Autour du *ppcm* et du *pgcd*

Daniel PERRIN

Avertissement *Le texte ci-dessous est le premier provenant de la récupération de mes vieux papiers du temps de Sèvres (l'école normale supérieure de jeunes filles). L'objectif de ces textes est de compléter le cours d'algèbre [DP].*

1 Introduction et notations

1.1 Notations

On considère un anneau A commutatif unitaire et on désigne par A^* l'ensemble des éléments inversibles de A. On note $a|b$ la relation de divisibilité : $a|b \iff \exists c \in A,\ b = ac$. La relation $\mathcal{R}$ de double divisibilité : $(a\mathcal{R}b \iff a|b \,\text{et}\, b|a)$ est une relation d'équivalence et l'ensemble quotient $A/\mathcal{R}$ est ordonné par la relation induite par la divisibilité. On a le résultat suivant :

1.1 Proposition. *Si l'anneau A est intègre, la relation de double divisibilité est équivalente à la relation d'association : $a\mathcal{R}b \iff \exists u \in A^*,\ b = au$.*

Démonstration. Le sens $\Longleftarrow$ est trivial. Pour l'autre on peut supposer a et b non nuls. On a $a|b$, donc $b = au$, et $b|a$, donc $a = vb$. On en déduit $a = vb = vua$ soit $a(1 - vu) = 0$ et, puisque a est non nul et A intègre, $uv = 1$ et le résultat.

Nous supposerons désormais que A est intègre.

On note $\mathcal{J}^*(A)$ l'ensemble des idéaux principaux de A, ordonné par inclusion. On sait, cf. [DP], que $\mathcal{J}^*(A)$ est anti-isomorphe, comme ensemble ordonné, à $A/\mathcal{R}$ par l'application qui à $a \in A$ associe l'idéal principal (a).

1.2 Définitions

1.2 Définition. *Soient a, b, d, m des éléments de $\in A - \{0\}$. On dit que d (resp. m) est un pgcd (resp. un ppcm) de a et b si d est la borne inférieure (resp. supérieure) de a et b dans $A/\mathcal{R}$.*

Pour d, cela revient à dire que d divise a et b et que si c divise a et b il divise d. Pour m cela signifie que a et b divisent m et que si a et b divisent c alors m divise c.

On dit que a et b sont **premiers entre eux** *si l'on a $pgcd(a,b) = 1$.*

1.3 *Remarques.* 1) Il revient au même de demander que les idéaux (d) et (m) soient des bornes supérieures et inférieures de (a) et (b) dans $\mathcal{J}^*(A)$, respectivement.

2) Le *pgcd* et le *ppcm* ne sont définis que dans $A/\mathcal{R}$, donc à un élément inversible près.

3) Dans $\mathbf{N}$ ou $\mathbf{Z}$ il y a une autre définition qui fait intervenir l'ordre naturel de $\mathbf{N}$. Il résulte de Bézout que les deux sont équivalentes. Voir, sur ma page web : `http://www.math.u-psud.fr/~perrin/CAPES/arithmetique/expose12-1.pdf`

1.3 *ppcm*, *pgcd* et idéaux

1.4 Proposition. *Si $m = ppcm(a,b)$, on a $(m) = (a) \cap (b)$. Autrement dit, (m) est aussi la borne inférieure des idéaux (a) et (b) dans l'ensemble de tous les idéaux de A.*

Démonstration. Comme a, b divisent m, on a $(m) \subset (a)$ et $(m) \subset (b)$, donc $(m) \subset (a) \cap (b)$. Inversement, si c est dans $(a) \cap (b)$ on a $c = aa' = bb'$, donc c est multiple de a et b, donc aussi de m par définition du *ppcm*, donc il est dans (m).

Pour le *pgcd*, on a un lien partiel avec la somme des idéaux :

1.5 Proposition-Définition. *Soient $a, b \in A - \{0\}$ et soit d un diviseur commun de a, b. Les propriétés suivantes sont équivalentes :*

1) On a $(d) = (a) + (b)$.

2) Il existe $\lambda, \mu \in A$ tels que l'on ait $d = \lambda a + \mu b$ **(relation de Bézout)**.

Si ces propriétés sont vérifiées, on a $d = pgcd(a,b)$. On dira que d est un pgcd **fort** *de a et b. Si 1 est un pgcd fort de a et b on dit que a et b sont* **fortement** *premiers entre eux.*

Démonstration. Le fait que d divise a et b donne $(a) \subset (d)$ et $(b) \subset (d)$, donc $(a) + (b) \subset (d)$ et l'inclusion inverse est équivalente à 2). Si l'on a ces propriétés et si c divise a et b, Bézout montre qu'il divise d.

1.6 *Remarques.* 1) Attention, l'idéal engendré par le *pgcd* n'est pas toujours la somme $(a) + (b)$ des idéaux. C'est vrai si A est principal, mais pas nécessairement sinon. Par exemple, dans $A = k[X,Y]$, on a $pgcd(X,Y) = 1$ mais l'idéal (X,Y) est strictement plus petit que l'idéal (1).

2) Il se peut que l'anneau vérifie le théorème de Bézout (pour tous $a, b \in A$, on a $(a, b) = (d)$ avec $d = pgcd(a, b)$) sans que A soit principal. C'est le cas si $A = \mathcal{H}(\mathbf{C})$, anneau des fonctions holomorphes sur $\mathbf{C}$ tout entier, voir ci-dessous.

1.4 Gauss avec des nombres fortement premiers entre eux

Le théorème de Gauss est facile lorsque a et b sont fortement premiers entre eux :

1.7 Théorème. (Théorème de Gauss) *Soient $a, b, c \in A$. On suppose que a divise bc et que a et b sont fortement premiers entre eux. Alors a divise c.*

Démonstration. On écrit une relation de Bézout : $\lambda a + \mu b = 1$ et on multiplie par c : $\lambda ac + \mu bc = c$.

2 Existence

2.1 *ppcm* implique *pgcd*

On sait que *pgcd* et *ppcm* existent si l'anneau est factoriel, voir par exemple [DP]. Les résultats qui suivent n'ont donc d'intérêt que si l'anneau n'est pas factoriel.

2.1 Proposition. *On suppose que a et b ont un ppcm noté m. Alors ils ont aussi un pgcd, noté d et on a $ab = dm$ aux inversibles près.*

Démonstration. On considère ab. Comme c'est un multiple de a et b, c'est un multiple de m et on a donc $ab = md$. On va montrer que d est un *pgcd* de a, b. Comme m est multiple de a on a $m = aa'$, d'où $ab = aa'd$ et, en simplifiant par a (c'est possible car A est intègre), $b = a'd$. On voit que d divise b et on montre de même qu'il divise a.

Soit maintenant c un diviseur commun de a, b. On a donc $a = ca''$ et $b = cb''$. Il est clair que $ca''b''$ est multiple de a, b, donc de m par définition du *ppcm*. Il en résulte que mc divise $c^2a''b'' = ab = md$, donc, par simplification par m, que c divise d.

2.2 Réciproque ?

La réciproque de 2.1 est fausse comme le montre l'exemple suivant.

2.2 Proposition. *On pose $A = \mathbf{Z}[i\sqrt{5}]$. Dans A, 3 et $2 + i\sqrt{5}$ ont 1 pour pgcd mais n'ont pas de ppcm.*

Démonstration. On renvoie à [TER] pour des détails. Notons déjà que 3 est irréductible dans A (car ce n'est pas une norme). Ses seuls diviseurs sont donc $\pm 1, \pm 3$. Comme 3 ne divise pas $2 + i\sqrt{5}$, le *pgcd* est bien égal à 1. S'il y avait un *ppcm*, ce serait donc $ab = 3(2 + i\sqrt{5})$ par la proposition précédente. Mais, comme 3 et $2 + i\sqrt{5}$ divisent $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, le *ppcm*, soit $m = 3(2 + i\sqrt{5})$ devrait diviser 9 lui aussi, donc $2 + i\sqrt{5}$ devrait diviser 3, ce qui est absurde.

Cependant on a une réciproque si a et b ont un *pgcd* fort :

2.3 Proposition. *Si a, b ont un pgcd fort, ils ont aussi un ppcm.*

Démonstration. On écrit $a = da'$, $b = db'$ et une relation de Bézout $d = \lambda a + \mu b$ qui donne aussi $1 = \lambda a' + \mu b'$, de sorte que a', b' sont fortement premiers entre eux. On pose $m = da'b'$. C'est un multiple de a et b et pour voir que c'est le *ppcm*, il suffit de montrer que si c est multiple de a, b il est multiple de m. Soit c un tel multiple. On a $c = au = bv$, donc $c = da'u = db'v$. Il suffit de montrer que a' (resp. b') divise v (resp. u). On a $a'u = b'v$, mais, comme a' et b' sont fortement premiers entre eux, le théorème de Gauss montre que a' divise v. L'autre assertion est analogue.

2.3 Avec tous les *pgcd*

Sans l'hypothèse de *pgcd* fort, on a aussi un résultat, mais il faut supposer que **tous les éléments** ont un *pgcd* :

2.4 Théorème. *Les propriétés suivantes sont équivalentes :*

1) Pour tous $a, b \in A - \{0\}$, a et b ont un ppcm noté m.

2) Pour tous $a, b \in A - \{0\}$, a et b ont un pgcd noté d.

De plus, on a alors $ab = md$ aux inversibles près et l'anneau A vérifie le théorème de Gauss.

Démonstration. Le sens 1) $\Longrightarrow$ 2) a été vu ci-dessus, ainsi que le rabiot sur $ab = md$. Pour l'autre sens, on commence par prouver un lemme.

2.5 Lemme. *On suppose la propriété 2) réalisée. Soient a, b deux éléments dont le pgcd est égal à 1. Alors, pour tout $c \neq 0$, on a $pgcd(ac, bc) = c$.*

Démonstration. Notons δ le *pgcd* de ac et bc. Comme c divise ac et bc, il divise δ et on a donc $\delta = c\epsilon$. Mais, on a aussi $ac = \delta a'$, $bc = \delta b'$, donc $ac = \epsilon c a'$ et $bc = \epsilon c b'$, d'où $a = \epsilon a'$ et $b = \epsilon b'$. Comme a et b ont pour *pgcd* 1, on voit que ϵ est inversible, donc $\delta = c$ aux inversibles près.

On peut alors prouver :

2.6 Théorème. (Théorème de Gauss) *On suppose la propriété 2) réalisée. Alors A vérifie le théorème de Gauss : si a divise bc et si pgcd*$(a, b) = 1$ *alors a divise c.*

Démonstration. D'après le lemme on a $pgcd(ac, bc) = c$ et comme a divise à la fois ac et bc, il divise leur *pgcd*, donc c.

Revenons au théorème 2.4.

Soient a, b deux éléments et d leur *pgcd*. On a $a = da'$, $b = db'$. De plus, le *pgcd* de a', b' est égal à 1. En effet, si l'on note δ ce *pgcd*, on voit que δd divise a et b, donc divise leur *pgcd*, c'est-à-dire d, et cela signifie que δ est inversible. Posons $m = da'b' = ab'$ et montrons que m est le *ppcm* de a, b. C'est évidemment un multiple commun. Si c est un autre multiple commun, on a $c = a\alpha = b\beta = da'\alpha = db'\beta$, donc $a'\alpha = b'\beta$. Mais alors, le théorème de Gauss montre que b' divise α, donc que $m = ab'$ divise $c = a\alpha$.

2.7 *Remarques.* 1) La preuve du théorème de Gauss donnée ci-dessus était celle que l'on donnait à mon époque sur $\mathbf{Z}$. Dans ce cas, ou celui d'un anneau principal, ou plus généralement si a et b vérifient une relation de Bézout $\lambda a + \mu b = 1$, on a vu en 1.7 une autre preuve qui consiste à écrire $c = \lambda ac + \mu bc$. L'intérêt de la preuve ci-dessus c'est qu'elle vaut dans le cas factoriel non principal, par exemple pour les anneaux de polynômes.

2) Si A vérifie le théorème de Gauss, il vérifie aussi le lemme d'Euclide : si p irréductible divise ab il divise a ou b (voir [DP] II 3.19).

2.8 Corollaire. *Soit A un anneau intègre vérifiant l'existence d'une décomposition en produit d'irréductibles (par exemple un anneau noetherien). Alors, les conditions suivantes sont équivalentes :*

1) A est factoriel.

2) Pour tous $a, b \in A - \{0\}$*, a et b ont un ppcm.*

3) Pour tous $a, b \in A - \{0\}$*, a et b ont un pgcd.*

Démonstration. C'est encore [DP] II 3.19, joint à ce qui précède.

2.9 *Remarques.* 1) Dans l'anneau $\mathbf{Z}[i\sqrt{5}]$ (qui n'est pas factoriel) il y a des éléments sans *pgcd* (par exemple 9 et $3(2 + i\sqrt{5})$, voir 2.10 ci-dessous).

2) Le corollaire est en défaut si l'on n'a pas l'existence de la décomposition en irréductibles : dans $\mathcal{H}(\mathbf{C})$ on a *pgcd* et *ppcm* mais l'anneau n'est pas factoriel.

3) Je ne connais pas d'exemple d'anneau qui vérifie le lemme d'Euclide mais où il n'y a pas de *ppcm* pour tous.

2.10 Proposition. *Dans l'anneau* $\mathbf{Z}[i\sqrt{5}]$*, les nombres* $a = 9$ *et* $b = 3(2 + i\sqrt{5})$ *n'ont pas de pgcd.*

Démonstration. On note que 3 et $2 + i\sqrt{5}$ divisent a et b (car $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$). Supposons que a et b ont un *pgcd* noté d. Comme 3 divise a, b, il divise d, donc $d = 3k$. Mais, comme d divise 9, k divise 3, donc $k = 1$ ou 3 au signe près. Le cas $k = 1$ est impossible car alors $d = 3$ mais $2 + i\sqrt{5}$, qui divise a et b, ne divise pas 3. Le cas $k = 3$ est impossible aussi car $d = 9$ ne divise pas b.

3 Un anneau exotique : l'anneau des entiers algébriques

Dans un premier temps, j'ai étudié cet anneau pour construire un exemple comme évoqué dans 2.9, remarque 3. Il ne fonctionne pas, mais il est cependant tout à fait intéressant à étudier.

3.1 Définition

Il s'agit de l'anneau des entiers algébriques. On utilise ici la notion d'entier sur un anneau et ses principales propriétés pour lesquelles on renvoie le lecteur à l'excellent livre de Samuel [S] ou au non moins excellent [ST].

3.1 Définition. *On note $\mathcal{O}$ le sous-anneau de $\mathbf{C}$ formé des z qui sont entiers sur $\mathbf{Z}$. On l'appelle* **anneau des entiers algébriques**

3.2 *Remarques.* 1) L'anneau $\mathcal{O}$ est intègre comme sous-anneau du corps $\mathbf{C}$, mais ce n'est pas un corps car $\sqrt{2}$ est dans $\mathcal{O}$, mais pas $1/\sqrt{2}$ dont le polynôme minimal sur $\mathbf{Q}$, $X^2 - 1/2$, n'est pas à coefficients entiers (voir [DP], III, §2,3, Ex. 11).

2) Dans $\mathcal{O}$, il n'y a aucun élément irréductible. En effet, si a est dans $\mathcal{O}$ et non inversible, il s'écrit $a = \sqrt{a}\,\sqrt{a}$ et cette décomposition est non triviale.

3) Il résulte de la remarque précédente que $\mathcal{O}$ ne vérifie pas l'existence d'une décomposition en irréductibles (donc n'est pas noetherien), mais vérifie évidemment l'unicité d'une telle décomposition et le lemme d'Euclide.

3.2 La "vraie" norme

Rappelons que, si z est entier sur $\mathbf{Z}$, son polynôme minimal (unitaire) P sur $\mathbf{Q}$ est à coefficients entiers et irréductible. Les racines de P sont les conjugués de z.

3.3 Définition. *Soit $z \in \mathcal{O}$, $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ son polynôme minimal unitaire sur $\mathbf{Z}$. La "vraie" norme de z, notée $N(z)$, est le produit des conjugués de z, c'est-à-dire $(-1)^n a_0$. C'est un élément de $\mathbf{Z}$.*

3.4 *Remarque.* **Attention**, la norme ainsi définie n'est pas la norme usuelle des corps de nombres (celle-ci est relative à une extension donnée). Par exemple, la norme de 3 dans $\mathbf{Q}(i\sqrt{5})$ est 9 alors que sa vraie norme est 3. Rappelons la définition et quelques propriétés de la norme usuelle.

• Si $K \subset L$ est une extension finie et si z est une élément de L, la norme $N_{L/K}(z)$ est le déterminant de μ_z, multiplication par z, dans le K-espace vectoriel L.

• On a la formule $N_{L/K}(zw) = N_{L/K}(z)N_{L/K}(w)$.

• Si M est une extension de degré n de L et si z est dans L on a $N_{M/K}(z) = N_{L/K}(z)^n = N_{L/K}(z^n)$.

Le lien entre les deux notions est explicité dans la proposition suivante.

3.5 Proposition. *Soit $z \in \mathcal{O}$, P son polynôme minimal, de degré n. Le corps $K = \mathbf{Q}(z)$ est alors un espace vectoriel de degré n et $N(z)$ est le déterminant de μ_z, multiplication par z dans K. On a donc $N(z) = N_{K/\mathbf{Q}}(z)$. Si L est une extension de degré s de K, on a $N_{L/\mathbf{Q}}(z) = N(z)^s$.*

Démonstration. La matrice de μ_z sur la base $1, z, \ldots, z^{n-1}$ est la matrice compagnon de P. Pour le dernier point, il suffit de prendre une base $e_1, \ldots, e_s$ de L sur K et d'utiliser la base télescopique $(e_i z^j)$.

3.6 *Remarque.* La formule usuelle $N(zw) = N(z)N(w)$ est fausse en général avec la vraie norme. Par exemple on a $N(3) = 3$, $N(2 + i\sqrt{5}) = 9$, mais $N(3(2 + i\sqrt{5})) = N(6 + 3i\sqrt{5}) = 36 + 45 = 81 \neq 3 \times 9$.

On a toutefois le succédané suivant.

3.7 Proposition. *Soient $z, w \in \mathcal{O}$. On suppose que les degrés de z, w et zw sont respectivement p, q, r et que l'extension $\mathbf{Q} \subset M := \mathbf{Q}(z, w)$ est de degré n (multiple de p, q, r). Alors on a la formule : $N(zw)^{n/r} = N(z)^{n/p}N(w)^{n/q}$.*

Démonstration. Cela résulte de la formule $N_{M/\mathbf{Q}}(zw) = N_{M/\mathbf{Q}}(z)N_{M/\mathbf{Q}}(w)$.

Une conséquence de cette formule est la caractérisation des éléments inversibles de $\mathcal{O}$:

3.8 Proposition. *Un élément $z \in \mathcal{O}$ est inversible si et seulement sa vraie norme est ± 1.*

Démonstration. Si $N(z)$ vaut ± 1, z a pour inverse le produit de ses conjugués au signe près. Inversement, si z est inversible on a $zw = 1$ avec $w \in \mathcal{O}$, donc, par 3.7, $N(z)^\alpha N(w)^\beta = 1^\gamma$ dans $\mathbf{Z}$, avec α, β, γ entiers. On en déduit que $N(z)$ est égal à ± 1.

3.9 Proposition. *Soient $a, b \in \mathcal{O}$. Si $N(a)$ et $N(b)$ sont premiers entre eux dans $\mathbf{Z}$, a et b sont premiers entre eux.*

Démonstration. Sinon, ils ont un diviseur commun c non inversible, donc de norme $\neq \pm 1$. On a alors $a = ca'$, $b = cb'$ donc $N(a)^{r_1} = N(c)^{p_1} N(a')^{q_1}$ et $N(b)^{r_2} = N(c)^{p_2} N(b')^{q_2}$. Si p est un diviseur premier de $N(c)$, on voit que p divise $N(a)$ et $N(b)$ contrairement à l'hypothèse.

3.10 *Remarques.* 1) La réciproque de cette proposition est fausse [1]. Ainsi, $a = 2 + i$ et $b = 2 - i$ sont des entiers algébriques, tous deux de norme 5, mais premiers entre eux (car on a une identité de Bézout : $a(b-1) - b = 1$).

2) Bien entendu, si $N(a)$ divise $N(b)$, ce n'est pas pour autant que a divise b. Exemple $a = 3$ et $b = 2 + i\sqrt{5}$, on a $b/a = \frac{2}{3} + \frac{i\sqrt{5}}{3}$ et ce nombre n'est pas dans $\mathcal{O}$ (sa trace vaut $4/3 \notin \mathbf{Z}$). En fait, a ne divise pas non plus une puissance de b, voir 3.13 ci-dessous.

3) Une référence intéressante sur ces questions est [Cahen], avec notamment la notion de *plus petit multiple rationnel*, très voisine de celle de norme.

3.3 Le théorème principal

Inutile de vouloir utiliser $\mathcal{O}$ pour trouver un exemple d'anneau sans *pgcd* ou *ppcm*. On a en effet :

3.11 Théorème. (Dedekind ?) *L'anneau $\mathcal{O}$ est bezoutien, autrement dit deux éléments quelconques de $\mathcal{O}$ ont un pgcd fort (et donc aussi un ppcm).*

Démonstration. (On en donne le principe, pour des détails voir [ST] §9.4 *How to make an ideal principal*, Th. 9.10).

Soient $a, b \in \mathcal{O}$ et $I = (a, b)$ l'idéal engendré. Il s'agit de montrer que I est principal. On considère $K = \mathbf{Q}(a, b)$ et son anneau d'entiers A. Soit h le nombre de classes de A. L'idéal $(I \cap A)^h$ est donc un idéal principal, soit c un générateur de cet idéal, $d = \sqrt[h]{c}$ et $L = K(d)$. Alors, dans l'anneau B des entiers de L, $I \cap B$ est engendré par d et on en déduit le résultat.

3.4 Un calcul de *pgcd*

On vient de voir que deux éléments ont toujours un *pgcd*. La proposition ci-dessous donne un exemple de calcul (comparer à 2.2) :

1. Merci à Antoine Chambert-Loir de m'avoir suggéré ce type de contre-exemple.

3.12 Proposition. *Le nombre* $\alpha = \dfrac{\sqrt{10}}{2} + i\dfrac{\sqrt{2}}{2}$ *(qui est l'une des racines carrées de* $2+i\sqrt{5}$*) est dans* $\mathcal{O}$*, non inversible et on a* $\alpha = pgcd(3, 2+i\sqrt{5})$*. De plus, on a une relation de Bézout :*

$$\lambda \times 3 + \mu(2+i\sqrt{5}) = \alpha \quad \text{avec} \quad \lambda, \mu \in \mathcal{O}$$

de sorte que α *est un pgcd fort de* 3 *et* $2+i\sqrt{5}$ *(et ces éléments ont donc aussi un ppcm en vertu de 2.3).*

Démonstration. En effet, si on considère son conjugué $\overline{\alpha} = \dfrac{\sqrt{10}}{2} - i\dfrac{\sqrt{2}}{2}$, $\alpha, -\alpha, \overline{\alpha}$ et $-\overline{\alpha}$ sont les quatre racines du polynôme $x^4 - 4x^2 + 9 = 0$, qui est irréductible sur $\mathbf{Z}$. Ce sont donc des éléments de $\mathcal{O}$. De plus, on a les formules $\alpha^2 = 2 + i\sqrt{5}$ et $\alpha\overline{\alpha} = 3$, ce qui montre que α est un diviseur commun de 3 et $2+i\sqrt{5}$. Si α était inversible, son inverse, qui est $\dfrac{\overline{\alpha}}{3}$, serait entier. Or, son équation minimale est $x^4 - \frac{4}{9}x^2 + \frac{1}{9} = 0$ qui n'est pas à coefficients entiers.

On a $\alpha + \overline{\alpha} = \sqrt{10}$ et $\alpha\overline{\alpha} = 3$, ce qui donne $(\alpha+\overline{\alpha})^2 - (\alpha\overline{\alpha})^2 = 1$. Cette relation est de la forme $\lambda\alpha + \mu\overline{\alpha} = 1$ avec $\lambda, \mu \in \mathcal{O}$. On en déduit $\lambda \times 3 + \mu(2+i\sqrt{5}) = \alpha$ et la conclusion.

3.13 *Remarque.* Le calcul précédent permet de montrer que $a := 3$ ne divise aucune puissance de $b := 2 + i\sqrt{5}$ (voir 3.10). En effet, cela signifierait que $\alpha\overline{\alpha}$ divise α^{2n}, donc que $\overline{\alpha}$ divise α^{2n-1}, mais on montre alors par récurrence, grâce à la relation de Bézout entre α et $\overline{\alpha}$, que $\overline{\alpha}$ divise α^k pour tout $k \geq 0$ et c'est absurde.

3.5 Un dernier calcul

3.14 Proposition. *Dans l'anneau* $\mathcal{O}$*, les éléments* $z = \sqrt{3}+1$ *et* $w = 1+i$ *sont associés.*

Démonstration. Notons que z et w sont bien dans $\mathcal{O}$, leur équation minimale respective étant $z^2 - 2z - 2 = 0$ et $w^2 - 2w + 2 = 0$. On a donc $N(z) = -2$ et $N(w) = 2$. Posons $u = w/z$. On calcule $u = -1 + \sqrt{3} - i + i\sqrt{3}$ et on calcule de même u^2, u^3, u^4 sur la base $1, \sqrt{3}, i, i\sqrt{3}$ de $\mathbf{Q}(i, \sqrt{3})$. On élimine les coefficients et il reste l'équation minimale de u :

$$u^4 + 2u^3 + 2u^2 - 2u + 1 = 0$$

ce qui montre que u est dans $\mathcal{O}$ et inversible (puisque de norme 1).

4 Un autre anneau exotique : les fonctions holomorphes sur un ouvert de C

On renvoie à [Cartan] ou à [Rudin] pour les résultats utilisés ici sur les fonctions holomorphes. Dans tout ce qui suit, U désigne un ouvert **connexe** (donc non vide) de $\mathbf{C}$. L'ensemble de toutes les fonctions holomorphes sur U forme un anneau [2] que l'on note $\mathcal{H}(U)$, voire $\mathcal{H}$ s'il n'y a pas d'ambiguité, et dont nous étudions les propriétés arithmétiques. On verra que l'anneau $\mathcal{H}$ présente quelques similitudes avec l'anneau $\mathcal{O}$ de la section précédente.

4.1 Rappels

4.1.1 Le principe des zéros isolés

Voir par exemple [Cartan] Ch. I, Prop. 4.1.
Pour $f \in \mathcal{H}(U)$, on note $V(f)$ l'ensemble des zéros de f dans U.

4.1 Proposition. *Si f est holomorphe sur U et non nulle, l'ensemble $V(f)$ de ses zéros est fermé et discret (donc [3] dénombrable).*

4.2 *Remarque.* Bien entendu, cette proposition est en défaut si U n'est pas connexe, il suffit de considérer une fonction nulle sur une composante et égale à 1 sur les autres.

On rappelle que pour toute fonction non nulle $f \in \mathcal{H}(U)$ et tout point $a \in U$, on peut écrire $f(z) = (z-a)^n h(z)$ avec h holomorphe sur U et non nulle en a et $n \in \mathbf{N}$. L'entier n est bien déterminé (c'est le plus petit entier tel que $f^{(n)}(a) \neq 0$), il est appelé **multiplicité** du zéro a de f (il peut être nul si f ne s'annule pas en a) et on le note $m_a(f)$.

4.1.2 Le théorème de Weierstrass

Voir [Rudin] th. 15.11.

4.3 Théorème. *Si A est un fermé discret de U, il existe une fonction $f \in \mathcal{H}(U)$ telle que $A = V(f)$.*

Plus précisément, si l'on se donne, pour chaque $a \in A$, un entier $\mu_a > 0$, il existe une fonction f telle que l'on ait $m_a(f) = \mu_a$ pour tout a.

2. Les éléments neutres pour l'addition et la multiplication sont les fonctions constantes égales à 0 et 1.
3. Voir Annexe

4.1.3 Le théorème d'interpolation Mittag-Leffler

Voir [Rudin] th. 15.13.

4.4 Théorème. *Soit A un fermé discret de U et, pour chaque $a \in A$, soit k_a un entier > 0 et soient $\lambda_{a,0}$, $\lambda_{a,1}$, ..., λ_{a,k_a} des nombres complexes. Alors, il existe $f \in \mathcal{H}(U)$ telle que l'on ait, pour tout $a \in A$, $f(a) = \lambda_{a,0}$, $f'(a) = \lambda_{a,1}$, ..., $f^{(k_a)}(a) = \lambda_{a,k_a}$.*

4.2 Les premiers résultats sur l'anneau $\mathcal{H}(U)$

4.5 Proposition. *Si U est connexe, l'anneau $\mathcal{H}(U)$ est intègre.*

Démonstration. Si l'on a $fg = 0$ avec $f, g \in \mathcal{H}$, on en déduit $V(f) \cup V(g) = U$. Si f et g sont non nuls, $V(f)$ et $V(g)$ sont dénombrables donc aussi U et c'est absurde.

4.6 *Remarque.* Si U n'est pas connexe, la propriété est en défaut (il suffit de prendre deux fonctions nulles sur des réunions disjointes de composantes). D'ailleurs, on montre aisément que si l'on a $U = U_1 \cup U_2$ avec U_1 et U_2 ouverts disjoints, l'anneau $\mathcal{H}(U)$ est le produit des $\mathcal{H}(U_i)$ (donc non intègre).

4.7 Proposition. *Le groupe $\mathcal{H}(U)^*$ des éléments inversibles de $\mathcal{H}(U)$ est l'ensemble des fonctions qui ne s'annulent pas sur U.*

4.8 *Remarque.* On sait que si U est simplement connexe et si $f \in \mathcal{H}(U)^*$ il existe $g \in \mathcal{H}(U)$ telle que $f = \exp(g)$.

4.9 Proposition. *Le corps des fractions de $\mathcal{H}(U)$ est le corps $\mathcal{M}(U)$ des fonctions méromorphes sur U.*

Attention, avec la définition locale usuelle de méromorphe, il n'est pas évident qu'une fonction méromorphe est de la forme f/g avec $f, g \in \mathcal{H}(U)$. Cela résulte du théorème de Weierstrass, voir [Rudin] 15.12. Une conséquence de cette proposition c'est que l'ensemble des zéros et des pôles d'une fonction méromorphe non nulle est un fermé discret.

4.10 Proposition-Définition. *Si f est méromorphe non nulle et $a \in U$ on peut écrire $f(z) = (z-a)^n h(z)$ avec $h \in \mathcal{H}(U)$ et $n \in \mathbf{Z}$. On pose encore $m_a(f) = n$ et cet entier est la multiplicité de a comme zéro (si $n > 0$) ou comme pôle (si $n < 0$) de f.*

4.3 Les diviseurs

Rappelons que le support d'une fonction $m : U \to \mathbf{Z}$ est l'ensemble des points $u \in U$ tels que $m(u) \neq 0$. On le note $\mathrm{Supp}\,(m)$.

4.11 Définition. *Un* **diviseur** *sur U est une application $m : U \to \mathbf{Z}$ dont le support est fermé et discret. L'ensemble des diviseurs sur U est noté $\mathcal{D}(U)$ (voire $\mathcal{D}$ s'il n'y a pas d'ambiguité).*

4.12 Proposition. *1) L'ensemble $\mathcal{D}(U)$ est un groupe abélien pour l'addition des fonctions (définie par $(m+n)(u) = m(u) + n(u)$ pour tout $u \in U$).*

2) C'est un groupe ordonné, dont l'ensemble d'éléments positifs est $\mathcal{D}^+(U) = \{m : U \to \mathbf{Z} \mid \forall u \in U,\ m(u) \geq 0\}$ (les diviseurs positifs).

3) L'ensemble $\mathcal{D}^+(U)$ est réticulé (deux éléments quelconques ont un inf *et un* sup *définis comme* inf *et* sup *au sens des fonctions).*

4) Ses éléments minimaux sont les fonctions caractéristiques des singletons.

Démonstration. Pour le point 1), il suffit de noter que $V(m+n) \subset V(m) \cup V(n)$ est un fermé discret. Pour 2), il faut vérifier que $\mathcal{D}^+(U)$ est stable par addition et que si m et $-m$ sont dans $\mathcal{D}^+(U)$, alors m est nul. Il n'y a pas de difficulté. La relation d'ordre est alors définie par $m \leq n \iff \forall u \in U,\ m(u) \leq n(u)$.

Pour 3), on définit le sup de deux fonctions m, n par la formule $\sup(m,n)(u) = \mathrm{Max}\,(m(u), n(u))$ et de même pour l'inf. Notons que le support de $\sup(m,n)$ est la réunion des supports de m, n et que celui de $\inf(m,n)$ est leur intersection.

4) Il est clair que la fonction caractéristique d'un point a est un élément minimal de $\mathcal{D}^+(U)$. Inversement, si une fonction m est > 1 en un point a ou si elle est non nulle en deux points a et b, il suffit de la diminuer d'une unité en a pour obtenir une fonction ≥ 0 et plus petite, ce qui montre que m n'est pas minimale.

4.4 Le lien entre $\mathcal{M}(U)$ et $\mathcal{D}(U)$

Comme l'ensemble des pôles et des zéros d'une fonction méromorphe est fermé discret, on a :

4.13 Proposition-Définition. *Soit $f \in \mathcal{M}(U)$, $f \neq 0$. L'application de U dans $\mathbf{Z}$ qui à a associe $m_a(f)$ est un diviseur, appelé* **diviseur associé** *à f et noté* $\mathrm{div}\, f$. *La fonction f est holomorphe si et seulement si* $\mathrm{div}\, f$ *est un diviseur positif (de support $V(f)$).*

On munit l'anneau $\mathcal{H}(U)$ de la relation de divisibilité et de la relation d'association $\mathcal{R}$ définies dans la section 1 et on considère l'ensemble ordonné $\mathcal{H}(U)/\mathcal{R}$. On a le théorème suivant :

4.14 Théorème. *1) L'application* div $: (\mathcal{M}(U)^*, \times) \to (\mathcal{D}(U), +)$ *est un homomorphisme de groupes, surjectif, de noyau* $\mathcal{H}(U)^*$.

2) L'application div *induit un isomorphisme d'ensembles ordonnés de* $\mathcal{H}(U) - \{0\}/\mathcal{R}$ *sur* $\mathcal{D}^+(U)$. *En particulier, les éléments irréductibles de* $\mathcal{H}(U)$ *sont les fonctions* $z \mapsto z - a$ *pour* $a \in U$, *à un inversible près. Deux éléments quelconques de* $\mathcal{H}(U)$ *ont un pgcd et un ppcm.*

Démonstration. 1) Si l'on écrit $f(z) = (z-a)^m h(z)$ et $g(z) = (z-a)^n k(z)$, avec $m, n \in \mathbf{Z}$ et $h, k \in \mathcal{H}$ non nulles en a, on a $(fg)(z) = (z-a)^{m+n} h(z)k(z)$, ce qui montre que $m_a(fg) = m_a(f) + m_a(g)$. Dire que f est dans le noyau de div signifie que $m_a(f) = 0$ pour tout a donc que f est holomorphe et inversible. La surjectivité de div vient du théorème de Weierstrass (appliqué à la partie positive et à la partie négative du diviseur).

2) Il est clair que l'application est bijective sur les ensembles considérés (si f et g ont le même diviseur, le quotient $h = f/g$ vérifie $\operatorname{div} h = 0$, donc est inversible). Elle respecte l'ordre car si f divise g on a $g = fh$ avec $h \in \mathcal{H}$ donc $\operatorname{div} g = \operatorname{div} f + \operatorname{div} h$ et $\operatorname{div} h$ est ≥ 0 puisque h est holomorphe, donc $\operatorname{div} f \leq \operatorname{div} g$. Comme les irréductibles sont les éléments minimaux de $\mathcal{H}/\mathcal{R}$, ils correspondent aux éléments minimaux de $\mathcal{D}^+(U)$, donc aux singletons. L'existence du *pgcd* et du *ppcm* dans $\mathcal{H}(U)$ résulte de celle de sup et inf dans $\mathcal{D}^+(U)$.

4.15 *Remarque.* On peut montrer directement que les irréductibles sont les fonctions $z - a$.

1) Si on a $z - a = fg$, f ou g s'annule en a, disons f, et l'on a $f(z) = (z-a)h(z)$ avec h holomorphe. Mais alors on a $gh = 1$, donc h est inversible et f et $z - a$ sont associés, ce qui montre l'irréductibilité.

2) Inversement, si f est irréductible, donc non inversible, elle s'annule en a et l'on a $f(z) = (z-a)h(z)$. Comme f est irréductible, h est inversible et f est associée à $z - a$.

4.16 Corollaire. *1) L'anneau* $\mathcal{H}(U)$ *ne vérifie pas la condition* (E) *de [DP] (existence de la décomposition en irréductibles).*

2) L'anneau $\mathcal{H}(U)$ *n'est ni noetherien, ni factoriel.*

Démonstration. 1) Si f est produit fini d'irréductibles, il s'écrit $f(z) = (z - a_1) \cdots (z - a_n)h(z)$ avec h inversible. On a ainsi $V(f) = \{a_1, \ldots, a_n\}$. Il suffit donc d'exhiber une fonction qui admet une infinité de zéros pour avoir un exemple de fonction non décomposable. C'est encore Weierstrass. (Dans le

cas $U = \mathbf{C}$ on peut prendre, par exemple, $f(z) = \sin \pi z$ qui s'annule sur $\mathbf{Z}$.) Le point 2) est conséquence de 1). (Pour noetherien, voir [DP] Ch. II, 3.17).

4.17 *Remarque.* On peut prouver directement que $\mathcal{H}$ n'est pas noetherien en exhibant une suite croissante non stationnaire d'idéaux. Par exemple, pour $U = \mathbf{C}$, on pose :

$$I_k = \{ f \in \mathcal{H}(\mathbf{C}) \ \mid \ V(f) \supset \mathbf{N} - \{0, 1, \ldots, k\} \ \}.$$

On a évidemment $I_k \subset I_{k+1}$ et l'inclusion est stricte à cause de la fonction $\dfrac{\sin \pi z}{z(z-1)\cdots(z-k-1)}$.

4.5 Le théorème de Bézout

Notons d'abord le lemme suivant :

4.18 Lemme. *Deux éléments $f, g \in \mathcal{H}(U)$ sont premiers entre eux si et seulement si on a $V(f) \cap V(g) = \emptyset$.*

Démonstration. Supposons $V(f) \cap V(g) = \emptyset$. Si h divise f et g, on a $V(h) \subset V(f)$ et $V(h) \subset V(g)$ donc $V(h) = \emptyset$ et h est inversible, ce qui signifie que f, g sont premiers entre eux. Inversement, si $a \in V(f) \cap V(g) \neq \emptyset$, la fonction $z - a$ divise f et g.

On a alors :

4.19 Théorème. (Bézout) *Soient $f, g \in \mathcal{H}(U) - \{0\}$, premiers entre eux. Il existe $u, v \in \mathcal{H}(U)$ tels que l'on ait $uf + vg = 1$.*

Démonstration. Il s'agit de trouver une fonction $v \in \mathcal{H}(U)$ telle que $u := (1 - vg)/f$ soit holomorphe. Pour cela, il suffit que $1 - vg$ admette un zéro d'ordre $\geq n$ en tout point qui est un zéro d'ordre $n > 0$ de f. Soit a un tel point. Comme f et g sont premiers entre eux, g ne s'annule pas en a, de sorte que $1/g$ est holomorphe en a et il revient au même de demander que $\dfrac{1}{g} - v$ admette un zéro d'ordre n en a. Mais cela signifie qu'on doit avoir $v(a) = \left(\frac{1}{g}\right)(a)$, $v'(a) = \left(\frac{1}{g}\right)'(a)$, ..., $v^{(n)}(a) = \left(\frac{1}{g}\right)^{(n)}(a)$ et une telle fonction v existe en vertu de Mittag-Leffler 4.4.

4.20 Corollaire. *Tout idéal de type fini de $\mathcal{H}(U)$ est principal.*

Démonstration. En raisonnant par récurrence sur le nombre de générateurs de I on se ramène au cas $I = (f, g)$. Si $h = pgcd(f, g)$, on a $f = hf_0$ et $g = hg_0$ avec f_0, g_0 premiers entre eux. Mais alors, il existe u, v tels que $uf_0 + vg_0 = 1$ et on en déduit $h = uf + vg$, ce qui montre qu'on a $(f, g) = (h)$.

4.6 Les idéaux de $\mathcal{H}(U)$

4.6.1 Filtres

Rappelons la définition d'un filtre et quelques propriétés.

4.21 Définition. *Soit X un ensemble ordonné admettant un plus petit élément noté 0 et tel que deux éléments quelconques admettent un* inf. *On appelle* **filtre** *une partie F de X telle que :*

1) $0 \notin F$,

2) si $a, b \in F$, $\inf(a, b) \in F$,

3) si $a \in F$ *et* $b \geq a$, *alors* $b \in F$.

Un **ultrafiltre** *est un filtre qui est maximal pour la relation d'inclusion des parties de X.*

4.22 *Exemples.* 1) Si a est non nul, $F_a = \{b \in X \mid b \geq a\}$ est un filtre, appelé filtre **principal** associé à a. C'est un ultrafiltre si et seulement si a est minimal dans $F - \{0\}$.

2) Si $F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots$ est une suite croissante de filtres, $F = \bigcup_{i \in \mathbf{N}^*} F_i$ est un filtre. C'est le cas par exemple avec $F_i = F_{a_i}$ si la suite (a_n) est croissante.

3) Le point 2) et le théorème de Zorn montrent que tout filtre est majoré par un ultrafiltre.

4.6.2 Filtres et idéaux

On a le théorème suivant :

4.23 Théorème. *On considère l'application* div $: \mathcal{H}(U) - \{0\} \to \mathcal{D}^+(U)$.

1) L'application div *induit, par passage aux parties, une bijection croissante de l'ensemble des idéaux de $\mathcal{H}(U)$, non nuls et distincts de $\mathcal{H}(U)$, sur l'ensemble des filtres de $\mathcal{D}^+(U)$.*

2) Dans cette bijection, les idéaux principaux correspondent aux filtres principaux et les idéaux maximaux aux ultrafiltres.

3) Les idéaux (z-a), $a \in U$, sont maximaux et sont caractérisés comme les idéaux maximaux m de $\mathcal{H}(U)$ qui sont tels que l'homomorphisme canonique $\mathbf{C} \to \mathcal{H}(U) \to \mathcal{H}(U)/m$ (associé aux fonctions constantes) soit un isomorphisme.

4) Il existe des idéaux maximaux non principaux dans $\mathcal{H}$.

Démonstration. 1) Soit I un idéal de $\mathcal{H}(U)$, distinct de (0) et de $\mathcal{H}(U)$. On associe à I l'ensemble $\operatorname{div} I$ des diviseurs $\operatorname{div} f$ pour $f \in I$, $f \neq 0$. Montrons que $\operatorname{div} I$ est un filtre. Comme I n'est pas l'idéal unité, il ne contient pas

d'inversible, de sorte que $\operatorname{div} f \neq 0$ si $f \in I$. Si b est dans $\mathcal{D}^+(U)$ avec $b \geq \operatorname{div} f$, $f \in I$, on a $b = \operatorname{div} f + a$ avec $a \in \mathcal{D}^+(U)$ et, par Weierstrass, il existe $g \in \mathcal{H}(U)$ tel que $a = \operatorname{div} g$. Mais alors, on a $b = \operatorname{div} f + \operatorname{div} g = \operatorname{div}(fg)$ et $fg \in I$, donc $b \in \operatorname{div} I$. Enfin, pour obtenir l'inf de $\operatorname{div} f$ et $\operatorname{div} g$, $f, g \in I$, on considère $h = pgcd(f, g)$. On a bien $\operatorname{div} h = \inf(\operatorname{div} f, \operatorname{div} g)$. De plus, on a une relation de Bézout $h = uf + vg$, de sorte que h est dans I et on a la conclusion.

La croissance de l'application est claire. Il reste à montrer la bijection. Pour cela, soit F un filtre. On pose :

$$I_F = \{ f \in \mathcal{H}(U), f \neq 0 \ \mid \ \operatorname{div} f \in F \ \}.$$

Montrons que I_F est un idéal. C'est clair pour l'assertion sur le produit. Pour la somme, soient $f, g \in I_F$ et h leur $pgcd$. On a donc $\operatorname{div} h = \inf(\operatorname{div} f, \operatorname{div} g)$, donc $\operatorname{div} h$ est dans F puisque F est un filtre. Mais, comme h divise f, g, il divise $f + g$ et on a donc $\operatorname{div} h \leq \operatorname{div}(f + g)$, de sorte que $\operatorname{div}(f + g)$ est dans F, donc $f + g$ dans I_F.

Alors, l'application $F \mapsto I_F$ est la réciproque de $I \mapsto \operatorname{div} I$. En effet, il est clair qu'on a $\operatorname{div} I_F \subset F$ et la réciproque vient de Weierstrass. Pour l'autre sens, $I(\operatorname{div} I)$ est l'ensemble des f tels que $\operatorname{div} f = \operatorname{div} g$ avec $g \in I$. Mais cela signifie que f et g sont associés et donc que f est dans I.

2) L'assertion sur les idéaux principaux est évidente, et celle sur les idéaux maximaux et les ultrafiltres résulte de la croissance.

3) Considérons l'homomorphisme canonique $\chi_a : \mathcal{H}(U) \to \mathbf{C}$ défini par $f \mapsto f(a)$ (évaluation de f en a). Il est surjectif à cause des constantes et son noyau est l'idéal $(z - a)$ qui est donc maximal. De plus, la composée de χ_a avec l'injection naturelle i de $\mathbf{C}$ dans $\mathcal{H}(U)$ qui à c associe la fonction constante et égale à c est l'identité.

Inversement, si m est un idéal maximal qui n'est pas de la forme $(z - a)$, il est clair que m ne contient aucune fonction polynôme (sinon, comme m est premier, il contiendrait un facteur $(z - a)$ et serait égal à $(z - a)$). Il en résulte que l'anneau des polynômes $\mathbf{C}[z]$ s'injecte dans le quotient $\mathcal{H}(U)/m$ ce qui montre que la composée $p \circ i$ n'est pas surjective.

4) On considère un fermé discret infini $A \subset U$, $A = \{a_n, n \in \mathbf{N}\}$. Soit I_n l'idéal défini par :

$$I_n = \{ f \in \mathcal{H}(U) \ \mid \ V(f) \supset A - \{a_0, \ldots, a_n\} \ \}.$$

La suite des idéaux I_n est croissante, de sorte que $I = \bigcup_{n \in \mathbf{N}} I_n$ est encore un idéal. Soit m un idéal maximal contenant I. Je dis que ce n'est pas un idéal principal $(z - a)$. En effet, il existe n tel que $a \notin A - \{a_0, \ldots, a_n\}$ et, par Mittag-Leffler, on peut trouver $f \in \mathcal{H}(U)$, nulle sur $A - \{a_0, \ldots, a_n\}$ et non nulle en a, de sorte qu'on a $f \in I_n$ et $f \notin (z - a)$.

4.24 *Remarque.* Un idéal de type fini de $\mathcal{H}(U)$ qui est premier est maximal (car il est principal). En revanche, il existe des idéaux premiers (non de type fini) et non maximaux, voir [4] l'article [H].

4.7 Le théorème de Chevalley-Kakutani

Voir aussi [L] sur ce sujet.

4.25 Théorème. *Soient U, U' deux ouverts de $\mathbf{C}$. Alors, les anneaux $\mathcal{H}(U)$ et $\mathcal{H}(u')$ sont isomorphes comme $\mathbf{C}$-algèbres si et seulement si U et U' sont conformément équivalents.*

Démonstration. Rappelons que deux ouverts de $\mathbf{C}$ sont dits conformément équivalents s'il existe une bijection holomorphe $\varphi : U \to U'$ (sa réciproque est alors holomorphe elle aussi). Dans ce cas, il est clair que l'application de $\mathcal{H}(U')$ dans $\mathcal{H}(U)$ qui à f associe $f \circ \varphi$ est un isomorphisme d'algèbres.

Inversement, supposons qu'on détienne un tel isomorphisme d'algèbres $\psi : \mathcal{H}(U) \to \mathcal{H}(U')$. Alors, ψ induit une bijection sur les idéaux maximaux, qui induit un isomorphisme sur leurs corps résiduels. En vertu de 4.23, on a ainsi une bijection des idéaux maximaux de type $(z-a)$ de $\mathcal{H}(U)$ sur ceux de même type de $\mathcal{H}(U')$, donc une bijection φ de U sur U'. Appelons u l'élément de $\mathcal{H}(U)$ défini par $u(z) = z$. On va montrer qu'on a $\psi^{-1}(u) = \varphi$, de sorte que φ sera holomorphe, donc une représentation conforme de U sur U'.

Pour cela, soit $a \in U$ et $b = \varphi(a) \in U'$. La définition de φ, montre que l'on a $\psi((z-a)) = (z-b)$. Mais, l'application $z \mapsto z-b$ n'est autre que $u-b$ et on a donc $\psi^{-1}(u-b) \in (z-a)$, ou encore, puisque ψ est un isomorphisme d'algèbres, $\psi^{-1}(u) - b \in (z-a)$. Cela signifie que $\psi^{-1}(u) - b$ est nulle en a, donc qu'on a $\psi^{-1}(u)(a) = b = \varphi(a)$. Comme cela vaut pour tout $a \in U$, on a bien montré $\varphi = \psi^{-1}(u)$.

5 Annexes

5.1 Ensembles discrets

Rappelons qu'un sous-ensemble E d'un espace topologique X est dit discret si la topologie induite sur E par celle de X est discrète, ce qui signifie que, pour tout $x \in E$, il existe un ouvert U_x de X tel que $U_x \cap E = \{x\}$.

5.1 Proposition. *1) Un sous-ensemble fermé et discret d'un compact est fini.*

2) Un sous-ensemble fermé E discret d'un ouvert U de $\mathbf{C}$ est dénombrable.

4. Merci à Antoine Chambert-Loir de m'avoir signalé cette référence.

Démonstration. 1) Si X est compact et E discret fermé, on a un recouvrement ouvert de X par les U_x, $x \in E$ et E^c. On peut en extraire un recouvrement fini : U_{x_1}, ..., U_{x_n}, E^c. Comme $U_{x_i} \cap E = \{x_i\}$, on voit que E contient seulement les points $x_1, \ldots, x_n$.

2) On peut supposer $U = \mathbf{C}$. Le point 1) montre qu'il n'y a qu'un nombre fini de points de E dans le disque fermé $D(0, n)$ et on en déduit que E est dénombrable.

5.2 *Remarques.* 1) Le point 2) vaut pour un espace localement compact dénombrable à l'infini.

2) Dans $\mathbf{C}$ on peut enlever l'hypothèse E fermé. En effet, on se ramène au cas d'un disque D. On a, pour chaque $x \in E$, un ouvert U_x qui ne contient pas d'autre point de E et on peut supposer qu'il s'agit d'un disque de rayon r_x. S'il y a une infinité non dénombrable de points de E, il existe un entier $n > 0$ tel qu'il y ait une infinité de x avec $r_x > 1/n$. On a ainsi une infinité A de points de E dont les distances mutuelles sont $> 1/n$. Les disques de centres $a \in A$ et de rayons $1/(2n)$ sont alors disjoints et contenus dans D. Mais c'est impossible car la somme de leurs aires est infinie.

6 Une dernière question

Trouver un exemple d'anneau qui vérifie le lemme d'Euclide mais où il n'y a pas de ppcm (ou de pgcd) pour tous.

(Il y en avait d'autres, mais Antoine Chambert-Loir est passé par là ...)

7 Références

[Cahen] CAHEN Eugène, *Sur l'arithmétique du corps des nombres algébriques*, Bull. S.M.F., tome 56 (1928), p. 7-17.

[Cartan] CARTAN Henri, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann, 1964.

[H] HENRIKSEN Melvin, *On the prime ideals of the ring of entire functions*, Pacific J. Math. , vol. 3, no. 4, (1953), p. 711-720,
`http://msp.org/pjm/1953/3-4/pjm-v3-n4-p04-s.pdf`

[L] LANG Serge, *Corps de fonctions méromorphes sur une surface de Riemann*, Séminaire Bourbaki, 9 (1964-1966), Exp. No. 292, 2 p.

[DP] PERRIN Daniel, *Cours d'algèbre*, Ellipses, 1996.

[Rudin] RUDIN Walter, *Real and complex analysis*, M$^{\text{c}}$Graw-Hill, 1966.

[S] SAMUEL Pierre, *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[ST] STEWART Ian & TALL David, *Algebraic Number Theory*, Chapmann-Hall, 1987.

[TER] PERRIN Daniel, *Anneaux d'entiers des corps quadratiques imaginaires*, rédaction de TER (disponible pour les collègues sur simple demande).