L'Anneau des Entiers de Gauss

1) Introduction

Anneau Euclidien, Anneau Principal, Anneau factoriel

L'anneau intègre A est dit euclidien s'il existe une division euclidienne, c'est-à-dire une valuation v à valeurs positives définie sur $A \setminus \{0\}$, telle que : $a/b \Longrightarrow v(a) \leq v(b)$, et un procédé permettant d'associer à deux éléments a, b $(b \neq 0)$ un quotient q et un reste r de a divisé par b :

$$a = bq + r, \qquad avec \ v(r) < v(b) \ (ou \ r = 0)$$

L'anneau intègre A est dit principal si tout idéal de A est principal, c'est-à-dire engendré par un seul élément. Un anneau euclidien est *ipso facto* principal : il suffit de prendre comme générateur un élément non-nul de valuation minimale dans l'idéal. La conséquence immédiate en est la théorie du pgcd et du ppcm grâce aux idéaux, et le théorème de Bezout :

$$aA + bA = \{au + bv, \ u \in A, v \in A\} = \delta A \ , \ \delta = pgcd(a,b) \ défini \ à \ association \ près$$

$$aA \cap bA = ensemble \ des \ mutiples \ communs \ à \ a, b = \mu A \ , \qquad \mu = ppcm(a,b) \ \ défini \ à \ association \ près$$

On peut montrer que tout anneau principal est factoriel, c'est-à-dire possède la propriété suivante :

tout élément peut se décomposer en un produit d'irréductibles et cette décomposition est unique à association près (a et b sont dits associés s'ils se divisent l'un l'autre, ce qui revient à dire que chacun est produit de l'autre par un élément inversible, que l'on appelle aussi élément unitaire, de l'anneau).

Elément Algébrique sur un Corps, Extension Simple

Un élément α extérieur à un corps K (pris dans un anneau ou un corps incluant K) est dit algébrique sur K s'il est racine d'une équation algébrique à coefficients dans K (i.e. d'un polynome non-nul de $K[X]$).

L'anneau des polynômes $K[X]$ étant principal (car euclidien), l'idéal annulateur de α, constitué des polynômes admettant α comme racine, est engendré par l'unique polynôme annulateur unitaire (ie de coefficient dominant égal à 1 , *attention, le sens du mot unitaire n'est plus le même ici*) et de degré minimal, que l'on notera $M(X)$.

(1) L'extension simple $K[\alpha]$ désigne le plus petit anneau contenant K et α , on voit facilement que c'est l'ensemble des éléments de la forme $x = P(\alpha)$, lorsque le polynôme P décrit $K[X]$.

Si l'on effectue la division euclidienne de P par M : $P = MQ + R, \deg(R) < \deg(M) = n$, on constate que x peut s'écrire $R(\alpha)$, et que cette écriture est unique ; $K[\alpha]$ apparaît donc comme espace vectoriel sur K, avec pour base $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$.

(2) De plus, il est clair que $M(X)$ est irréductible dans $K[X]$, sinon cela contredirait son caractère de polynôme minimal de α sur K ; il est donc premier avec tout polynôme non-nul $R(X)$ de degré inférieur ou égal à $n-1$, et vérifie donc la relation de Bezout :

$$MU + RV = 1 \quad avec \quad U, V \ \in K[X]$$

(3) Si on considère un élément $x = R(\alpha)$ non-nul dans $K[\alpha]$, cet élément est donc inversible, d'inverse égal à $V(\alpha)$. $K[\alpha]$ est donc un corps , et peut être noté $K(\alpha)$.

Remarque : Qu'est-ce qui subsiste de ces raisonnements, si l'on considère une extension du type $A[\alpha]$, où A est un anneau intègre, et α un élément algébrique sur A, dont on suppose ici qu'il admet un annulateur unitaire.

Réponse : Le point (1) va pouvoir être étendu, du fait qu'il existe bien un minimal unitaire (le justifier), et que dans ces conditions l'on peut toujours effectuer la division euclidienne de P par M (à ceci près qu'on ne parle plus d'espace vectoriel de dimension n sur le corps K , mais de module de dimension n sur l'anneau A) . Le plus important est de constater que l'ensemble des combinaisons à coefficients dans A de $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ est stable par multiplication, du fait de la relation d'annulation $M(\alpha) = 0$; et que d'autre part l'écriture, sous forme d'une telle combinaison, d'un élément de l'extension $A[\alpha]$ est unique.

Par contre, l'anneau des polynômes $A[X]$ n'est plus euclidien, et le second membre de la relation de Bezout devient une constante non nécessairement égale à 1, ce qui ne permet pas de généraliser le point (2) : $A[\alpha]$ n'est pas en général un corps, comme on va le voir plus en détail à propos de l'anneau des entiers de Gauss $\mathbb{Z}[i]$. Par exemple, dans $\mathbb{Z}[X]$, la « meilleure » relation de Bezout entre l'annulateur de $\alpha = i$, c'est-à-dire $M(X) = X^2 + 1$, et un polynôme du premier degré, mettons $R(X) = X + 1$, s'écrit : $M(X) - R(X)(X - 1) = 2$, ce qui ne permet pas d'inverser $R(\alpha)$.

D'ailleurs, en y regardant de plus près, l'anneau des polynômes à coefficients entiers $\mathbb{Z}[X]$ n'est même pas principal : étudions par exemple le cas des deux polynômes $P = 2(X + 1)$ et $Q = 3(X - 1)$.

A titre de comparaison, si on se plaçait sur $\mathbb{Q}[X]$, ces deux polynômes, premiers entre eux, vérifieraient la relation de Bezout :

$\frac{1}{4}P(X - 1) - \frac{1}{6}Q(X + 1) = 1$, et l'idéal $P\mathbb{Q}[X] + \mathrm{Q}\mathbb{Q}[X]$ étant égal à $\mathbb{Q}[X]$ tout entier, on pourrait affirmer qu'il est principal et admet pour générateur 1 ou n'importe quelle constante non-nulle.

Sur $\mathbb{Z}[X]$ maintenant, ces deux polynômes sont encore premiers entre eux (ils n'ont manifestement aucun diviseur commun du premier degré, et les irréductibles dans $\mathbb{Z}[X]$ sont, d'une part les nombres premiers, et d'autre part les polynômes de degré ≥ 1 qui sont déjà irréductibles sur $\mathbb{Q}[X]$ et dont le contenu (pgcd des coefficients) est égal à 1).

Or, la « meilleure » relation de Bezout que l'on puisse écrire dans ce contexte est la suivante : $3P - 2Q = 12$. En effet, pour être la meilleure, cette relation doit déjà minimiser le degré du second membre, donc donner une constante, ce qui impose de prendre une combinaison $PU + QV$ de la forme $(3k)P - (2k)Q$, ce qui donne un second membre égal à $12k$; on voit que 12 est bien la meilleure constante de Bezout.

D'autre part, si on s'intéresse à un diviseur éventuel de l'idéal engendré par P et Q , la relation ci-dessus et l'hypothèse $P\mathbb{Z}[X] + \mathrm{Q}\mathbb{Z}[X] = D\mathbb{Z}[X]$ montrent que 12 doit nécessairement être un multiple du polynôme D, au total on devrait avoir :

$D(X) = constante\ C \in \{\pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$; or il est manifeste que P et Q ne sont pas tous deux multiples d'une de ces constantes, d'où contradiction ;

on en conclut que l'idéal $P\mathbb{Z}[X] + \mathrm{Q}\mathbb{Z}[X]$ n'est pas principal : le pgcd des polynômes P et Q est la constante 1, mais ce pgcd ne se définit pas comme diviseur de l' idéal engendré par P et Q et ne vérifie pas de relation de Bezout.

L'Anneau des Entiers de Gauss

L'écriture $n = a^2 + b^2 = (a + bi)(a - bi),\ a \in \mathbb{N},\ b \in \mathbb{N}$ est à l'origine de l'étude de l'anneau $\mathbb{Z}[i] = \{\mathrm{a} + \mathrm{bi}, a \in \mathbb{N},\ b \in \mathbb{N}\ \}$ pour résoudre la question de la décomposabilité de l'entier n en somme de deux carrés ; cette méthode est historiquement attribuée à Gauss.

La remarque préliminaire essentielle est celle-ci : grâce à l'écriture ci-dessus dans $\mathbb{Z}[i]$, l'ensemble $\Sigma = \{n \in \mathbb{N}\ tq\ n = a^2 + b^2,\ a \in \mathbb{N}, b \in \mathbb{N}\ \}$ des entiers qui peuvent s'écrire comme somme de deux carrés est manifestement stable par multiplication.

En effet, si $n = a^2 + b^2 = z\bar{z}$ et $m = c^2 + d^2 = z'\overline{z'}$, alors on a **l'identité de Lagrange** :

$$mn = (a + bi)(a - bi)(c + di)(c - di) = (z\bar{z})(z'\bar{z'}) = (zz')\overline{(zz')} = (ac - bd)^2 + (ad + bc)^2$$

Etude de l'Anneau $\mathbb{Z}[i]$

Premier point : $\mathbb{Z}[i]$ est muni d'une valuation naturelle, à savoir $N(a + bi) = a^2 + b^2 = z\bar{z} = |z|^2$ (carré du module) ; grâce à cela on voit que les inversibles sont nécessairement de module égal à 1 :

En effet : $uv = 1 \Longrightarrow N(uv) = N(u)N(v) = 1 \Longrightarrow N(u) = N(v) = 1 \Longrightarrow u, v \in \{1, -1, i, -i\}$
$(puisque\ N(u), N(v) sont\ des\ entiers\ positifs)$

Deuxième Point : Si l'on veut obtenir la division euclidienne de $z = a + bi$ par $s = c + di$, l'idée est de d'écrire la condition visée : $z = sq + r\ \ avec\ N(r) < N(s)$, quitte à se placer dans le corps des complexes, sous la forme :

$$zs^{-1} = q + rs^{-1}\ \ avec\ N(rs^{-1}) < 1$$

Or cela revient à trouver sur le maillage des entiers de Gauss un point q qui soit à distance plus petite que l'unité du point d'affixe zs^{-1}, comme le point de coordonnées entières le plus proche est toujours à distance inférieure ou égale à $\frac{\sqrt{2}}{2}$, l'existence de la division euclidienne de z par s est assurée.

(et même l'unicité si on se fixe un critère de choix (point entier le plus proche, le cas d'ambiguité d'une distance égale à $\frac{\sqrt{2}}{2}$, où zs^{-1} serait situé au centre d'un carré du maillage, ne pouvant pas se produire du fait de l'irrationnalité de $\frac{\sqrt{2}}{2}$)

En conséquence du fait que $\mathbb{Z}[i]$ est euclidien, on peut montrer facilement qu'il est aussi factoriel : pour l'existence de la décomposition en produit d'irréductibles, il suffit d'écrire un algorithme de décomposition, d'où construction d'un arbre dont les feuilles sont des irréductibles, en un nombre d'étapes fini du fait de la décroissance stricte de la valuation le long des branches de l'arbre. Quant à l'unicité des facteurs de cette décomposition à association près, elle tient au Lemme de Gauss, lui-même conséquence du théorème de Bezout et du fait qu'un anneau euclidien est *ipso facto* principal.

2) Le théorème des deux carrés

On se propose ici de définir entièrement, grâce à l'anneau des entiers de Gauss, l'ensemble $\Sigma = \{n \in \mathbb{N}\ tq\ n = a^2 + b^2,\ a \in \mathbb{N}, b \in \mathbb{N}\}$ des entiers qui peuvent s'écrire comme somme de deux carrés.

Cas d'un nombre premier

Commençons par le cas où l'entier n est un nombre premier p. Les carrés modulo 4 sont 0,1 ; les sommes de deux carrés modulo 4 valent 0,1 ou 2. Par conséquent, un nombre premier p, qui ne peut être congru qu'à 1 ou 3 modulo 4, est nécessairement indécomposable en somme de deux carrés dans le second cas :

$$p \equiv 3\ (modulo\ 4) \Rightarrow p \notin \Sigma$$

$$p \in \Sigma \Rightarrow p \equiv 1\ (modulo\ 4)$$

On va démontrer que ces implications sont des équivalences, autrement dit, dans le cas d'un nombre premier , la congruence de p modulo 4 caractérise entièrement sa décomposabilité en somme de deux carrés .

Pour cela, on montre d'abord le critère suivant :

$$p \in \Sigma \Leftrightarrow p\ est\ réductible\ dans\ \mathbb{Z}[i] \Leftrightarrow -1\ est\ un\ carré\ dans\ F_p = \mathbb{Z}/p\mathbb{Z}$$

Démonstration du Critère :

Première équivalence :
Si $p \in \Sigma$, alors on a $p = a^2 + b^2 = (a + ib)(a - ib)\ (a, b \in \mathbb{N})$ d'où p réductible dans $\mathbb{Z}[i]$ (si l'un des facteurs $a + ib, a - ib$ était un unitaire, alors l'un des entiers a, b serait nul, ce qui est impossible, car p étant premier n'est pas un carré). Réciproquement, si p est réductible dans $\mathbb{Z}[i]$: $p = zz'$, alors $z' = \bar{z}$ (car la partie imaginaire de p est nulle), d'où l'écriture ci-dessus, qui décompose p en somme de deux carrés.

Deuxième équivalence :
Si $p = a^2 + b^2$, alors on peut écrire $a^2 + b^2 \equiv 0\ (modulo\ p)$, mais $\dot{a}$ est nécessairement non-nul dans F_p, d'où l'égalité $1 + (\dot{a}^{-1}\dot{b}) = 0$ dans F_p, ce qui montre que -1 est un carré dans F_p. Réciproquement, si on suppose que -1 est un carré dans F_p, alors $X^2 + 1$ est réductible dans F_p, ie $X^2 + 1 = (X - a)(X + a)$, donc dans $\mathbb{Z}[i]$ on a $(i - a)(i + a) \equiv 0\ (modulo\ p), (i - a)(i + a) = kp$; si p était irréductible dans $\mathbb{Z}[i]$, comme il ne peut être associé à $i - a$ ou à $i + a$ (car a est nécessairement non-nul), ceci contredirait l'unicité de décomposition dans l'anneau factoriel $\mathbb{Z}[i]$.

On étudie ensuite les carrés dans F_p. L'équation de Fermat s'écrit : $x^{p-1} = 1\ \ \forall x \in F_p \backslash \{0\}$. Si x est un carré non-nul : $x = y^2,\ y \neq 0,$ il vérifie même : $x^{\frac{p-1}{2}} = y^{p-1} = 1$. Or, l'équation $x^{\frac{p-1}{2}} = 1$ admet au plus $\frac{p-1}{2}$ solutions, et chaque nombre admet soit zéro, soit deux racines carrées. Il y a donc exactement $\frac{p-1}{2}$ nombres non-nuls qui sont des carrés, et ce sont précisément ceux qui vérifient $x^{\frac{p-1}{2}} = 1.$ Pour savoir si -1 est un carré dans F_p , on utilise ce dernier critère : $-1\ est\ un\ carré\ modulo\ p \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1,$ et on trouve alors :

$$-1\ est\ un\ carré\ modulo\ p \Leftrightarrow p \equiv 1\ (modulo\ 4)$$

ce qui conclut notre étude des entiers premiers décomposables en somme de deux carrés.

Cas d'un entier quelconque

Décomposons l'entier n en produit de facteurs premiers (dans l'anneau factoriel $\mathbb{Z}$), en prenant soin de distinguer ceux qui sont dans Σ et ceux qui n'y sont pas :

$$n = \prod_{\substack{q\in\Sigma \\ (q\equiv 1\,[4])}} q^{\beta_q} \prod_{\substack{p\notin\Sigma \\ (p\equiv 3\,[4])}} p^{\alpha_p}$$

La partie $\prod_{q\in\Sigma} q^{\beta_q}$ de cette décomposition est dans Σ, grâce à la stabilité de Σ pour la multiplication que nous avons notée en introduction (identité de Lagrange).

Soit p un facteur premier de n du second produit, (p indécomposable en somme de deux carrés, c'est-à-dire irréductible dans $\mathbb{Z}[i]$), alors en utilisant la factorialité de l'anneau $\mathbb{Z}[i]$, on constate le fait suivant :

si on suppose $n \in \Sigma$, c'est-à-dire $n = a^2 + b^2 = (a + bi)(a - bi)$, $a \in \mathbb{N}$, $b \in \mathbb{N}$, alors p divise nécessairement l'un des deux facteurs $a + bi$, $a - bi$; mais alors comme p n'a pas de partie imaginaire cela impose que p divise chacun des deux entiers a et b, et finalement que p divise à la fois $a + bi$ et $a - bi$, donc que p^2 divise n ; de plus on aura :

$a + bi = p(a' + b'i)$ *et* $a - bi = p(a' - b'i)$, d'où $n/p^2 = (a' + b'i)(a' - b'i) = a'^2 + b'^2$

ce qui prouve que l'entier n/p^2 est lui-même élément de Σ.

Supposons que certains exposants α_p soient impairs ; alors en divisant n un certain nombre de fois par p^2, pour des facteurs p figurant dans le second produit, on obtiendrait la décomposition :

$$n' = \prod_{\substack{q\in\Sigma \\ (q\equiv 1\,[4])}} q^{\beta_q} \prod_{\substack{p\notin\Sigma \\ (p\equiv 3\,[4]) \\ et\ \alpha_p\ impair}} p \quad avec\ n' \in \Sigma$$

Mais ceci est impossible en vertu du résultat que nous venons de démontrer (les facteurs p figurant dans le second produit pour ne peuvent en effet avoir la propriété de diviser n' sans que p^2 ne le divise). On en conclut qu'il n'existe pas d'exposant α_p impair, autrement dit, un entier n élément de Σ est nécessairement de la forme :

$$n = \prod_{\substack{q\in\Sigma \\ (q\equiv 1\,[4])}} q^{\beta_q} \prod_{\substack{p\notin\Sigma \\ (p\equiv 3\,[4])}} p^{2\gamma_p}$$

Réciproquement, un tel entier n est élément de , grâce à la stabilité de Σ par multiplication ; plus précisément, le second produit P est un carré : $P = k^2$, donc élément de Σ : $P = k^2 + 0^2$, et le premier produit Q est somme de deux carrés $Q = A^2 + B^2$, d'où $n = PQ = (kA)^2 + (kB)^2 \in \Sigma$.

On a ainsi caractérisé exactement les entiers qui peuvent s'écrire comme somme de deux carrés.

3) Les irréductibles de $\mathbb{Z}[i]$

Les considérations qui précèdent permettent aussi de caractériser les irréductibles de $\mathbb{Z}[i]$: ce sont, d'une part, (1) les entiers p premiers qui sont congrus à 3 modulo 4, ou les nombres qui leur sont associés (à savoir $p, -p, ip, -ip$) , et d'autre part, (2) les entiers de Gauss $z = a + ib$, $ni\ réels\ ni\ imaginaires\ purs$, tels que $a^2 + b^2$ soit premier.

En effet, le cas (1) résulte de l'étude qui précède, et pour le cas (2) :

- si z est décomposable dans $\mathbb{Z}[i]$ de manière non triviale (en produit de deux facteurs non inversibles : $z = st$), alors il en va de même de $N(z) = z\bar{z} = (s\bar{s})(t\bar{t})$ qui n'est donc pas premier dans $\mathbb{Z}$;

- réciproquement, si $N(z)$ est décomposable dans $\mathbb{Z}$, alors soit p un facteur premier de $N(z)$, de deux choses l'une :

  (a) ou bien p est irréductible dans $\mathbb{Z}[i]$ ($p \equiv 3\ [4]$), auquel cas il divise z ou $\bar{z}$ (en fait z et $\bar{z}$) comme on l'a déjà vu, et cette décomposition est non triviale (car $z \notin \mathbb{Z}$ et $z \notin i\mathbb{Z}$)

  (b) ou bien p s'écrit comme produit d'irréductibles dans $\mathbb{Z}[i]$, dans ce cas soit s l'un de ces irréductibles : $p = st\ \ avec\ t \notin \{1, -1, i, -i\}$, en fait t est nécessairement égal à $\bar{s}$, et $p = s\bar{s}$ divise $N(z) = z\bar{z}$, ce qui impose que s ou bien $\bar{s}$ divise z (strictement, ie sans association, puisque déjà p divise strictement $N(z)$ dans $\mathbb{Z}$) ; ainsi z est décomposable de manière non triviale dans $\mathbb{Z}[i]$, cqfd.