R}$ tels que $\beta_i^2 - 4\gamma_i < 0$, les P_i étant uniques à ordre près.

1.2 Anneaux principaux

Tout idéal de $\mathbb{Z}$ est également un sous-groupe de $(\mathbb{Z}, +)$, or nous avons vu que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. On en déduit que tout idéal de $\mathbb{Z}$ est de la forme (n) avec $n \in \mathbb{Z}$. Cela permet de faire une identification entre les idéaux de $\mathbb{Z}$ et les classes d'association dans $\mathbb{Z}$. Or toutes les notions liées à la divisibilité ne dépendent en réalité que de la classe d'association. En effet, pour tout $a, b \in \mathbb{Z}^*$, on a $a|b \Leftrightarrow b \in (a)$, et pour tout $a_1, a_2 \in \mathbb{Z}^*$, $(a_1) \cap (a_2) = \big(\mathrm{ppcm}(a_1, a_2)\big)$ et $(a_1) + (a_2) = \big(\mathrm{pgcd}(a_1, a_2)\big)$, le second point étant une reformulation du théorème de Bézout. Toutes les propriétés arithmétiques peuvent de fait se réinterpréter en terme d'idéaux. Cela motive les définitions suivantes.

Définition 1.2.1. Soit $a_1, a_2 \in A$. On dit que :

- a_1 *divise* a_2, ou encore que a_2 est un *multiple* de a_1 si $a_2 \in (a_1)$;
- $m \in A$ est un *plus petit multiple commun* de a_1 et a_2 si m est un multiple de a_1 et de a_2 et que tout multiple commun à a_1 et a_2 est aussi un multiple de m ;
- $d \in A$ est un *plus grand diviseur commun* de a_1 et a_2 si d est un diviseur de a_1 et de a_2 et que tout diviseur commun à a_1 et a_2 est un diviseur de d.

Remarques 1.2.2.

- L'ensemble des multiples communs à deux éléments n'est jamais vide car il contient toujours au moins leur produit, et l'ensemble des diviseurs communs non plus car il contient toujours au moins l'élément unité.
- Comme son nom l'indique, la notion de plus petit multiple commun (resp. plus grand diviseur commun) correspond à un minimum global (resp. maximum global), au sens de la divisibilité, sur l'ensemble des multiples communs (resp. diviseurs communs). Il est toutefois délicat de l'exprimer ainsi car, en général, la relation de divisibilité n'est pas une relation d'ordre. Comme dans le cas des entiers relatifs, elle vérifie en effet la réflexivité et la transitivité, mais pas forcément l'antisymétrie, deux éléments associés étant mutuellement divisibles l'un par l'autre. C'est d'ailleurs pour cela que l'on parle d'*un* plus petit multiple commun (resp. plus grand diviseur commun) et non *du* car ces derniers ne sont définis qu'à association près. Notons toutefois au passage que, si un choix de représentant a été fait dans chaque classe d'association, on peut alors parler, pour tous $a_1, a_2 \in A$, *du* plus grand diviseur commun $\mathrm{pgcd}(a_1, a_2)$ et *du* plus petit multiple commun $\mathrm{ppcm}(a_1, a_2)$. C'est

le cas dans $\mathbb{Z}$, où l'on choisit l'unique représentant positif, ainsi que dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$ où l'on choisit l'unique représentant unitaire.

- Les notions de plus petit multiple et de plus grand diviseurs communs peuvent se réinterpréter en terme d'inclusions d'idéaux. En effet :
  - ⋆ dire que m est un multiple de a_1 et de a_2, c'est dire que m appartient à (a_1) et à (a_2), donc à $(a_1) \cap (a_2)$, ou encore dire que $(m) \subset (a_1) \cap (a_2)$;
    ⋆ dire que tout multiple commun à a_1 et a_2 est aussi un multiple de m, c'est dire que $(a_1) \cap (a_2) \subset (m)$;

  donc dire que m est un plus petit multiple commun de a_1 et a_2, c'est dire que $(m) = (a_1) \cap (a_2)$;
  - ⋆ dire que d est un diviseur commun de a_1 et de a_2, c'est dire que $a_1, a_2 \in (d)$ et donc que $(a_1), (a_2) \subset (d)$, ce qui revient à dire que $(a_1) + (a_2) \subset (d)$;
    ⋆ dire que tout diviseur commun à a_1 et a_2 est aussi un diviseur de d, c'est dire que tout idéal de la forme (a) contenant (a_1) et (a_2), ce qui est équivalent à contenir $(a_1) + (a_2)$, contient également (d) ;

  donc dire que d est un plus grand diviseur commun de a_1 et a_2, c'est dire que (d) est un minimum global, au sens de l'inclusion, parmi les idéaux engendré par un élément et contenant $(a_1) + (a_2)$.

Définition 1.2.3. On dit qu'un idéal $I \subset A$ est *principal* s'il existe $a \in A$ tel que $I = (a)$. On dit que A est *principal* si tout idéal de A est principal.

Exemples 1.2.4.

- L'anneau des entiers $\mathbb{Z}$ est principal.
- Tout corps $\mathbb{K}$ est principal car ses seuls idéaux sont $\{0\} = (0)$ et $\mathbb{K} = (1)$.
- Nous allons voir que les anneaux $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont principaux.
- L'anneau $\mathbb{Z}[X]$, par contre, n'est pas principal car $I = (2, X)$ n'est pas principal. En effet, I correspond aux polynômes dont le terme constant est pair. S'il était engendré par un élément $P \in \mathbb{Z}[X]$, cet élément devrait être de degré 0 car sinon I ne pourrait pas contenir 2 ; mais s'il était engendré par un élément $n \in \mathbb{Z}$, alors n devrait être pair et tous les coefficients de tous les éléments de I seraient pairs.

Sous l'hypothèse que A est principal, deux éléments $a_1, a_2 \in A$ possèdent toujours des plus petit multiple et plus grand diviseur communs puisque $(a_1) \cap (a_2)$ et $(a_1) + (a_2)$ sont alors principaux et s'écrivent donc respectivement sous la forme $(a_1) \cap (a_2) = (m)$ et $(a_1) + (a_2) = (d)$ avec $m, d \in A$. Dès lors, le résultat suivant devient totalement tautologique.

Proposition 1.2.5 (Bachet–Bézout)**.** Si A est principal, alors pour tout $a_1, a_2 \in A$, il existe $b_1, b_2 \in A$ tels que $a_1.b_1 + a_2.b_2$ soit un plus grand diviseur commun de a_1 et a_2.

Remarques 1.2.6.

- On peut dès lors développer toute une arithmétique similaire à celle des entiers relatifs. On peut par exemple définir la notion d'éléments $a_1, a_2 \in A$ *premiers entre eux* par le fait d'avoir 1 comme plus grand diviseur commun. Cela se traduit également par $(a_1) + (a_2) = (1) = A$.
- Pour un anneau non principal, on peut également développer une arithmétique, mais celle-ci ne se fera alors pas sur l'ensemble de ses éléments, mais sur l'ensemble de ses idéaux.

Les anneaux principaux sont en fait un cas particulier des anneaux factoriels.

Proposition 1.2.7. Tout anneau principal est factoriel.

Démonstration. La démonstration étant relativement technique, nous admettrons ce résultat. Le lecteur intéressé pourra toutefois trouver une preuve dans les notes de cours. □

Corollaire 1.2.8. Dans tout anneau principal, un élément non nul et non inversible admet une décomposition en facteurs irréductibles, et cette décomposition est unique à ordre et association des facteurs près.

Exemple 1.2.9. Nous avons vu que l'anneau $\mathbb{Z}[X]$ n'est pas principal car il contient l'idéal $(2, X)$ qui n'est pas principal.On peut toutefois montrer qu'il est factoriel. Il n'y a donc pas équivalence entre anneaux factoriels et anneaux principaux.

Avec les définitions données dans la section précédente et en reprenant verbatim, lorsque nécessaire, les preuves du cas $A = \mathbb{Z}$, on obtient les lemmes usuels d'arithmétique :

Lemme 1.2.10. Si A est principal, alors :

- (lemme d'Euclide) si $a \in A^* \setminus A^\times$ irréductible divise un produit $b.c$, alors a divise b ou a divise c ;
- (lemme de Gauss) si $a, b, c \in A^*$ sont tels que a divise $b.c$ et que a et b sont premiers entre eux, alors a divise c ;
- si $a, b \in A^*$ sont premiers entre eux et divisent $c \in A$, alors $a.b$ divise c.

1.2.1 Anneaux euclidiens

Dans notre étude des entiers relatifs, la division euclidienne est clairement apparue comme un outil crucial. Donnons-en maintenant une définition générale.

Définition 1.2.11. On dit que A est *euclidien* s'il existe une application $\nu : A \to \mathbb{N}$, appelée *stathme*, telle que :

- pour tout $a \in A$, $\nu(a) = 0$ si et seulement si $a = 0_A$;
- pour tous $a, b \in A^*$, $\nu(a.b) \geq \nu(a)$;
- pour tout $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tels que $a = b.q + r$ et $\nu(r) < \nu(b)$.

Remarques 1.2.12.

- On n'impose, *a priori*, aucune condition d'unicité sur q et r.
- La seconde condition affirme qu'un stathme est "croissant pour le pré-ordre de la divisibilité", dans le sens où, pour tous $a, b \in A^*$, si a divise b, alors $\nu(a) \leq \nu(b)$.

Exemples 1.2.13.

- L'application $\nu : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & |n| \end{array}$ est un stathme pour l'anneau $\mathbb{Z}$.
- Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'application $\nu : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{N} \\ P & \longmapsto & 1 + \deg(P) \end{array}$, avec la convention que $\deg(0) = -1$, est un stathme pour l'anneau $\mathbb{K}[X]$.
- L'application $\nu : \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ a + ib & \longmapsto & a^2 + b^2 \end{array}$ est un stathme pour l'anneau des *entiers de Gauss*, défini comme le sous-anneau $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ de $\mathbb{C}$.

Les anneaux euclidiens sont en fait un cas particulier des anneaux principaux, et donc des anneaux factoriels.

Proposition 1.2.14. Tout anneau euclidien est principal.

Démonstration. Soit A un anneau euclidien et $I \subset A$ un idéal. Si $I = \{0\}$, alors $I = (0)$. Autrement, l'ensemble $\nu(I^*)$ est un sous-ensemble non vide de $\mathbb{N}$, il possède donc un plus petit élément et on peut considèrer $b \in I^*$ tel que $\nu(b) = \min\{\nu(a) \mid a \in I^*\}$. On a alors $(b) \subset I$. Et réciproquement, pour tout $a \in I$, il existe $q, r \in A$ tels que $a = q.b + r$ avec $\nu(r) < \nu(b)$. Mais $r = a - q.b \in I$ et donc, par minimalité de b, on ne peut avoir que $r = 0_A$. On en déduit que $a = q.b \in (b)$ et donc que $I = (b)$. □

Remarque 1.2.15. Il existe des anneaux principaux non euclidiens. On peut par exemple montrer que l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] := \left\{a + \frac{1+i\sqrt{19}}{2}b \mid a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$ est principal mais pas euclidien.

De fait, sur tout anneau euclidien, on peut développer une arithmétique, et tout élément non nul et non inversible admet une décomposition en facteurs irréductibles, et cette décomposition est unique à ordre et association des facteurs près.