Anneaux d'entiers des corps quadratiques imaginaires

Daniel PERRIN

Ce texte reprend le thème d'un TER (Travail d'Étude et de Recherche de maîtrise) plusieurs fois posé à Orsay. Je me suis notamment appuyé sur les rédactions d'Émilie Battaglin, Émilie Bertin, Loïc Cappanera, Anouk Perrot, Sylvie Rauch et Adeline Yvernes que je remercie.

On renvoie à [DP] *pour le b.a. ba de théorie des anneaux et des corps utilisé ici.*

1 Introduction

1.1 Motivation

La motivation principale pour l'étude des anneaux d'entiers des corps de nombres est essentiellement arithmétique. L'idée, pour traiter un problème d'arithmétique portant sur les entiers ou les rationnels, de sortir du cadre de ces nombres pour travailler dans les nombres réels ou complexes est ancienne. Certains pensent que c'est ainsi que Fermat imaginait de prouver son grand théorème [1]. On peut, en tous cas, la faire remonter à Euler (1707-1783) et à ses contemporains Lagrange (1736-1813) et Legendre (1752-1833) et elle est développée par Gauss (1777-1855), puis Kümmer (1810-1893) (pour aborder le théorème de Fermat). Outre Kümmer, la théorie des anneaux de nombres est essentiellement l'œuvre de Dedekind (1831-1916) et Kronecker (1823-1891). On renvoie à [Bachet] et [Bachet-o] pour des détails sur ces aspects historiques et une bibliographie complémentaire.

Deux problèmes élémentaires vont permettre de comprendre le principe de la démarche.

• *Quels sont les entiers $d \in \mathbf{Z}$ qui s'écrivent sous la forme $d = a^2 - b^2$ avec $a, b \in \mathbf{Z}$?*

1. Bourbaki le suggère dans la note historique du chapitre 7 du livre d'algèbre commutative, mais cela ne semble pas être l'avis d'André Weil, voir [Weil].

On trouve aisément les solutions en factorisant le second membre : $d = (a-b)(a+b)$ et en utilisant les propriétés de l'anneau $\mathbf{Z}$ (notamment la décomposition unique en produit de facteurs premiers). Voir au besoin [ME], exercice 39.

• *Résoudre l'équation diophantienne $x^2 + y^2 = z^2$, c'est-à-dire en trouver les solutions entières*[2].

Là encore, la ruse est d'écrire $x^2 = z^2 - y^2 = (z-y)(z+y)$ et de faire des raisonnements de divisibilité dans $\mathbf{Z}$, voir dans [ME] le problème sur les triplets pythagoriciens.

On voit que l'idée principale de cette méthode est de décomposer les entiers en produits de facteurs, car c'est sous cette forme que l'on peut utiliser la divisibilité. Bien sûr, cette méthode ne fonctionne pas toujours car il n'y a pas nécessairement une telle factorisation entière. Cependant, on peut tenter de s'en inspirer en sortant du cadre des entiers. Voici trois exemples :

1) Si au lieu de chercher les d de la forme $a^2 - b^2$ on cherche les entiers sommes de deux carrés : $n = a^2 + b^2$, $a, b \in \mathbf{N}$, on ne peut plus factoriser le second membre dans $\mathbf{Z}$, mais on peut le faire en passant aux complexes : $d = (a+ib)(a-ib)$. Cela amène à sortir de $\mathbf{Z}$ pour travailler dans l'anneau $\mathbf{Z}[i]$ des entiers de Gauss, voir [DP] Ch. II. De la même manière, on étudiera les entiers de la forme $a^2 + db^2$ en travaillant dans $\mathbf{Z}[i\sqrt{d}]$, voir section 6 ci-dessous.

2) La résolution de l'équation diophantienne $t^3 = x^2 + d$ (dite équation de Bachet) en factorisant $x^2 + d = (x + i\sqrt{d})(x - i\sqrt{d})$ nécessite elle aussi de travailler dans $\mathbf{Z}[i\sqrt{d}]$, voir par exemple [Bachet] et [Bachet-o].

3) La voie d'approche du grand théorème de Fermat (il n'y a pas de solutions entières non triviales de $x^n + y^n = z^n$ pour $n \geq 3$, contrairement au cas $n = 2$ vu ci-dessus) inaugurée par Kümmer consiste à factoriser :

$$x^n + y^n = (x+y)(x+\zeta y)\cdots(x+\zeta^{n-1}y)$$

dans l'anneau $\mathbf{Z}[\zeta]$ où ζ est une racine n-ième primitive de l'unité.

Dans tous ces exemples, le principe consiste à travailler dans un anneau A plus grand que l'anneau des entiers et adapté au problème au sens où on y détient une factorisation, et à y faire des raisonnements de divisibilité. Cela n'est possible que si l'anneau a suffisamment de bonnes propriétés arithmétiques, qui permettent de copier ce que l'on fait sur $\mathbf{Z}$, la propriété essentielle étant l'existence d'une décomposition unique en produit de facteurs premiers (i.e. le fait que A est factoriel). Attention, les anneaux considérés

2. Il y en a une infinité, dont $3, 4, 5$ ou $5, 12, 13$, etc. qui correspondent aux longueurs des côtés de triangles rectangles.

ci-dessus ne sont pas toujours factoriels. Ainsi, par exemple, dans $\mathbf{Z}[i\sqrt{5}]$ on a deux décompositions non équivalentes du nombre 6 en produit de facteurs irréductibles :

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

C'est cette difficulté fondamentale de la théorie qui a notamment motivé les travaux de Kümmer et ses successeurs. Pour une discussion sur ce thème, voir [DP] pour l'exemple des deux carrés, [Bachet], [Bachet-o], ou section 6 ci-dessous, [S], [ST].

Le but de cette rédaction est d'examiner cette question des propriétés arithmétiques dans le cas de l'anneau des entiers d'un corps quadratique imaginaire $\mathbf{Q}(i\sqrt{d})$ que l'on a vu intervenir dans plusieurs exemples et qui présente l'avantage d'être (au moins au départ) très simple.

1.2 Rappels et notations

1.2.1 Anneaux intégralement clos

On considère ici des anneaux commutatifs. On renvoie à [DP] pour les définitions suivantes concernant les anneaux : intègre, factoriel, principal, euclidien, noethérien, ou concernant les idéaux : premier, maximal et pour la notion de corps des fractions de A noté $\mathrm{Fr}\, A$. Rappelons simplement :

1.1 Définition. *1) Soient $A \subset B$ deux anneaux et $x \in B$. On dit que x est* **entier** *sur A s'il vérifie une équation* **unitaire** *:*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

avec $a_i \in A$. On dit que B est entier sur A si tous les éléments de B le sont.

2) Soit A un anneau intègre et K son corps de fractions. On dit que A est **intégralement clos** *si tout élément de K entier sur A est dans A.*

1.2 *Exemples.* 1) L'élément $x = \sqrt{2}$ est entier sur $\mathbf{Z}$ car il vérifie l'équation unitaire $x^2 - 2 = 0$. En revanche $y = 1/\sqrt{2}$ est algébrique sur $\mathbf{Q}$ (il vérifie $2y^2 - 1 = 0$), mais pas entier sur $\mathbf{Z}$.

2) L'anneau $A = \mathbf{Z}[i\sqrt{3}]$ n'est pas intégralement clos. En effet, l'élément $j = \dfrac{-1 + i\sqrt{3}}{2}$ est dans le corps des fractions $\mathbf{Q}(i\sqrt{3})$ de A, entier sur A (il vérifie $j^2 + j + 1 = 0$) mais pas dans A.

La notion d'anneau intégralement clos est importante pour deux raisons. La première, c'est que cette propriété est une condition nécessaire pour d'autres :

1.3 Proposition. *Soit A un anneau. On a les implications : A euclidien $\Longrightarrow$ A principal $\Longrightarrow$ A factoriel $\Longrightarrow$ A intégralement clos $\Longrightarrow$ A intègre.*

Démonstration. Montrons l'implication factoriel implique intégralement clos, pour les autres le lecteur consultera [DP]. Soit $K = \mathrm{Fr}\, A$ et $x \in K$ entier sur A. Comme A est factoriel, on peut écrire $x = p/q$ avec p, q premiers entre eux. On a donc une relation :

$$\Big(\frac{p}{q}\Big)^n + a_{n-1}\Big(\frac{p}{q}\Big)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0$$

avec $a_i \in A$. On en déduit, en multipliant par q^n :

$$p^n = -a_{n-1}p^{n-1}q - \cdots - a_1pq^{n-1} - a_0q^n.$$

Comme q divise le second membre il divise p^n et comme p et q sont premiers entre eux, le lemme de Gauss (qui résulte de l'hypothèse A factoriel) montre que q est inversible, donc que x est dans A.

La seconde raison de l'intérêt de la notion d'anneau intégralement clos c'est qu'on dispose d'un moyen de fabriquer un anneau intégralement clos à partir d'un anneau qui ne l'est pas :

1.4 Proposition. *Soit A un anneau intègre, K son corps des fractions. L'ensemble A' des $x \in K$ entiers sur A est un sous-anneau de K qui contient A et est intégralement clos. On l'appelle* **clôture intégrale** *de A.*

Démonstration. Voir les références [S] ou [ST].

1.5 Commentaire. Si l'on veut faire de la divisibilité dans un anneau "comme dans **Z**", il faut que l'anneau soit factoriel et donc intégralement clos. Dans les exemples que nous étudierons, si ce n'est pas le cas, on remplacera l'anneau par sa clôture intégrale.

1.6 *Remarque.* En fait, voir [Bachet] ou la section 6 ci-dessous, on peut faire de l'arithmétique sur des anneaux non factoriels (mais cependant intégralement clos) en remplaçant la notion de décomposition unique d'un élément en éléments premiers par celle d'un idéal en produit d'idéaux premiers, voir [S] ou [ST]. C'est l'apport essentiel de Kümmer. Les anneaux qui vérifient cette condition sont les anneaux dits de Dedekind (intégralement clos, noethérien, de dimension 1) et les anneaux de nombres vérifient ces propriétés (voir 2.8). Pour ces anneaux, on montre qu'il y a équivalence entre les conditions factoriel et principal, voir ci-dessous 2.10.

1.2.2 Corps et anneaux de nombres

Précisons les notations :

1.7 Définition. *On appelle* **corps de nombres** *une extension finie K de $\mathbf{Q}$ (i.e. un corps K qui contient $\mathbf{Q}$ et est un $\mathbf{Q}$-espace vectoriel de dimension finie) et* **anneau des entiers** *du corps de nombres K l'ensemble A des $x \in K$ entiers sur $\mathbf{Z}$. C'est un anneau intégralement clos.*

1.2.3 Reconnaître qu'un anneau est factoriel

Rappelons que tout anneau noethérien vérifie l'existence d'une décomposition en produit de facteurs premiers, voir [DP] Ch. II 3.17. Le ressort de nos investigations sera le lemme suivant (*loc. cit.* 3.19) :

1.8 Lemme. *Soit A un anneau intègre.*

1) Soit $p \in A$, non nul et non inversible. Si l'idéal (p) est premier, l'élément p est irréductible.

2) Réciproquement, si l'anneau est factoriel et si p est irréductible, l'idéal (p) est premier.

2) Inversement, si pour tout p irréductible, l'idéal (p) est premier, l'anneau vérifie l'unicité de la décomposition en irréductibles. Si de plus il est noethérien, il est factoriel.

1.9 *Remarque.* Dire que l'idéal (p) est premier signifie que p vérifie le "lemme d'Euclide" : si p divise un produit ab, il divise a ou b.

2 Les anneaux d'entiers des corps quadratiques

2.1 Les corps quadratiques

2.1 Proposition-Définition. *Soit Δ un nombre entier relatif, $\neq 0, 1$ et sans facteur carré et soit $\sqrt{\Delta}$ une racine carrée de Δ dans $\mathbf{C}$. L'ensemble $\mathbf{Q}(\sqrt{\Delta})$ formé des nombres complexes de la forme $a + b\sqrt{\Delta}$ avec $a, b \in \mathbf{Q}$ est un sous-corps de $\mathbf{C}$, qui est un espace vectoriel de dimension 2 sur $\mathbf{Q}$. On désigne ces corps sous le nom de* **corps quadratiques**. *On note $\mathbf{Z}[\sqrt{\Delta}]$ l'ensemble des $a + b\sqrt{\Delta}$ avec $a, b \in \mathbf{Z}$. C'est un sous-anneau de $\mathbf{Q}(\sqrt{\Delta})$.*

Démonstration. C'est une vérification facile, le seul point est de noter que $\sqrt{\Delta}$ n'est pas rationnel, ce qui a deux conséquences :

a) la dimension de $\mathbf{Q}(\sqrt{\Delta})$ sur $\mathbf{Q}$ est bien égale à 2,

b) si a, b ne sont pas tous deux nuls, $a + b\sqrt{\Delta}$ admet un inverse égal à $\dfrac{a - b\sqrt{\Delta}}{a^2 - \Delta b^2}$.

2.2 *Remarques.* 1) Si Δ admet un facteur carré : $\Delta = k^2\Delta'$ avec k entier > 1 et $\Delta' \in \mathbf{Z}$, le corps $\mathbf{Q}(\sqrt{\Delta})$ est égal à $\mathbf{Q}(\sqrt{\Delta'})$ ce qui permet de se ramener au cas sans facteur carré.

2) Un entier $\neq 0, 1$ sans facteur carré s'écrit $\Delta = \pm p_1 \dots p_r$ avec les p_i premiers distincts (et $r \geq 1$ si le signe est $+$).

3) Les corps $\mathbf{Q}(\sqrt{\Delta})$ décrivent toutes les extensions de degré 2 de $\mathbf{Q}$ (une telle extension est engendrée par une racine d'une équation du second degré, donc, *via* le discriminant, par la racine carrée d'un rationnel, et le corps engendré par $\sqrt{p/q}$ est le même que celui engendré par $\sqrt{pq}$).

4) Quand Δ est négatif, on note $\Delta = -d$ et le corps quadratique associé est $\mathbf{Q}(i\sqrt{d})$.

2.2 Conjugaison, trace, norme

Le corps $\mathbf{Q}(\sqrt{\Delta})$ admet un automorphisme, la conjugaison [3], σ, qui à $z = a + b\sqrt{\Delta}$ associe $\overline{z} = a - b\sqrt{\Delta}$. Le groupe de Galois de $\mathbf{Q}(\sqrt{\Delta})$ sur $\mathbf{Q}$ est le groupe à deux éléments $\{\mathrm{Id}, \sigma\}$. L'anneau $\mathbf{Z}[\sqrt{\Delta}]$ est stable par σ.

On définit aussi la trace d'un élément $z = a + b\sqrt{\Delta}$ par la formule $\mathrm{Tr}\,(z) = z + \overline{z} = 2a \in \mathbf{Q}$ et sa norme [4] $N(z) = z\overline{z} = a^2 - \Delta b^2 \in \mathbf{Q}$. Il est clair que la trace est additive et la norme multiplicative. On note que si z est dans $\mathbf{Z}[\sqrt{\Delta}]$, sa trace et sa norme sont des entiers.

2.3 Lemme. *Soit $z = a + b\sqrt{\Delta} \in \mathbf{Q}(\sqrt{\Delta})$. Le polynôme minimal de z sur $\mathbf{Q}$ est $X - z$ si z est dans $\mathbf{Q}$ et sinon c'est $X^2 - \mathrm{Tr}\, z\, X + N(z) = (X - z)(X - \overline{z})$.*

2.3 L'anneau des entiers

2.3.1 Énoncé

Comme on l'a rappelé plus haut, quand on a une extension K de $\mathbf{Q}$, on obtient un anneau intégralement clos en prenant l'ensemble A des éléments de K entiers sur $\mathbf{Z}$. Dans le cas de $K = \mathbf{Q}(\sqrt{\Delta})$, cet anneau contient $\mathbf{Z}[\sqrt{\Delta}]$ en vertu du lemme précédent, mais en général il ne lui est pas égal. Précisément :

3. Dans le cas $\Delta < 0$ c'est aussi la conjugaison complexe.

4. Il s'agit de la norme au sens des arithméticiens. Dans le cas $\Delta < 0$ c'est le carré du module de z.

2.4 Théorème. *L'ensemble des éléments de* $\mathbf{Q}(\sqrt{\Delta})$ *entiers sur* $\mathbf{Z}$ *est noté* A_Δ *et on a :*

1) $A_\Delta = \mathbf{Z}[\sqrt{\Delta}]$ *si* $\Delta \equiv 2, 3 \pmod 4$,

2) $A_\Delta = \mathbf{Z}\big[\frac{1+\sqrt{\Delta}}{2}\big] = \big\{a+b\big(\frac{1+\sqrt{\Delta}}{2}\big) \ \mid \ a, b \in \mathbf{Z} \ \big\}$ *si* $\Delta \equiv 1 \pmod 4$.

2.5 *Remarques.* 1) le cas $\Delta \equiv 0 \pmod 4$ est exclu puisque Δ est sans facteur carré.

2) On a $\mathbf{Z}[\sqrt{\Delta}] \subset \mathbf{Z}\big[\frac{1+\sqrt{\Delta}}{2}\big]$. En effet, si l'on pose $\alpha = \frac{1+\sqrt{\Delta}}{2}$, on a $\sqrt{\Delta} = 2\alpha - 1$. Mais la réciproque est inexacte (par exemple pour $\Delta = -3$).

3) Si Δ est congru à 1 modulo 4 l'élément α est entier sur $\mathbf{Z}$. En effet, son équation minimale sur $\mathbf{Q}$ est $X^2 - X - \dfrac{\Delta - 1}{4} = 0$ et elle est à coefficients entiers. Plus généralement, on voit ainsi que les anneaux proposés sont bien entiers sur $\mathbf{Z}$.

2.3.2 Preuve de 2.4

Le théorème repose sur le lemme suivant :

2.6 Lemme. *Un élément* $z \in \mathbf{Q}(\sqrt{\Delta})$ *est entier sur* $\mathbf{Z}$ *si et seulement si* $\mathrm{Tr}\,(z)$ *et* $N(z)$ *sont entiers.*

Démonstration. Vu 2.3, il est clair que si la trace et la norme sont entières l'élément est entier sur $\mathbf{Z}$. Inversement, soit $z \in \mathbf{Q}(\sqrt{\Delta})$ entier sur $\mathbf{Z}$. S'il est dans $\mathbf{Q}$, comme $\mathbf{Z}$ est factoriel donc intégralement clos, il est dans $\mathbf{Z}$ et sa trace et sa norme aussi. Sinon, il est racine d'un polynôme unitaire $P(X)$ à coefficients entiers. Quitte à remplacer ce polynôme par un de ses facteurs irréductibles [5], on peut supposer P irréductible sur $\mathbf{Z}$, donc sur $\mathbf{Q}$. C'est donc le polynôme minimal de z, $X^2 - \mathrm{Tr}\, z\, X + N(z)$, et on en déduit que norme et trace sont des entiers.

Revenons au théorème. Soit $z = a + b\sqrt{\Delta} \in \mathbf{Q}(\sqrt{\Delta})$ un élément entier sur $\mathbf{Z}$. D'après le lemme, sa trace, $2a$, et sa norme, $a^2 - \Delta b^2$, sont entières. Il y a deux cas.

1) Si a est entier, Δb^2 aussi. On pose $b = \dfrac{r}{s}$ avec $r \in \mathbf{Z}$, $s \in \mathbf{N}$, $s \neq 0$ et r, s premiers entre eux. Comme Δb^2 est dans $\mathbf{Z}$, on voit que s^2 divise Δr^2 et, comme il est premier avec r^2, le lemme de Gauss montre qu'il divise Δ. Comme Δ a été supposé sans facteur carré c'est qu'on a $s = 1$. En définitive, a et b sont entiers et z est dans $\mathbf{Z}[\sqrt{\Delta}]$.

5. L'anneau $\mathbf{Z}[X]$ est factoriel.

2) Sinon, on a $2a \in \mathbf{Z}$, mais $a \notin \mathbf{Z}$, donc $a = \dfrac{a'}{2}$ avec $a' \in \mathbf{Z}$, impair. On pose encore $b = \dfrac{r}{s}$ comme ci-dessus et on a $N(z) = \dfrac{a'^2}{4} - \Delta\dfrac{r^2}{s^2} = n \in \mathbf{Z}$, soit encore $4s^2n = a'^2s^2 - 4\Delta r^2$. Comme 4 divise a'^2s^2 et que a' est impair, s est pair, $s = 2s'$ et l'équation devient $4s'^2n = a'^2s^2 - \Delta r^2$. On voit que s'^2 divise Δr^2 puis, par Gauss, qu'il divise Δ et cela impose $s' = 1$. Il reste $4n = a'^2 - \Delta r^2$. Comme s vaut 2 et qu'il est premier avec r, cela montre que r est impair, comme a', et leurs carrés sont congrus à 1 modulo 4. On en déduit qu'on a $\Delta \equiv 1 \pmod 4$.

Cela montre déjà que le deuxième cas ne peut se produire lorsque Δ est congru à 2 ou 3 modulo 4 et le théorème est prouvé dans ces deux cas. Si Δ est congru à 1, le calcul précédent montre que z s'écrit $z = \dfrac{a'}{2} + \dfrac{r}{2}\sqrt{\Delta}$ avec r et a' impairs, donc :

$$z = \frac{1+\sqrt{\Delta}}{2} + \frac{a'-1}{2} + \frac{r-1}{2}\sqrt{\Delta}$$

et, vu la remarque 2.5.2, il est dans $\mathbf{Z}\big[\dfrac{1+\sqrt{\Delta}}{2}\big]$.

2.4 Anneaux de Dedekind

Le fait que les anneaux d'entiers des corps de nombres sont des anneaux de Dedekind est général (voir [S] ou [ST]), mais, dans le cas des corps quadratiques, on peut prouver le résultat de manière élémentaire. Rappelons d'abord la définition :

2.7 Définition. *Soit A un anneau commutatif. On dit que c'est un anneau de Dedekind s'il vérifie les trois propriétés suivantes (voir* [DP] *Ch. II pour le sens des mots) :*

1) A est noethérien,

2) A est intégralement clos,

3) A est de dimension 1 *(i.e. tout idéal premier non nul est maximal).*

On a alors la proposition suivante :

2.8 Proposition. *L'anneau A_Δ est de Dedekind.*

Démonstration. 1) L'anneau A_Δ s'écrit comme le quotient de $\mathbf{Z}[X]$ obtenu en envoyant X soit sur $\sqrt{\Delta}$ soit sur $\dfrac{1+\sqrt{\Delta}}{2}$. Il est donc noethérien (cf. [DP] Ch. II, 2.5).

2) Que A_Δ soit intégralement clos résulte de la transitivité de l'intégralité : si x est entier sur un anneau B, lui-même entier sur A, x est entier sur A. En effet, on applique ce résultat avec $A = \mathbf{Z}$, $B = A_\Delta$ et $x \in \mathbf{Q}(\sqrt{\Delta})$.

Ici on peut prouver directement la propriété de transitivité, par exemple dans le cas $\Delta \equiv 2, 3 \pmod 4$, l'autre est analogue. On suppose que x est entier sur $A_\Delta = \mathbf{Z}[\sqrt{\Delta}]$. On a donc une équation :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

avec $a_i = \alpha_i + \beta_i\sqrt{\Delta} \in A_\Delta$. On en déduit :

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 + \sqrt{\Delta}(\beta_{n-1}x^{n-1} + \cdots + \beta_0) = 0$$

donc une équation de la forme $P(x) + \sqrt{\Delta}\,Q(x) = 0$ avec P, Q polynômes à coefficients entiers. On en déduit $P(x)^2 - \Delta Q(x)^2 = 0$, donc une équation intégrale sur $\mathbf{Z}$ de degré $2n$ vérifiée par x.

Pour le point 3), on a le lemme suivant :

2.9 Lemme. *Soient $A \subset B$ deux anneaux intègres avec B entier sur A.*
1) Si A est un corps il en est de même de B.
2) Si A est de dimension 1 il en est de même de B.

Comme $\mathbf{Z}$ est de dimension 1, ce lemme assure que A_Δ est bien de dimension 1.

Prouvons le lemme. Pour le point 1), soit $x \in B$, $x \neq 0$. Il vérifie une équation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ avec $a_i \in A$ et, quitte à simplifier par une puissance de x, on peut supposer $a_0 \neq 0$. Mais alors, on a $-x(x^{n-1} + \cdots + a_1)a_0^{-1} = 1$ et x est inversible dans B.

Pour 2) on considère un idéal premier $\mathfrak{P}$ non nul de B. Il s'agit de voir qu'il est maximal. Soit $x \in \mathfrak{P}$, $x \neq 0$. Il vérifie une équation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ avec $a_i \in A$ et, on peut supposer $a_0 \neq 0$. Cet élément est dans $A \cap \mathfrak{P}$ qui est un idéal premier, non nul puisque a_0 est non nul, donc un idéal maximal m de A. On a alors l'injection $A/m \subset B/\mathfrak{P}$ et $B/\mathfrak{P}$ est entier sur A/m par réduction des équations modulo $\mathfrak{P}$. Par le point 1) on en déduit que c'est un corps, donc que $\mathfrak{P}$ est maximal.

Dans le cas des anneaux de Dedekind, deux des notions étudiées ici coïncident :

2.10 Proposition. *Soit A un anneau de Dedekind. Alors A est principal si et seulement si il est factoriel.*

Démonstration. Supposons A factoriel. Montrons d'abord que les idéaux maximaux de A sont principaux. Soit m maximal et $x \in m$, non nul. On décompose x en produit de facteurs premiers $x = p_1 \cdots p_r$. Comme m est maximal donc premier, l'un des p_i est dans m. On a donc un élément p irréductible dans m, d'où l'inclusion $(0) \subset (p) \subset m$ et, comme A est factoriel, (p) est premier non nul, donc maximal puisque l'anneau est de dimension 1 et on a bien $m = (p)$.

Soit maintenant I un idéal quelconque. Comme A est noethérien, I est engendré par un nombre fini d'éléments $I = (x_1, \ldots, x_n)$. On montre par récurrence sur n que I est principal et il suffit pour cela de traiter le cas $I = (x, y)$. Comme A est factoriel, x, y ont un *pgcd*, soit d et on a $x = dx'$, $y = dy'$ (donc $(x, y) \subset (d)$) avec x', y' premiers entre eux. Cela implique que l'idéal (x', y') est égal à (1). Sinon, il est contenu dans un idéal maximal m, principal comme on l'a vu, et on a donc $(x', y') \subset (p)$, ce qui signifie que p divise x' et y' et c'est absurde. On a donc $(x', y') = (1)$ d'où une relation de Bézout $1 = \lambda x' + \mu y'$ et par suite $d = \lambda x + \mu y$. On voit que d est dans I qui est donc égal à (d) comme souhaité.

2.11 *Remarque.* Ce résultat va nous permettre d'oublier la propriété de factorialité dans ce qui suit.

3 Le cas des corps quadratiques imaginaires : notations, résultats et préliminaires

Nous allons donc étudier maintenant les corps quadratiques imaginaires, ceux qui correspondent à $\Delta < 0$. Un mot sur ce choix. D'abord, ce sont ceux qui nous seront utiles dans deux des problèmes évoqués ci-dessus : l'équation de Bachet $y^2 + d = t^3$ et la recherche des nombres de la forme $x^2 + dy^2$. Ensuite, et plus sérieusement, le cas imaginaire est notablement plus simple que le cas réel à cause des inversibles. En effet, on verra qu'il n'y a que très peu d'inversibles dans l'anneau des entiers du cas imaginaire (le plus souvent ± 1 seulement) alors que $\mathbf{Z}[\sqrt{\Delta}]$ en contient à profusion (une infinité) donnés par l'équation de Pell-Fermat $x^2 - \Delta y^2 = \pm 1$ lorsque Δ est positif. Enfin, le résultat concernant les anneaux principaux est connu dans le cas imaginaire, mais pas dans le cas réel.

3.1 Notations

On reprend les notations du paragraphe précédent, mais on suppose désormais $\Delta < 0$ et on pose $\Delta = -d$. On note $K_d = \mathbf{Q}(i\sqrt{d})$ le corps

quadratique associé et A_d l'anneau des entiers de K_d. On notera qu'on a $A_d = \mathbf{Z}[i\sqrt{d}]$ si $d \equiv 1, 2 \pmod 4$ et $A_d = \mathbf{Z}[\frac{1+i\sqrt{d}}{2}]$ si $d \equiv 3 \pmod 4$ (attention au renversement de congruence). On note α_d (voire α s'il n'y a pas d'ambiguïté) le nombre $\dfrac{1+i\sqrt{d}}{2}$.

3.1 *Remarque.* La remarque évidente suivante sera souvent utile : si un entier $n \in \mathbf{Z}$ divise $a + ib\sqrt{d}$ ou $a + b\alpha_d$ dans A_d, il divise a et b dans $\mathbf{Z}$.

3.2 Les résultats

Soit $d \in \mathbf{N}^*$ un entier sans facteur carré, $K_d = \mathbf{Q}(i\sqrt{d})$ et A_d l'anneau des entiers de K_d. On rappelle que c'est un anneau de Dedekind.

3.2 Théorème. *L'anneau A_d est euclidien si et seulement si on a $d = 1, 2, 3, 7, 11$.*

3.3 Théorème. *L'anneau A_d est principal si et seulement si on a $d = 1, 2, 3, 7, 11, 19, 43, 67$ ou 163.*

3.4 *Remarques.* 1) Les listes précédentes fournissent en particulier quatre exemples d'anneaux principaux non euclidiens.

2) On voit qu'il n'y a en tout que neuf anneaux principaux parmi l'infinité considérée : les travaux de Kümmer, Dedekind, etc. qui visent à étudier les anneaux de nombres qui ne sont pas factoriels sont donc vraiment nécessaires.

3.3 Normes, inversibles, irréductibles

On rappelle qu'on a posé $\alpha = \dfrac{1+i\sqrt{d}}{2}$.

3.3.1 Représentation des anneaux comme quotients

3.5 Proposition. *Soit d un entier positif sans facteur carré. On a $A_d \simeq \mathbf{Z}[X]/(X^2+d)$ si $d \equiv 1, 2 \pmod 4$ et $A_d \simeq \mathbf{Z}[X]/(X^2 - X + \dfrac{d+1}{4})$ si $d \equiv 3 \pmod 4$.*

Démonstration. On définit un homomorphisme d'anneaux Φ de $\mathbf{Z}[X]$ dans A_d en envoyant $\mathbf{Z}$ par l'inclusion et l'indéterminée X sur $i\sqrt{d}$ ou α. Il est clair que cet homomorphisme est surjectif. Si $P(X)$ est dans $\operatorname{Ker}\Phi$, on effectue la division euclidienne de P par le polynôme unitaire $B(X) := X^2 + d$ ou $B(X) := (X^2 - X + \dfrac{d+1}{4})$ dans $\mathbf{Z}[X]$. On obtient $P(X) = B(X)Q(X) + R(X)$

avec $R(X) = a+bX$, $a, b \in \mathbf{Z}$. Le polynôme R est nul en $i\sqrt{d}$ ou α et, comme ces nombres ne sont pas rationnels, il est identiquement nul. On a donc $\operatorname{Ker}\Phi = (B)$ et le résultat est une conséquence du théorème d'isomorphisme.

3.6 *Remarque.* Bien entendu, lorsque d est congru à 3 modulo 4, $(d+1)/4$ est un entier et le polynôme B est bien dans $\mathbf{Z}[X]$.

3.3.2 Étude de la norme

Notons d'abord les deux formules :

$$N(a+ib\sqrt{d}) = a^2+db^2 \quad \text{et} \quad N(a+b\alpha_d) = a^2+ab+\frac{d+1}{4}b^2.$$

3.7 Lemme. *Soit $z \in A_d$. Alors $N(z)$ est un entier ≥ 0 et il est nul si et seulement si z l'est.*

Démonstration. Dans tous les cas on a $N(z) = z\overline{z}$ où la conjugaison est prise au sens complexe. La norme est donc le carré du module de z, donc ≥ 0 et elle n'est nulle que si z l'est. Par ailleurs, on sait (voir 2.6) que $N(z)$ est dans $\mathbf{Z}$, donc dans $\mathbf{N}$.

3.8 Lemme. *On suppose $q \equiv 1, 2 \pmod 4$. Si z est dans $A_d - \mathbf{Z}$ on a $N(z) \geq d$ avec égalité si et seulement si $z = \pm i\sqrt{d}$.*

Démonstration. On écrit $z = a+ib\sqrt{d}$ avec $b \neq 0$. On a $N(z) = a^2+db^2 \geq db^2 \geq d$ et l'égalité n'a lieu que si a est nul et si $b = \pm 1$.

3.9 Lemme. *On suppose $q \equiv 3 \pmod 4$. Si z est dans $A_d - \mathbf{Z}$ on a $N(z) \geq \dfrac{d+1}{4}$ avec égalité si et seulement si $z = \pm\alpha$ ou $\pm\overline{\alpha} = \pm(1-\alpha)$.*

Démonstration. On écrit $z = a+b\alpha$ avec $b \neq 0$. On a $N(a+b\alpha_d) = a^2 + ab + \dfrac{d+1}{4}b^2 = \left(a+\dfrac{b}{2}\right)^2 + \dfrac{db^2}{4} \geq \dfrac{d}{4}$. Mais $N(z)$ étant un entier et $d \equiv -1 \pmod 4$, donc $d = 4k-1$, cela implique $N(z) \geq k = \dfrac{d+1}{4}$ qui est l'entier immédiatement supérieur. Si $|b|$ est ≥ 2, on a $N(z) \geq d > \dfrac{d+1}{4}$. Si $|b|$ est égal à 1, il reste à résoudre $\left|a+\dfrac{b}{2}\right| = \dfrac{1}{2}$. On distingue les cas $b = 1$ et $b = -1$ et l'on trouve dans le premier cas $a = 0$ ou -1 et dans le second $a = 0$ ou 1 d'où le résultat.

3.3.3 Les éléments inversibles

On note A^* l'ensemble des éléments inversibles de l'anneau A. On remarque que l'anneau $A_3 = \mathbf{Z}[\alpha_3]$ est aussi égal à $\mathbf{Z}[j]$ avec $j^3 = 1$.

3.10 Proposition. *1) On a* $A_1^* = \mathbf{Z}[i]^* = \{\pm 1, \pm i\}$.
2) On a $A_3^* = \mathbf{Z}[j]^* = \{\pm 1, \pm j, \pm j^2\}$.
3) Pour tout $d \neq 1, 3$ *on a* $A_d^* = \{\pm 1\}$.

Démonstration. On montre d'abord que z est inversible si et seulement si il est de norme 1. Si $N(z) = z\overline{z} = 1$, z est inversible d'inverse $\overline{z}$. Inversement, si z a pour inverse w, on a $zw = 1$, donc $N(zw) = N(z)N(w) = N(1) = 1$. Mais, comme $N(z)$ et $N(w)$ sont des entiers positifs, cela implique $N(z) = N(w) = 1$.

Il reste à résoudre $N(z) = 1$. Si z est entier, $N(z) = z^2$ est égal à 1 si et seulement si $z = \pm 1$. Si z n'est pas entier, on sait que le minimum de la norme est d dans le cas $\equiv 1, 2 \pmod 4$ et $\dfrac{d+1}{4}$ dans l'autre cas. On voit qu'il n'il a pas d'autre inversibles que ± 1 dans le premier cas si $d \geq 2$ et dans le second si $d \geq 7$. Il reste à examiner les cas $d = 1$ et $d = 3$ et le résultat vient des lemmes précédents. (Pour $n = 3$ on notera qu'on a $\alpha = -j^2$, $\overline{\alpha} = -j$, $-\alpha = j^2$ et $-\overline{\alpha} = j$.)

3.3.4 Les éléments irréductibles

3.11 Proposition. *Soit* $p \in \mathbf{N}$ *un nombre premier ordinaire. Alors,* p *est réductible dans* A_d *si et seulement si* p *est une norme (i.e.* $\exists z \in A_d$, $p = N(z)$*).*

Démonstration. Si p est une norme on a $p = N(z) = z\overline{z}$ et p est produit de deux éléments non inversibles (leur norme n'est pas 1), donc est réductible. Inversement, si p est réductible on a $p = zw$ avec $z, w \in A_d$, non inversibles, d'où $N(p) = p^2 = N(z)N(w)$. Mais comme p est premier et $N(z), N(w)$ entiers positifs et différents de 1, on a nécessairement $N(z) = N(w) = p$.

3.12 *Exemples.* 1) Si d est congru à 1 ou 2 modulo 4 et si p est premier dans $\mathbf{N}$ et $< d$, p est irréductible dans A_d. En effet, sinon p est une norme $p = N(z) = a^2 + db^2$. On voit que b est non nul et, en vertu de 3.8, p est $\geq d$ et c'est absurde. En particulier, 2 est irréductible pour $d > 2$.

2) Si d est congru à 3 modulo 4, et si p est premier et $< \dfrac{d+1}{4}$, p est irréductible dans A_d pour la même raison. En particulier 2 est irréductible pour $d > 7$.

3.4 Une première application : beaucoup des A_d sont non principaux

Rappelons qu'on note $\mathbf{F}_q$ le corps fini à q éléments. En particulier, si p est premier, on a $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Rappelons aussi, cf. [DP], que si k est un corps et P un polynôme non nul à coefficients dans k, l'anneau $k[X]/(P)$ est intègre (et un corps) si et seulement si P est irréductible sur k.

3.13 Proposition. *Pour $d \equiv 1, 2 \pmod 4$ et $d > 2$ l'anneau A_d n'est pas principal.*

Démonstration. En effet, on a vu ci-dessus que l'entier 2 est irréductible dans $A_d = \mathbf{Z}[i\sqrt{d}]$ pour $d > 2$. En vertu de 1.8, il suffit donc de montrer que l'idéal (2) n'est pas premier ou encore que l'anneau $A_d/(2)$ n'est pas intègre. Mais, comme on a l'isomorphisme $\mathbf{Z}[i\sqrt{d}] \simeq \mathbf{Z}[X]/(X^2 + d)$ on en déduit aussitôt [6] $\mathbf{Z}[i\sqrt{d}]/(2) \simeq \mathbf{Z}[X]/(X^2 + d, 2) \simeq \mathbf{F}_2[X]/(X^2 + d)$. Il reste donc à voir que $X^2 + d$ n'est pas irréductible sur $\mathbf{F}_2$. Mais, si d est pair on a $X^2 + d = X^2$ et si d est impair $X^2 + d = X^2 + 1 = (X + 1)^2$.

Une manière plus élémentaire de dire la même chose consiste à noter que, bien que 2 soit irréductible, il ne vérifie pas le lemme d'Euclide car il divise $d^2 + d = (d + i\sqrt{d})(d - i\sqrt{d})$ mais aucun des deux facteurs.

3.14 Proposition. *Pour $d \equiv -1 \pmod 8$ et $d > 7$ l'anneau A_d n'est pas principal.*

Démonstration. La démonstration est analogue en notant cette fois qu'on a $A_d/(2) \simeq \mathbf{F}_2[X]/(X^2 - X + \dfrac{d+1}{4})$. Si d est congru à -1 modulo 8, $(d+1)/4$ est pair et le polynôme devient $X^2 + X = X(X + 1)$ d'où le résultat. En revanche, si d est congru à 3 modulo 8, le polynôme est $X^2 + X + 1$ qui est irréductible sur $\mathbf{F}_2$ et on ne peut pas conclure.

Voici une dernière remarque qui permet d'éliminer les d non premiers :

3.15 Proposition. *Si d est un entier sans facteur carré, $d > 1$ et d non premier, l'anneau A_d n'est pas principal.*

Démonstration. On peut supposer $d \equiv 3 \pmod 4$ et $d \geq 15$ (les nombres $3, 7$ et 11 sont premiers). Si d n'est pas premier, il admet un facteur premier (impair) $p \leq \sqrt{d}$. Mais on a $\sqrt{d} < \dfrac{d+1}{4}$, c'est-à-dire $d - 4\sqrt{d} + 1 > 0$. En effet, la plus grande racine du trinôme $x^2 - 4x + 1$ est $2 + \sqrt{3} < \sqrt{15}$. Il en résulte que p est irréductible dans A_d. Pourtant, il n'est pas premier. En effet,

6. Le lecteur non convaincu ira lire l'annexe 7.

le quotient $A_d/(p)$ est isomorphe à $\mathbf{F}_p[X]/(X^2 - X + \frac{d+1}{4})$ et le discriminant $-d$ de ce polynôme est nul modulo p. (Si l'on préfère, p divise $(2\alpha-1)^2 = -d$ mais ne divise pas $2\alpha - 1$.)

3.16 Commentaire. Les résultats qui précèdent, bien que très simples, montrent déjà que plus des trois quarts des anneaux considérés sont non principaux.

4 Les anneaux euclidiens

Nous démontrons maintenant 3.2 en commençant par le côté négatif :

4.1 Proposition. *Pour $d \neq 1, 2, 3, 7, 11$, l'anneau A_d n'est pas euclidien.*

Démonstration. Si d e'st congru à 1 ou 2 modulo 4, on a vu en 3.13 que A_d n'est pas principal, sauf peut-être pour $d = 1$ ou $d = 2$. *A fortiori* il n'est donc pas euclidien.

Supposons donc $d \equiv 3 \pmod 4$ et même $d \equiv 3 \pmod 8$ en vertu de 3.14, et $d > 11$, donc ≥ 19. Rappelons le résultat suivant ([DP] Ch.II prop. 5.1) :

4.2 Proposition. *Soit A un anneau euclidien. Il existe $z \in A$, non inversible, tel que la restriction à $A^* \cup \{0\}$ de la projection $A \to A/(z)$ soit surjective.*

Dans le cas présent on a le lemme :

4.3 Lemme. *Soit d un entier sans facteur carré et $z \in A_d$ non nul. Le cardinal de $A_d/(z)$ est égal à $N(z)$.*

Forts de ce lemme nous pouvons finir de prouver 4.1. En effet, comme d est plus grand que 11, on a $A_d^* = \{1, -1\}$ en vertu de 3.10. Si l'anneau est euclidien on a un $z \in A_d$, non inversible, vérifiant la conclusion de 4.2. Le cardinal de $A_d/(z)$, qui n'est autre que $N(z)$, est donc ≤ 3. Mais, en vertu de 3.9, c'est impossible. En effet, si z est entier on a $N(z) = z^2$ et, comme z est $\neq \pm 1$ cette norme vaut au moins 4. Si z n'est pas entier, on a $N(z) \geq (d+1)/4 \geq 5$ et c'est absurde.

Il reste à prouver le lemme. Une façon très rapide de le faire consiste à noter que $A_d = \mathbf{Z}[\alpha]$ est un réseau de $\mathbf{C}$ et que $(z) = zA_d$ en est un sous-réseau. On sait alors (voir [ST]) que le groupe quotient a pour cardinal le rapport des aires de ces réseaux[7]. Mais, on passe de A_d à zA_d par la

7. C'est-à-dire des parallélogrammes bâtis sur les $\mathbf{Z}$-bases.

multiplication par $z \in \mathbf{C}$, qui est une similitude, produit d'une rotation et d'une homothétie de rapport $|z|$, qui multiplie les aires par $|z|^2 = N(z)$.

On peut d'ailleurs se passer de ce lemme pour établir 4.1. En effet, si A_d est euclidien, le quotient $A_d/(z)$ fourni par 4.2 est de cardinal ≤ 3 et c'est un corps (car ses éléments non nuls sont images d'inversibles, donc inversibles). C'est donc $\mathbf{F}_2$ ou $\mathbf{F}_3$. Cela implique que les éléments 2 ou 3 sont dans l'idéal (z), mais, comme ces éléments sont irréductibles, donc premiers, donc maximaux (voir 2.8) on a $(z) = (2)$ ou $(z) = (3)$. Mais alors, le quotient est égal à $\mathbf{F}_p[X]/(X^2 - X + (d+1)/4)$ (avec $p = 2$ ou 3) comme on l'a vu et cela implique que son cardinal est 4 ou 9 car c'est un $\mathbf{F}_p$-espace vectoriel de dimension 2, et c'est absurde.

Il reste à prouver le côté positif de 3.2 :

4.4 Proposition. *L'anneau A_d est euclidien pour $d = 1, 2, 3, 7, 11$.*

Démonstration. On va montrer que l'anneau est euclidien relativement à la norme, autrement dit : pour tous $z, w \in A_d - \{0\}$, il existe $q, r \in A_d$ tels que $z = qw + r$ et $N(r) < N(w)$.

Cela résulte d'un lemme d'approximation :

4.5 Lemme. *On suppose $d = 1, 2, 3, 7$ ou 11. Pour tout $z \in \mathbf{C}$ il existe $t \in A_d$ vérifiant $N(z - t) < 1$ (ou encore $|z - t| < 1$).*

Admettons un instant ce lemme. On l'applique à $z/w \in \mathbf{C}$. Il existe donc $q \in A_d$ avec $N(z/w - q) < 1$. On pose $r = z - qw = w(\frac{z}{w} - q)$. C'est un élément de A_d et on a $N(r) = N(w)N(z/w - q) < N(w)$ comme attendu.

La preuve du lemme est différente selon les congruences modulo 4.

1) Supposons $d = 1$ ou 2. On écrit $z = x + iy\sqrt{d}$ avec $x, y \in \mathbf{R}$. Soient $a, b \in \mathbf{Z}$, les entiers les plus proches de x et y respectivement. On a donc $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$. Posons $t = a + ib\sqrt{d} \in A_d$. On a alors $N(z - t) = (x - a)^2 + d(y - b)^2 \leq \dfrac{1 + d}{4}$ et comme d est ≤ 2, cette quantité est bien plus petite que 1.

2) Supposons $d = 3, 7$ ou 11. On écrit $z = x + y\alpha$ avec $x, y \in \mathbf{R}$ et on cherche $t = a + b\alpha$ avec $a, b \in \mathbf{Z}$. On a donc :

$$N(z - t) = (x - a + \frac{y - b}{2})^2 + d\frac{(y - b)^2}{4}.$$

On choisit b tel que $|y - b| \leq 1/2$, puis a tel que $|x + \dfrac{y - b}{2} - a| \leq 1/2$. Alors, on a $N(z) \leq \dfrac{1}{4} + \dfrac{d}{16} \leq \dfrac{d + 4}{16} \leq \dfrac{11 + 4}{16} = \dfrac{15}{16} < 1$.

5 Les anneaux principaux

5.1 Ceux qui ne le sont pas

Nous abordons ici le théorème 3.3 dans le sens négatif. Il s'agit de montrer qu'il n'y a pas d'autres anneaux principaux parmi les A_d que les neuf annoncés. En fait, ce résultat, dans le langage de la classification des formes quadratiques binaires, a été conjecturé par Gauss (on parlait du problème du dixième discriminant) et il n'a été obtenu qu'en 1967 par Stark [8]. Le niveau de cet article dépassant largement celui d'un TER, nous nous contenterons de le démontrer en bornant l'entier d par 200. Le lecteur n'aura pas grand-peine à étendre ce résultat pour $d \leq 10000$ voire plus s'il a du courage.

5.1 Proposition. *Pour $d < 200$ et $d \neq 1, 2, 3, 7, 11, 19, 43, 67$ et 163, l'anneau A_d n'est pas principal.*

Démonstration. On peut se limiter aux entiers $d > 7$ et congrus à 3 modulo 8, en éliminant ceux qui ont un facteur carré. Il reste les entiers suivants : $19, 35, 43, 51, 59, 67, 83, 91, 107, 115, 123, 131, 139, 147, 155, 163, 179, 187$ et 195.

Le principe de la preuve est le suivant. On sait (voir 3.12) que si p est un nombre premier $< \dfrac{d+1}{4}$, il est encore irréductible dans A_d. Si l'idéal (p) de A_d n'est pas premier cela montre que A_d n'est pas principal. Or, on a vu que le quotient $A_d/(p)$ n'est autre que $\mathbf{F}_p[X]/(X^2 - X + \dfrac{d+1}{4})$ et, pour $p > 2$, il s'agit de montrer que ce polynôme est réductible sur $\mathbf{F}_p$, ou encore que son discriminant, qui vaut $-d$, est un carré de $\mathbf{F}_p$.

On applique ceci avec les p suivants :

1) $p = 3$ est irréductible pour $d > 11$ et $-d$ est un carré de $\mathbf{F}_3$ si et seulement si d est congru à 0 ou 2 modulo 3. On peut donc rayer dans notre liste les d admettant ces congruences, c'est-à-dire $35, 51, 59, 83, 107, 123, 131, 147, 155$, 179 et 195.

2) $p = 5$ est irréductible pour $d > 19$ et $-d$ est un carré modulo 5 si et seulement si d est congru à 0, 1 ou -1 modulo 5. On peut donc éliminer les d admettant ces congruences, donc, parmi ceux qui restent, 91, 115 et 139.

3) $p = 7$ est irréductible pour $d > 27$, ce qui permet d'éliminer le dernier entier réfractaire, à savoir $d = 187$, qui est congru à -2 modulo 7, donc tel que $-d \equiv 2 \equiv 9$ est un carré.

5.2 *Remarque.* Il ne reste donc que les quatre entiers $19, 43, 67$ et 163 dont on verra qu'ils donnent des anneaux principaux. Il sera utile pour cela de se

8. *A complete determination of the complex quadratic fields of class-numer one*, Michigan Math. J. 14 (1967), pp. 1-27.

souvenir que l'idéal (p), pour $p = 2$ (resp. $2, 3$, resp. $2, 3, 5$, resp. $2, 3, 5, 7$) est premier dans A_d pour $d = 19$ (resp. 43, resp. 67, resp. 163).

5.3 *Exercice.* Montrer que A_d avec $d = 93307$ n'est pas principal. Indication : il s'agit de trouver un entier p premier $< (d+1)/4$ tel que $-d$ soit un carré modulo p. Il faut en essayer quelques-uns ...

5.2 Les principaux non euclidiens

Il reste à prouver le sens positif de 3.3 :

5.4 Proposition. *Pour $d = 1, 2, 3, 7, 11, 19, 43, 67$ et 163, l'anneau A_d est principal.*

Vu 4.4, il reste à prouver :

5.5 Corollaire. *Pour $d = 19, 43, 67$ et 163, l'anneau A_d est principal (et non euclidien).*

5.2.1 Le principe

On suppose que d est l'un des quatre entiers ci-dessus. En vertu de 2.10 il suffit de montrer que l'anneau est factoriel. Le ressort de la preuve est le lemme 1.8. Il s'agit de montrer que si $z \in A_d$ est irréductible, l'idéal zA_d est premier. Pour cela il faut commencer par déterminer les irréductibles. En vertu de 3.11, il y a déjà les nombres premiers $p \in \mathbf{N}$ qui ne sont pas des normes. Il faudra donc montrer, en tous cas :

5.6 Proposition. (Condition (H)) *On suppose $d = 19, 43, 67$ ou 163. Si p est premier dans $\mathbf{N}$ et n'est pas une norme de A_d, l'idéal pA_d est premier.*

En fait, cette condition suffit à assurer la factorialité. En effet, on peut alors préciser quels sont les autres irréductibles de A_d et voir qu'ils ne posent pas de problème :

5.7 Proposition. *On suppose la condition (H) réalisée. Alors, les irréductibles de A_d sont, au signe près :*

- *les $p \in \mathbf{N}$, premiers, qui ne sont pas des normes dans A_d,*
- *les $z \in A_d$ dont la norme est un nombre premier de $\mathbf{N}$.*

Dans les deux cas, les idéaux engendrés par ces éléments sont premiers.

Démonstration. Montrons d'abord la dernière assertion. Le cas d'un nombre premier qui n'est pas une norme vient de (H). Soit $z \in A_d$ tel que $N(z) = p$, premier. On a vu en 4.3 que le cardinal de $A_d/(z)$ est égal à $N(z)$, donc à p.

Mais alors, ce quotient n'est autre que $\mathbf{Z}/p\mathbf{Z}$ (il n'y a qu'un seul anneau de cardinal p premier comme on le voit en considérant l'homomorphisme naturel de $\mathbf{Z}$ dans cet anneau) et c'est un corps, ce qui assure que (z) est maximal donc premier.

Passons à la description des irréductibles. Soit z un irréductible de A_d et p un facteur premier de $N(z)$. Il y a deux cas :

• Si p est irréductible dans A_d, l'hypothèse (H) assure que l'idéal pA_d est premier. Comme p divise $N(z) = z\overline{z}$ il divise z ou $\overline{z}$, donc z puisque p est entier. Mais, comme z est irréductible, c'est que z et p sont associés [9] donc $z = \pm p$.

• Sinon, c'est que p est une norme de A_d, $p = N(w)$. Mais alors, on a vu que l'idéal (w) est premier. Comme w divise $z\overline{z}$, il divise z ou $\overline{z}$. Comme ces éléments sont irréductibles, z ou $\overline{z}$ est associé à w et il a donc même norme, égale à p.

Il reste donc à prouver la condition (H). On commence par formuler sa contraposée :

5.8 Proposition. (Condition (H^*)) *On suppose $d = 19, 43, 67$ ou 163. Soit p un nombre premier de $\mathbf{N}$. Si l'anneau A_d/pA_d n'est pas intègre (c'est-à-dire si pA_d n'est pas premier) p est une norme de A_d.*

5.2.2 La ligne de la preuve de (H^*)

La preuve de la proposition 5.8 se fait en plusieurs temps. Commençons par formuler la condition "A_d/pA_d n'est pas intègre" :

5.9 Proposition. *Soit p un nombre premier impair. Dire que A_d/pA_d n'est pas intègre c'est dire qu'il existe $z \in A_d$, $z \notin \mathbf{Z}$, tel que $N(z) = \lambda p$ avec $\lambda \in \mathbf{N}^*$. Plus précisément, on peut supposer $z = -u + \alpha$ avec $|u| \leq \dfrac{p-1}{2}$.*

Démonstration. On a vu que l'anneau A_d/pA_d est isomorphe à $\mathbf{F}_p[X]/(X^2 - X + \dfrac{d+1}{4})$. Dire que cet anneau n'est pas intègre c'est dire que le polynôme admet une racine $\overline{u} \in \mathbf{F}_p$, autrement dit qu'on a $u^2 - u + \dfrac{d+1}{4} = \lambda p$ avec $\lambda, u \in \mathbf{Z}$ ou encore $\lambda p = N(-u + \alpha)$. En prenant u positif ou négatif on peut supposer $|u| \leq p/2$, c'est-à-dire, comme p est impair, $|u| \leq \dfrac{p-1}{2}$.

9. i.e. $z = pu$ avec u inversible.

On voit que l'hypothèse assure que λp est une norme, ce qui est la condition (H^*) "à un facteur près". Toute la difficulté est de contrôler la taille de ce facteur :

5.10 Proposition. *On suppose $d = 19, 43, 67$ ou 163. On introduit deux constantes $M_d = \dfrac{2\sqrt{d}}{\pi} \simeq 0,636\sqrt{d}$ et $T_d = \sqrt{\dfrac{d}{3}} \simeq 0,577\sqrt{d}$. Soit p un nombre premier de $\mathbf{N}$. Si l'anneau A_d/pA_d n'est pas intègre il existe $k \in \mathbf{N}$ avec $1 \leq k \leq M_d$ ou $1 \leq k \leq T_d$ tel que kp est une norme de A_d.*

Cette proposition est le cœur de la preuve du théorème. Nous la démontrerons par deux méthodes qui mènent aux deux constantes M_d et T_d (d'ailleurs assez voisines comme on l'a vu). La première utilise les réseaux et le théorème de Minkowski, la seconde le principe des tiroirs, à la manière de Dirichlet.

L'autre ingrédient de la preuve a déjà été vu :

5.11 Proposition. *On suppose $d = 19, 43, 67$ ou 163. Pour tout nombre premier q de $\mathbf{N}$ avec $1 \leq q \leq M_d$ ou T_d, l'anneau A_d/qA_d est intègre.*

Démonstration. Pour $d = 19, 43, 67, 163$, les q à tester sont respectivement 2 ; $2, 3$; $2, 3, 5$; $2, 3, 5, 7$ et le travail a été fait en 5.2.

5.2.3 Fin de la preuve de (H^*)

Faisons la preuve avec la constante M_d pour fixer les idées, l'autre cas est identique.

Comme l'anneau A_d/pA_d n'est pas intègre, c'est que p est $> M_d$ en vertu de 5.11. En vertu de 5.10 il existe $k \leq M_d$ tel que kp est une norme. On choisit le plus petit k ainsi et on a donc $kp = z\overline{z}$. Si k n'est pas égal à 1 on en prend un facteur premier q qui est plus petit que M_d, donc vérifie le lemme d'Euclide en vertu de 5.11. Le nombre entier q divise donc z ou $\overline{z}$, donc z, et on a $z = qw$. Si on pose $k = qk'$, on a $k'p = qw\overline{w} = qN(w)$ dans $\mathbf{N}$. Comme q ne divise pas p (ils sont premiers et l'un est plus petit que M_d et l'autre plus grand), c'est que q divise k', $k' = qk''$. Mais alors, on a $k''p = N(w)$ avec $k'' < k$ ce qui contredit le fait que k était minimal pour cette propriété.

5.2.4 Preuve numéro 1 de 5.10 : *via* Minkowski

Comme A_d/pA_d n'est pas intègre, on a vu en 5.9 qu'il existe $z \in A_d$, $z = -u + \alpha$, tel que $N(z) = \lambda p$ avec $\lambda \in \mathbf{N}^*$. On voit qu'il y a dans le réseau A_d des z dont la norme est multiple de p et on va en chercher un plus petit. Il y a une technique pour cela qui est d'utiliser le théorème de Minkowski (voir ci-dessous). Mais ce théorème s'applique à un sous-réseau et la difficulté ici

est que l'ensemble des z de norme multiple de p n'est pas un sous-réseau [10] de A_d. C'est pourquoi on considère la partie :

$$L = \{a + b\alpha \in A_d \ \mid \ a, b \in \mathbf{Z} \text{ avec } a + bu \equiv 0 \pmod{p} \}.$$

On vérifie sans peine que L est un sous-réseau de base $-u + \alpha, p$ et que les éléments de L sont tous de norme multiple de p.

Pour obtenir des éléments de L de petite norme, on utilise le théorème de Minkowski (voir [S] ou [ST]) :

5.12 Théorème. *Soit L un sous-réseau de rang 2 de $\mathbf{Z}^2$ et soit $\mathcal{A}(L)$ son aire. Soit $B(O, R)$ le disque euclidien de centre l'origine et de rayon R. On suppose qu'on a $\pi R^2 \geq 4\mathcal{A}(L)$. Alors $B(O, R)$ contient un point $z \in L$ non nul.*

L'aire du réseau, c'est-à-dire l'aire d'un parallélogramme bâti sur une base du réseau, n'est autre que la valeur absolue du déterminant des vecteurs de base sur la base canonique, soit $\begin{vmatrix} -u + \frac{1}{2} & \frac{\sqrt{d}}{2} \\ p & 0 \end{vmatrix}$. On a donc $\mathcal{A}(L) = p\sqrt{d}/2$. Il y a donc un point non nul z du réseau L dans le disque de rayon R tel que $R^2 = 2p\sqrt{d}/\pi$ et, comme sa norme est multiple de p, on a $|z|^2 = N(z) = kp$ avec $k \leq 2\sqrt{d}/\pi$: c'est ce qu'on voulait.

5.2.5 Preuve numéro 2 de 5.10 : *via* Dirichlet

Le ressort de cette preuve est le fameux **principe des tiroirs** : si l'on a plus de chaussettes que de tiroirs, l'un des tiroirs contient au moins deux chaussettes. Cette remarque évidente a été utilisée notamment par Dirichlet avec une efficacité extraordinaire. C'est le ressort du lemme d'approximation des réels suivant :

5.13 Lemme. *Soit $v \in \mathbf{R}$ (resp. $v \notin \mathbf{Q}$) et soit $l \in \mathbf{N}^*$. Il existe $k \in \mathbf{N}$ avec $1 \leq k \leq l - 1$ et $n \in \mathbf{Z}$ tels que l'on ait $|kv - n| \leq \dfrac{1}{l}$ (resp. $<$).*

Démonstration. On note $[x]$ la partie entière de x. On considère les $l + 1$ nombres de $[0, 1]$: 0, $v - [v]$, $2v - [2v]$, $\ldots$, $(l-1)v - [(l-1)v]$, 1. On les ordonne : $0 = v_0 \leq v_1 \leq \cdots \leq v_l = 1$, ce sont les chaussettes. On considère ensuite les l tiroirs $[\dfrac{i}{l}, \dfrac{i+1}{l}]$ pour i variant de 0 à $l - 1$. Si les chaussettes sont toutes distinctes c'est que deux sont dans le même tiroir et

10. Par exemple, pour $d = 19$ et $p = 61$, $7 + \alpha$ et $-8 + \alpha$ sont tous deux de normes multiples de 61, mais pas leur somme ou leur différence.

si deux sont égales c'est encore plus vrai. Il y a trois cas. Si une chaussette $av - [av]$ autre que 0 est dans le premier tiroir on a $|av - [av]| \leq 1/l$ et le résultat est acquis. Si une chaussette $av - [av]$ autre que 1 est dans le dernier tiroir on a $|av - [av] - 1| \leq 1/l$ et ce qu'on veut. Enfin, si deux chaussettes distinctes $av - [av]$ et $bv - [bv]$ avec $a < b$ sont dans un même tiroir on a $|(b-a)v - [bv] + [av]| \leq 1/l$ et on a fini.

Si v est irrationnel, l'inégalité est nécessairement stricte.

Le lemme précédent donne un lemme d'approximation dans le corps quadratique K_d :

5.14 Lemme. *Soit d un entier positif sans facteur carré congru à -1 modulo 4 et soient K_d et A_d comme ci-dessus. Soit $l \in \mathbf{N}^*$ vérifiant $l > \sqrt{\frac{d}{3}}$. Alors, si x est dans K_d, il existe $k \in \mathbf{N}^*$, avec $1 \leq k \leq l-1$, et $q \in A_d$ tels que l'on ait $N(kx - q) < 1$ (ou encore $|kx - q| < 1$).*

Démonstration. On écrit x sous la forme $x = u + v\alpha$ avec $u, v \in \mathbf{Q}$ et $\alpha = \frac{1 + i\sqrt{d}}{2}$. On a $kx = ku + kv\alpha = ku + \frac{kv}{2} + \frac{kvi\sqrt{d}}{2}$. On applique 5.13 à v. Il existe donc $k \in \mathbf{N}$, avec $1 \leq k \leq l-1$, et $n \in \mathbf{Z}$ tel que $|kv - n| \leq 1/l$. On choisit un entier m tel que $|ku + \frac{kv}{2} - \frac{n}{2} - m| \leq \frac{1}{2}$ et on pose $q = m + n\alpha \in A_d$. On en déduit :

$$N(kx - q) = |ku + \frac{kv}{2} - \frac{n}{2} - m|^2 + \frac{|kv - n|^2 d}{4} \leq \frac{1}{4} + \frac{d}{4l^2} = \frac{d + l^2}{4l^2} < 1$$

puisqu'on a $l > \sqrt{\frac{d}{3}}$ donc $3l^2 > d$.

Enfin, le lemme d'approximation permet de montrer l'existence d'une pseudo-division euclidienne dans A_d :

5.15 Lemme. *On reprend les notations de 5.14, avec $l > \sqrt{\frac{d}{3}}$. Soient $z, w \in A_d$, avec $w \neq 0$. Il existe $k \in \mathbf{N}$ avec $1 \leq k \leq l-1$ et $q, r \in A_d$ tels que l'on ait $kz = qw + r$ et $N(r) < N(w)$.*

Démonstration. On applique 5.14 à $x = z/w \in K_d$. On obtient k et q tels que $N(kx - q) < 1$, donc $N(kz - qw) < N(w)$ et il suffit de poser $r = kz - qw$.

Fin de la preuve de 5.10

La pseudo-division permet de prouver 5.10. On suppose que l'idéal pA_d n'est pas premier. On a vu en 5.9 que cela implique qu'il existe $z = -u + \alpha \in A_d$, avec $|u| \leq (p-1)/2$, tel que $N(z) = \lambda p$. En vertu de 5.11, p est plus grand

que $T_d = \sqrt{\frac{d}{3}}$. On a donc $3p^2 > d$ et cela implique que λ est $< p$. En effet, on a $N(-u+\alpha) = u^2 - u + \frac{d+1}{4} \leq \frac{(p-1)^2}{4} + \frac{p-1}{2} + \frac{d+1}{4} = \frac{p^2+d}{4} < p^2$. On choisit alors un z vérifiant $N(z) = \lambda p \neq 0$ tel que λ soit minimum. Si λ est $\leq T_d$ on a fini. Sinon, on effectue la pseudo-division euclidienne de p par z. Il existe k avec $1 \leq k \leq T_d$ tel que $kp = bz + r$ avec $N(r) < N(z)$. On vérifie aussitôt que $N(r)$ est multiple de p et, comme z a été choisi minimum, cela impose que r est nul. On a donc $kp = bz$, d'où $k^2p^2 = N(b)N(z) = N(b)\lambda p$, donc $\lambda N(b) = k^2 p$. Comme on a $\lambda < p$, p est premier avec λ, donc divise $N(b)$. On a ainsi $N(b) = \mu p$ avec $\lambda\mu = k^2$, mais comme on a $k \leq T_d < \lambda$, c'est que μ est $< k$ et on a le résultat voulu.

5.16 *Exercice.* **(Preuve directe de la principalité)**

On se propose de montrer directement que A_d est principal pour $d = 19, 43, 67$ et 163 à partir de la pseudo-division euclidienne. Soit I un idéal non nul de A_d et soit a un élément non nul de I, de norme minimale. On va montrer par l'absurde qu'on a $I = (a)$. Sinon, soit $x \in I - (a)$.

1) En effectuant la pseudo-division de x par a, montrer qu'on a $kx = aq$ avec $1 \leq k \leq l - 1$.

2) On choisit un tel x de sorte que k soit minimal.

a) Montrer que k est > 1.

b) Soit p un facteur premier de k. Montrer que l'idéal pA_d maximal.

c) Montrer que q n'est pas dans pA_d et en déduire qu'on a une relation de Bézout $1 = \lambda p + \mu q$.

d) Montrer que a est dans pA_d, $a = pa'$, en déduire que a' est dans I et conclure.

5.3 Une application : une belle série de nombres premiers

Il n'y a pas de formule donnant à coup sûr des nombres premiers, mais la suivante n'est pas si mal :

5.17 Proposition. *Pour $n = 0, 1, \ldots, 39$, n^2+n+41 est un nombre premier.*

Démonstration. On peut évidemment vérifier ce résultat à la main, mais on ne comprend pas sa provenance, alors que la preuve suivante la révèle.

L'idée principale c'est que $q_n = n^2 + n + 41$ n'est autre que $N(n + \alpha)$ où $\alpha = \frac{1 + i\sqrt{d}}{2}$ avec $d = 163$. En effet, on a $\frac{d+1}{4} = 41$. Supposons q_n non premier. Il admet donc un diviseur premier $p < \sqrt{q}_n$ (c'est le principe du

crible d'Ératosthène). On a donc $p^2 < n^2 + n + 41 < 40^2 + 40 + 41 = 41^2$, donc $p < 41$. Il en résulte que p est irréductible dans A_{163}. En effet, en vertu de 3.9, ce n'est pas une norme. Comme on a $N(n+\alpha) = (n+\alpha)(n+\overline{\alpha})$, et comme A_{163} est principal, le lemme d'Euclide montre que p divise $n+\alpha$ ou $n+\overline{\alpha}$ dans A_{163}. Mais c'est impossible car p diviserait (dans $\mathbf{Z}$) le coefficient de α, qui vaut 1.

5.18 *Remarque.* On a des formules analogues, mais un peu moins belles, avec les nombres x^2+x+5, x^2+x+11 et x^2+x+17 qui correspondent aux cas $d = 19, 43, 67$.

6 Les entiers de la forme $x^2 + 5y^2$

6.1 Introduction

Lorsqu'on cherche les entiers qui sont sommes de deux carrés, la réponse est assez simple, voir [DP] Ch. II §6. On peut voir ces nombres comme les normes des éléments de l'anneau $\mathbf{Z}[i]$ ce qui montre déjà que leur ensemble est stable par multiplication. Cela conduit à examiner d'abord le cas des nombres premiers. Il y en a deux sortes, les bons qui sont sommes de deux carrés et les mauvais qui ne le sont pas. Les bons sont le nombre 2 et les nombres premiers congrus à 1 modulo 4 et les mauvais les nombres premiers congrus à 3 modulo 4. Ensuite, un entier n quelconque est somme de deux carrés si et seulement si les mauvais nombres premiers n'interviennent que par leurs carrés dans sa décomposition, donc sont élevés à une puissance paire.

Nous allons voir que pour les nombres de la forme x^2+5y^2 les choses sont un peu plus compliquées. La raison en est que, contrairement à l'anneau $\mathbf{Z}[i]$ utilisé dans le cas des deux carrés, l'anneau pertinent ici est $\mathbf{Z}[i\sqrt{5}]$ dont on a vu qu'il n'est pas factoriel. L'objectif de ce paragraphe est de montrer qu'on peut néanmoins l'utiliser pour faire de l'arithmétique.

6.2 Des conditions nécessaires

On note Σ_5 l'ensemble des nombres entiers de la forme x^2+5y^2 avec x, y entiers. Une première remarque est évidente, mais essentielle :

6.1 Proposition. *L'ensemble Σ_5 est l'ensemble des normes de l'anneau $A_5 = \mathbf{Z}[i\sqrt{5}]$. Il est stable par multiplication.*

Démonstration. En effet, si $z = x + iy\sqrt{5}$ est dans A_5, on a $N(z) = x^2+5y^2$ et la stabilité vient de la formule $N(zw) = N(z)N(w)$.

On a ensuite deux conditions nécessaires portant sur les nombres premiers :

6.2 Proposition-Définition. *Soit P l'ensemble des nombres premiers de* $\mathbf{N}$. *On pose :*

$$P_1 = \{p \in P \mid p \equiv \pm 1 \pmod 5 \text{ et } p \equiv 1 \pmod 4\} \cup \{5\},$$

$$P_2 = \{p \in P \mid p \equiv \pm 2 \pmod 5 \text{ et } p \equiv -1 \pmod 4\} \cup \{2\},$$

et $P_3 = P - P_1 - P_2$. Alors on a les conditions suivantes :

0) Si un nombre entier est dans Σ_5 il est congru à $0, 1$ ou -1 modulo 5.

1) Si un nombre premier p est dans Σ_5, il est dans P_1.

2) Si un nombre premier p divise un élément $n \in \Sigma_5$ et que p^2 ne divise pas n, p est dans $P_1 \cup P_2$.

Démonstration. 0) On a $n = x^2 + 5y^2$ de sorte que n est un carré modulo 5, donc congru à $0, 1$ ou -1.

1) On note que 2 n'est pas de la forme $x^2 + 5y^2$ et on peut donc supposer p impair. Si l'on a $p = x^2 + 5y^2$, le point 0) montre que p est égal à 5 ou congru à ± 1 modulo 5. Il est aussi somme de deux carrés modulo 4, ce qui implique qu'il est congru à $0, 1$ ou 2, donc à 1 puisqu'il est impair.

2) Notons que le nombre 2 est dans P_2, de sorte qu'on peut supposer p impair. Si p divise $n = x^2+5y^2$ on a $x^2+5y^2 \equiv 0 \pmod p$. Le nombre y n'est pas multiple de p, sinon x le serait aussi et p^2 diviserait n. Il en résulte que que $-5 \equiv x^2/y^2$ est un carré de $\mathbf{F}_p$. Vu [DP] Ch. III, cela implique soit que -1 et 5 sont tous deux des carrés modulo p, soit qu'ils sont tous deux non carrés. On sait que -1 est un carré modulo p si et seulement p est congru à 1 modulo 4. En vertu de la loi de réciprocité quadratique [11] (voir [Serre]), 5 est un carré modulo p si et seulement si p est un carré modulo 5, donc congru à $0, 1, -1$ et on a le résultat.

Nous donnons ici une preuve directe de la loi de réciprocité quadratique dans le cas considéré :

6.3 Proposition. *Soit p un nombre premier différent de 2 et 5. Le nombre 5 est un carré modulo p si et seulement si p est un carré modulo 5.*

Démonstration. On considère le corps $K = \mathbf{F}_p$ et ses extensions $L = \mathbf{F}_{p^2}$ et $M = \mathbf{F}_{p^4}$. Le corps M contient une racine primitive cinquième de l'unité ζ. En effet, M^* est de cardinal $p^4 - 1$, qui est multiple de 5 (c'est le petit théorème de Fermat, évident ici), donc il contient un élément d'ordre 5. On a donc

11. Voir en 6.3 ci-dessous une preuve directe du résultat dans le cas particulier envisagé.

$\zeta^5-1=0=(\zeta-1)(\zeta^4+\zeta^3+\zeta^2+\zeta+1)$ et comme ζ est primitive, elle est racine du polynôme (cyclotomique) de degré 4. On pose $\beta=\zeta+\zeta^{-1}$. En divisant le polynôme cyclotomique par ζ^2, on obtient $\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2}=0$, soit $\beta^2+\beta-1=0$. Mais alors, le nombre [12] $\alpha=2\beta+1$ vérifie $\alpha^2=4\beta^2+4\beta+1=4+1=5$.

On peut maintenant conclure :

• Supposons que 5 est un carré de $\mathbf{F}_p$. Cela signifie que $\sqrt{5}=2\beta+1$ est dans $\mathbf{F}_p$. Mais ζ, qui vérifie $\zeta^2-\beta\zeta+1=0$, est alors de degré 2 sur $\mathbf{F}_p$, donc est dans $\mathbf{F}_{p^2}$. Il en résulte que $\mathbf{F}_{p^2}^*$ contient un élément d'ordre 5, donc que 5 divise p^2-1, donc $p\equiv\pm1 \pmod 5$ est un carré modulo 5.

• Inversement, supposons que p soit congru à ±1 modulo 5. On calcule, dans M, $\beta^p=\zeta^p+\zeta^{-p}$ (on est en caractéristique p) et, que p soit congru à 1 ou à -1 modulo 5, comme ζ^5 est égal à 1, on a $\beta^p=\beta$. Mais, cela signifie que β est dans $\mathbf{F}_p$ (ses éléments sont exactement les x vérifiant $x^p=x$), donc aussi $\sqrt{5}=2\beta+1$ et 5 est un carré modulo p.

6.3 Le théorème

6.4 Théorème. *Soit n un nombre entier positif. On note $n=\prod_{p\in P}p^{v_p(n)}$ la décomposition en produit de facteurs premiers de n. Alors, n est dans Σ_5 si et seulement si :*

1) pour tout $p\in P_3$, $v_p(n)$ est pair,

2) la somme $\sum_{p\in P_2}v_p(n)$ est paire.

6.5 *Remarque.* Il y a donc trois sortes de nombres premiers par rapport au problème considéré :

1) Les bons, qui sont dans P_1. Ils sont dans Σ_5 et on peut en mettre autant qu'on en veut dans un entier n de Σ_5. C'est le cas par exemple de $29=9+5\times4$ ou $41=36+5\times1$, etc.

2) Les moyens, qui sont dans P_2. Eux ne sont pas dans Σ_5, mais si l'on en met deux ensemble ils y sont. C'est le cas des nombres 2, 3, 7, 23, 43, etc. et on a $2\times3=6=1+5\times1$, $2\times7=14=9+5\times1$, $2\times23=46=1+5\times9$, $3\times7=21=1+5\times4$, etc.

3) Les mauvais qui sont dans P_3. Ils ne sont tolérés dans un nombre de Σ_5 que s'ils sont au carré. C'est le cas de 11, 13, 17, etc.

Démonstration. (de 6.4) Comme dans la preuve de la principalité des anneaux vue ci-dessus, il y a deux voies, celle de Minkowski et celle de Di-

12. Que l'on trouve en résolvant l'équation du second degré ...

richlet. Utilisons par exemple cette dernière. Elle repose sur un lemme de pseudo-division analogue à 5.15 que le lecteur établira sans peine :

6.6 Lemme. *Soit d un entier positif sans facteur carré congru à 1 ou 2 modulo 4 et soient K_d et A_d définis comme en 3.1. Soit $l \in \mathbf{N}^*$ vérifiant $l > 2\sqrt{\frac{d}{3}}$. Soient $a, b \in A_d$, avec $b \neq 0$. Il existe $k \in \mathbf{N}$ avec $1 \leq k \leq l-1$ et $q, r \in A_d$ tels que l'on ait $ka = bq + r$ et $N(r) < N(b)$.*

Ce lemme permet de montrer la proposition suivante (pour $d = 5$, le nombre k ci-dessus vaut 1 ou 2) :

6.7 Proposition. *Soit p un nombre premier.*

1) L'idéal $(p) \subset \mathbf{Z}[i\sqrt{5}]$ est premier si et seulement si p est dans P_3.

2) Le nombre p est dans P_1 si et seulement si il est dans Σ_5 (et dans ce cas $2p$ n'est pas dans Σ_5).

3) Le nombre p est dans P_2 si et seulement si $2p$ est dans Σ_5 (et dans ce cas p n'est pas dans Σ_5). De plus, si p et q sont dans P_2 leur produit est dans Σ_5.

Démonstration. Le nombre 2 est dans P_2 et $2 \times 2 = 4 + 0 \times 5$ est bien dans Σ_5. On suppose désormais p impair. Dire que l'idéal (p) est premier signifie que le polynôme X^2+5 n'a pas de racine dans $\mathbf{F}_p$ ou encore que -5 n'est pas un carré de $\mathbf{F}_p$ et on a vu que c'était équivalent à $p \in P_3$. Au contraire, si p est dans $P_1 \cup P_2$, -5 est un carré modulo p et on note $\overline{u}$ l'une de ses racines carrées. En choisissant le signe de u, on peut supposer qu'on a $|u| < p/2$. On considère alors l'élément $u + i\sqrt{5}$ de A_5. Sa norme est $u^2 + 5$ et elle est $< p^2$ car p est ≥ 3. On considère l'idéal $I = (p, u + i\sqrt{5})$. Ses éléments sont de norme multiple de p et on choisit $a \in I$ non nul, de norme minimale. On a donc $N(a) < p^2$. La pseudo-division euclidienne de p par a montre qu'on a $kp = aq + r$ avec $k = 1, 2$ et $N(r) < N(a)$ et, comme r est dans I, il est nul. On a donc $kp = aq$ d'où $k^2p^2 = N(a)N(q)$. Comme $N(a)$ est multiple de p et $< p^2$, c'est que $N(q)$ est multiple de p. Comme k^2 vaut 1 ou 4, on a bien trouvé, entre a et q, un élément de norme p ou $2p$. Autrement dit, p ou $2p$ est dans Σ_5. Précisément, si p est dans P_2 il n'est pas dans Σ_5 et c'est donc $2p$ qui s'y trouve. Si p est dans P_1, $2p$ n'a pas la bonne congruence pour être dans Σ_5 et c'est donc p qui y est.

Il reste à montrer l'assertion sur pq. Il est clair que $4pq$ est dans Σ_5, $4pq = x^2 + 5y^2$. Si x et y sont pairs on peut simplifier par 4 et pq est de la forme voulue. Sinon, x et y sont tous deux impairs, x^2 et $5y^2$ sont congrus à 1 modulo 4 et leur somme à 2 et c'est absurde.

6.3.1 Fin de la preuve de 6.4

La proposition 6.7, jointe à la stabilité par multiplication 6.1, montre déjà que les nombres annoncés sont bien dans Σ_5.

Inversement, soit n dans Σ_5. On a donc $n = z\overline{z} = a^2 + 5b^2$ avec $z = a + ib\sqrt{5} \in \mathbf{Z}[i\sqrt{5}]$. Si p est dans P_3 et divise n, on a vu ci-dessus que (p) est un idéal premier, de sorte que p divise z ou $\overline{z}$ donc a et b. Mais alors p^2 divise n et une récurrence immédiate montre que l'exposant $v_p(n)$ est pair.

Il reste à montrer l'assertion sur P_2. On note d'abord que si $n = 5n'$ est dans Σ_5, il en est de même de n'. En effet, on a $n = a^2 + 5b^2$ et 5 divise a, $a = 5a'$, et on a $n' = b^2 + 5a'^2$. En divisant par une puissance de 5, on se ramène au cas où n n'est pas multiple de 5. En vertu de 6.2.0, n est donc congru à ± 1 modulo 5. Si la somme $\sum_{p \in P_2} v_p(n)$ était impaire, le sens direct du théorème montre que $2n$ serait dans Σ_5. Mais, il serait congru à ± 2 modulo 5 et c'est absurde, toujours par 6.2.0.

7 Annexe : prouver les isomorphismes d'anneaux

7.1 L'objectif

L'expérience montre que les étudiants ont souvent des difficultés à montrer les isomorphismes d'anneaux mettant en jeu des quotients comme ceux apparus dans 3.5 ou dans la preuve de 3.13. Cette annexe est donc là pour leur [13] donner quelques règles simples et faire que ce genre de choses leur apparaisse pour ce qu'il est, c'est-à-dire essentiellement trivial.

La première chose à comprendre est : qu'est-ce qu'un quotient, de manière intuitive ? Et la réponse est digne de la Mafia : un quotient c'est fait pour supprimer quelqu'un qui vous gêne. Par exemple, dans $\mathbf{Z}/n\mathbf{Z}$, n devient 0 (penser à la preuve par 9). C'est ce qui gouverne un isomorphisme comme celui de $\mathbf{Z}[X]/(X^2 + d)$ avec $\mathbf{Z}[i\sqrt{d}]$: on veut ajouter à $\mathbf{Z}$ l'élément $i\sqrt{d}$, on sait ajouter un élément X en construisant l'anneau des polynômes, mais X est alors une indéterminée et ne vérifie pas $X^2 = -d$. Qu'à cela ne tienne, en passant au quotient par $X^2 + d$ on tue cet élément et on obtient ce qu'on veut. Le lecteur vérifiera qu'il a compris le principe en identifiant l'anneau $\mathbf{Z}[X]/(10X - 1)$ comme un objet familier.

13. Je prie mes collègues de vouloir bien m'excuser d'enfoncer ainsi des portes ouvertes.

7.2 Les règles

Cette vision intuitive est essentielle, mais il faut aussi savoir formaliser les choses. Pour cela on utilisera deux résultats :

7.1 Proposition. (La propriété universelle des anneaux de polynômes) *Soient A, B des anneaux commutatifs, $\varphi : A \to B$ un homomorphisme d'anneaux et x un élément de B. Il existe un unique homomorphisme $\Phi : A[X] \to B$ dont la restriction à A est φ et qui envoie X sur x. On a la formule :*

$$\Phi(a_n X^n + \cdots + a_1 X + a_0) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0).$$

On retiendra ce résultat sous forme d'une règle :

Règle numéro 1 : *Pour envoyer un anneau de polynômes dans un anneau on commence par envoyer l'anneau de base, puis on envoie l'indéterminée sur un élément quelconque.*

7.2 Proposition. (Le théorème d'isomorphisme) *Soit $\Phi : A \to B$ un homomorphisme d'anneaux. Soit I un idéal de A et $p : A \to A/I$ la projection canonique. Si I est contenu dans $\operatorname{Ker}\Phi$, Φ se "factorise" par le quotient, i.e. il existe un homomorphisme $\overline{\Phi} : A/I \to B$ tel que l'on ait $\Phi = \overline{\Phi} \circ p$. De plus :*
1) $\overline{\Phi}$ est surjectif si et seulement si Φ l'est,
2) $\overline{\Phi}$ est injectif si et seulement si I est égal à $\operatorname{Ker}\Phi$.

On résume cette situation en parlant de "diagramme commutatif" :

$$\begin{array}{ccc} A & \xrightarrow{p} & A/I \\ & \searrow^{\Phi} & \downarrow{\scriptstyle \overline{\Phi}} \\ & & B \end{array}$$

Là encore ce résultat donne naissance à une règle :

Règle numéro 2 : *Pour envoyer un anneau quotient A/I dans un anneau, on commence par envoyer l'anneau A puis on factorise par I (si possible par le noyau).*

7.3 Mise en œuvre

Montrons d'abord, pour $d \equiv 1, 2 \pmod 4$ l'isomorphisme $A_d = \mathbf{Z}[i\sqrt{d}] \simeq \mathbf{Z}[X]/(X^2 + d)$. On commence par envoyer l'anneau de polynômes $\mathbf{Z}[X]$ dans $\mathbf{Z}[i\sqrt{d}]$ par un homomorphisme Φ en envoyant $\mathbf{Z}$ par l'inclusion et X en $i\sqrt{d}$. Il est clair que cet homomorphisme est surjectif (car $a + bi\sqrt{d} = \Phi(a + bX)$)

et que son noyau contient l'idéal X^2+d. Il reste à voir que le noyau est exactement cet idéal. Pour cela on effectue la division euclidienne de $P(X) \in \mathrm{Ker}\,\Phi$ par le polynôme unitaire X^2+d dans $\mathbf{Z}[X]$ (voir [DP] Ch. II 3.31). On a $P(X) = (X^2+d)Q(X)+R(X)$ avec R de degré au plus 1, $R(X) = a+bX$. Comme P et X^2+d sont dans $\mathrm{Ker}\,\Phi$ on a $R(i\sqrt{d}) = 0 = a+bi\sqrt{d}$ et donc $a = b = 0$ comme attendu.

Montrons ensuite les isomorphismes :

$$\mathbf{Z}[i\sqrt{d}]/(p) \simeq \mathbf{Z}[X]/(X^2+d,p) \simeq \mathbf{F}_p[X]/(X^2+d).$$

La règle numéro 2 indique qu'il faut partir du plus gros anneau et factoriser ensuite. Ici on part donc de $\mathbf{Z}[X]$. Pour l'isomorphisme de gauche, on l'envoie d'abord dans $\mathbf{Z}[i\sqrt{d}]$ comme ci-dessus, puis dans le quotient $\mathbf{Z}[i\sqrt{d}]/(p)$ par la projection canonique. On obtient un homomorphisme surjectif $\Phi : \mathbf{Z}[X] \to \mathbf{Z}[i\sqrt{d}]/(p)$ et il est clair que l'idéal $I = (X^2+d,p)$ est dans le noyau. Pour voir que c'est exactement le noyau on part de $P \in \mathrm{Ker}\,\Phi$, on commence par le diviser par X^2+d comme ci-dessus. On a $P(X) = (X^2+d)Q(X)+R(X)$ avec R de degré au plus 1, $R(X) = a+bX$ et $\Phi(R) = 0$. Cela signifie que $a+ib\sqrt{d}$ est dans $(p) = p\mathbf{Z}[i\sqrt{d}]$, donc qu'on a $a+ib\sqrt{d} = p(x+iy\sqrt{d})$, donc que a,b sont multiples de p. C'est exactement dire que R est multiple de p dans $\mathbf{Z}[X]$ donc qu'il est dans l'idéal (p) de $\mathbf{Z}[X]$ et $P(X) = (X^2+d)Q(X)+R(X)$ est bien dans (X^2+d,p).

Pour l'isomorphisme de droite on procède de même en envoyant d'abord $\mathbf{Z}$ dans son quotient $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, puis $\mathbf{Z}[X]$ dans $\mathbf{F}_p[X]$ par la règle numéro 1 et enfin en envoyant $\mathbf{F}_p[X]$ dans son quotient $\mathbf{F}_p[X]/(X^2+d)$. On obtient un homomorphisme Ψ, surjectif, et dont le noyau contient évidemment l'idéal (X^2+d,p). Si P est dans le noyau, on voit que sa réduction modulo p, soit $\overline{P}$, est multiple de X^2+d, autrement dit, on a $P(X) \equiv (X^2+d)Q(X) \pmod{p}$, donc $P \in (X^2+d,p)$.

8 Références

[Bachet] PERRIN Daniel, *L'équation de Bachet*, sur ma page web : `http://www.math.u-psud.fr/~perrin/Conferences/Bachet.pdf`

[Bachet-o] PERRIN Daniel, *L'équation de Bachet, version olympiades*, `http://www.math.u-psud.fr/~perrin/Conferences/OlympiadeDP.pdf`

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

[ME] PERRIN Daniel, *Mathématiques d'école*, Cassini, 2011.

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

[Serre] SERRE Jean-Pierre, *Cours d'arithmétique*, PUF, 1970.

[ST] STEWART Ian & TALL David, *Algebraic number theory*, Chapmann-Hall, 1979.

[Weil] WEIL André, *Number Theory, An approach through history, From Hammurapi to Legendre*, Birkhaüser, 1984.