Université Claude Bernard Lyon 1 Anneaux et polynômes
L3 enseignement de mathématiques : Algèbre et mathématiques discrètes
Année 2017–2018

# I Vols de canards

## 1° Étude algébrique

**Lemme.** *Le réel $\sqrt{2}$ est irrationnel.*

*Démonstration.* Supposons qu'il existe un couple d'entiers $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $\sqrt{2} = a/b$. Observons un rectangle de côtés $a$ et $b$. On retire un carré puis un nouveau carré. Les côtés du

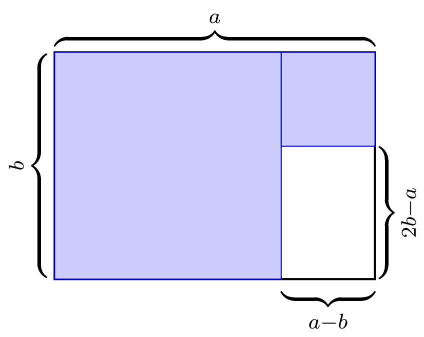


FIGURE 1 – Irrationnalité de $\sqrt{2}$ par descente infinie

rectangle blanc restant sont $a - b$ et $b - (a - b) = 2b - a$. Or on a :

$$\frac{2b-a}{a-b} = \frac{2-\frac{a}{b}}{\frac{a}{b}-1} = \frac{2-\sqrt{2}}{\sqrt{2}-1} = \frac{(2-\sqrt{2})(\sqrt{2}+1)}{\sqrt{2}^2-1} = \sqrt{2}.$$

Cela signifie que le rectangle blanc a les mêmes proportions que le rectangle initial ; de plus, les dimensions ayant diminué, on a : $2b - a < a$ et $a - b < b$. On peut recommencer *ad infinitum.* Ainsi, sous l'hypothèse que $\sqrt{2}$ est rationnel, on peut construire une suite infinie strictement décroissante d'entiers (les côtés des rectangles), ce qui est absurde. $\square$

**Lemme.** *Soit $z \in \mathbb{Z}[\sqrt{2}]$. Il existe un unique couple $(a, b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{2}$.*

*Démonstration.* L'existence provient de la définition de $\mathbb{Z}[\sqrt{2}]$, seule l'unicité doit être démontrée. Supposons que $a$, $b$, $a'$, $b'$ soient des entiers tels que $a+b\sqrt{2} = a'+b'\sqrt{2}$. Alors $a-a' = (b'-b)\sqrt{2}$. Si $b$ était différent de $b'$, on pourrait en déduire que $\sqrt{2} = (a - a')/(b' - b)$, ce qui contredit le lemme précédent. D'où $b = b'$, puis $a = a'$. $\square$

**Lemme.** *L'application $\sigma : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ préserve la somme et le produit.*

*Démonstration.* Soient $a$, $a'$, $b$, $b'$ des entiers, soient $z = a + b\sqrt{2}$ et $z' = a' + b'\sqrt{2}$, on a :

$$\sigma(z + z') = \sigma\big(a + a' + (b + b')\sqrt{2}\big) = a + a' - (b + b')\sqrt{2} = a - b\sqrt{2} + a' - b'\sqrt{2} = \sigma(z) + \sigma(z');$$
$$\sigma(zz') = \sigma\big(aa' + 2bb' + (ab' + ba')\sqrt{2}\big) = aa' + 2bb' - (ab' + ba')\sqrt{2} = (a - b\sqrt{2})(a' - b'\sqrt{2}).$$

On peut conclure. $\square$

**Définition.** On appelle *norme* sur $\mathbb{Z}[\sqrt{2}]$ l'application

$$N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}, \quad z \mapsto z\sigma(z).$$

La norme de tout élément est bien un entier puisque pour $z = a + b\sqrt{2}$, on a :

$$N(z) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

**Lemme.** *La norme du produit est le produit des normes.*

*Démonstration.* Soient $z$ et $z'$ des éléments de $\mathbb{Z}[\sqrt{2}]$, on a :

$$N(zz') = zz'\sigma(zz') = z\sigma(z)z'\sigma(z') = N(z)N(z'),$$

ce qui permet de conclure. □

**Lemme.** *Soit $z \in \mathbb{Z}[\sqrt{2}]$. Montrer que $z$ est inversible si et seulement si $N(z) = \pm 1$.*

On rappelle qu'un élément $z \in \mathbb{Z}[\sqrt{2}]$ est inversible s'il existe $z' \in A$ tel que $zz' = 1$. Par exemple, $1 + \sqrt{2}$ est inversible puisque $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$.

*Démonstration.* Soit $z \in \mathbb{Z}[\sqrt{2}]$. Supposons que $z$ soit inversible et soit $z'$ son inverse. Comme $zz' = 1$, on a : $N(z)N(z') = N(zz') = N(1) = 1$ donc, comme $N(z)$ et $N(z')$ sont des entiers, $N(z) = \pm 1$. Réciproquement, supposons que $N(z) = \varepsilon \in \{-1, 1\}$. Alors $1/\varepsilon = \varepsilon$ et $z\sigma(z) = N(z) = \varepsilon$ donc $\varepsilon\sigma(z)$, qui appartient à $\mathbb{Z}[\sqrt{2}]$, est l'inverse de $z$. □

Les inversibles de $\mathbb{Z}[\sqrt{2}]$, sont donc les solutions $(a, b)$ entières de $a^2 - 2b^2 = \pm 1$.

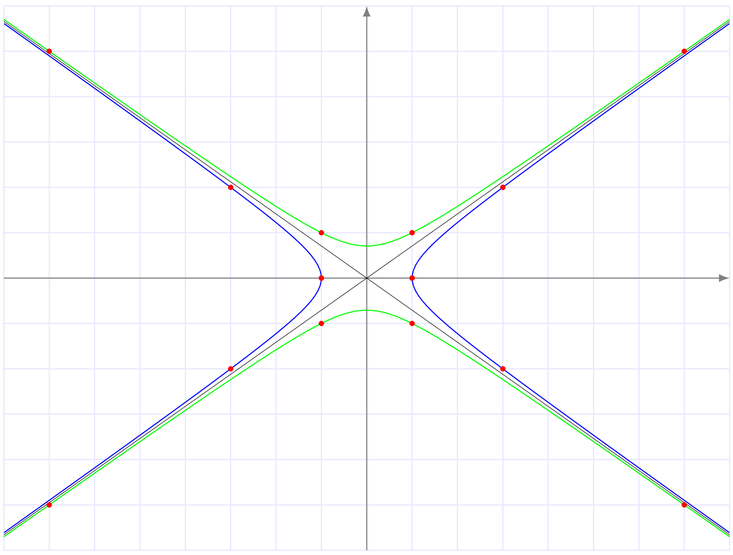

FIGURE 2 – Équations $a^2 - 2b^2 = 1$ et $a^2 - 2b^2 = -1$

**Proposition.** *Les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont, au signe près, les puissances de $1 + \sqrt{2}$.*

*Démonstration.* Soit $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ inversible. Comme l'inversibilité équivaut à $a^2 - 2b^2 = \pm 1$, propriété qui reste vraie si on change le signe de $a$ ou $b$, $a + b\sqrt{2}$ est inversible si et seulement si $\pm a \pm b\sqrt{2}$ l'est. On peut donc supposer sans perte de généralité que $a \geqslant 0$ et $b \geqslant 0$.

Si $b=0$, alors $a^2=\pm 1$ donc $a^2=1$ et, comme $a\geqslant 0$, on a : $a=1$.
Désormais, on suppose que $b>0$. Comme $a^2-2b^2=\pm 1$, on a : $a^2-b^2=b^2\pm 1\geqslant 0$ et $4b^2-a^2=2b^2\pm 1>0$. On en déduit que $a-b\geqslant 0$ et que $2b-a>0$.
Par ailleurs,

$$(-1+\sqrt{2})(a+b\sqrt{2})=(2b-a)+(a-b)\sqrt{2}.$$

Cet élément de $\mathbb{Z}[\sqrt{2}]$ est inversible puisque sa norme est $N(-1+\sqrt{2})N(a+b\sqrt{2})=-N(a+b\sqrt{2})=\pm 1$. De plus, d'après les inégalités précédentes, ses composantes $2b-a$ et $a-b$ sont dans $\mathbb{N}$. De plus, $a-b<b$ puisque $2b-a>0$.
Si $a-b=0$, alors $2b-a=1$ (d'après le cas « $b=0$ » ci-dessus). Sinon, on multiplie à nouveau par $-1+\sqrt{2}$, et ainsi de suite. On fabrique ainsi deux suites d'entiers naturels par : $a_0+b_0\sqrt{2}=a+b\sqrt{2}$ et, si $a_{n-1}+b_{n-1}\sqrt{2}$ est défini et si $b_{n-1}>0$, on pose $a_n+b_n\sqrt{2}=(-1+\sqrt{2})(a_{n-1}+b_{n-1}\sqrt{2})$. Comme $b_0>b_1>\cdots>b_n$, la suite est nécessairement finie et il existe $n$ tel que $b_n=0$ ; dans ce cas, $a_n=1$. Mais alors, par construction, $1=a_n+b_n\sqrt{2}=(-1+\sqrt{2})^n(a+b\sqrt{2})$ donc, comme $-1+\sqrt{2}=1/(1+\sqrt{2})$, on a : $a+b\sqrt{2}=(1+\sqrt{2})^n$. □

Définissons les suites entières $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ par :

$$\forall n\in\mathbb{N},\quad u_n+v_n\sqrt{2}=(1+\sqrt{2})^n.$$

Les premières valeurs de $(u_n,v_n)$ sont :

$(1,0)$, $(1,1)$, $(3,2)$, $(7,5)$, $(17,12)$, $(41,29)$, $(99,70)$, $(239,169)$, $(577,408)$, etc.

**Lemme.** *Soit $n\in\mathbb{N}$, alors :*
(i) $N\big((1+\sqrt{2})^n\big)=(-1)^n$ ;
(ii) *pour tout $n$, $u_n$ est impair et $v_n$ a la même parité que $n$ ;*
(iii) *pour tout $n\in\mathbb{N}$, $u_n=\dfrac{(1+\sqrt{2})^n+(1-\sqrt{2})^n}{2}$ et $v_n=\dfrac{(1+\sqrt{2})^n-(1-\sqrt{2})^n}{2\sqrt{2}}$ ;*
(iv) $u_n\sim\dfrac{(1+\sqrt{2})^n}{2}$ *et* $v_n\sim\dfrac{(1+\sqrt{2})^n}{2\sqrt{2}}$.

*Démonstration.* (i) Une récurrence immédiate montre que $\sigma(z^n)=\sigma(z)^n$ et $N(z^n)=N(z)^n$ pour tout $z\in\mathbb{Z}[\sqrt{2}]$ et tout $n\in\mathbb{N}$. Si $z=1+\sqrt{2}$, on a $N(z)=-1$, d'où la première assertion.
(ii) On a, en séparant les termes pairs ($k=2p$) et les termes impairs ($k=2p+1$) :

$$(1+\sqrt{2})^n=\sum_{k=0}^{n}\binom{n}{k}\sqrt{2}^k=\sum_{p=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2p}2^p+\sqrt{2}\sum_{p=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2p+1}2^p.$$

Par unicité de l'écriture des éléments de $\mathbb{Z}[\sqrt{2}]$, on en déduit que

$$u_n=\sum_{p=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2p}2^p\quad\text{et}\quad v_n=\sqrt{2}\sum_{p=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2p+1}2^p.$$

Dans la somme qui définit $u_n$, les termes d'indice $p\geqslant 1$ sont pairs (à cause du $2^p$) et le premier vaut $\binom{n}{0}=1$ donc $u_n$ est impair. Quant à $v_n$, tous les termes sont pairs sauf peut-être celui d'indice $p=0$ qui vaut $\binom{n}{1}=n$, de sorte que $v_n$ et $n$ ont la même parité.
(iii) En appliquant $\sigma$ à l'égalité $u_n+v_n\sqrt{2}=(1+\sqrt{2})^n$, il vient : $u_n-v_n\sqrt{2}=(1-\sqrt{2})^n$. Les expressions cherchées s'en déduisent par somme et différence de ces deux égalités.
(iv) Comme $|-1+\sqrt{2}|<1<1+\sqrt{2}$, $(-1+\sqrt{2})^n$ est négligeable devant $(1+\sqrt{2})^n$. □

**2°** On souhaite résoudre, pour $(m,n) \in \mathbb{N}^2$, l'équation

$$\frac{m(m+1)}{2} = 2\,\frac{n(n+1)}{2}. \tag{1}$$

On a :

$$\begin{aligned}
(1) \iff{} & 4m^2 + 4m - 2(4n^2 + 4n) = 0\\
\iff{} & (2m+1)^2 - 1 - 2\big((2n+1)^2 - 1\big) = 0\\
\iff{} & (2m+1)^2 - 2(2n+1)^2 = -1\\
\iff{} & N\big(2m+1 + (2n+1)\sqrt{2}\big) = -1.
\end{aligned}$$

D'après la description des inversibles de $\mathbb{Z}[\sqrt{2}]$, il existe un exposant *impair*, donc de la forme $2k+1$, tel que

$$2m+1+(2n+1)\sqrt{2} = (1+\sqrt{2})^{2k+1}.$$

Coup de chance, $u_{2k+1}$ et $v_{2k+1}$ sont impairs. Les solutions sont donc de la forme :

$$m = \frac{u_{2k+1}-1}{2} \quad \text{et} \quad n = \frac{v_{2k+1}-1}{2} \qquad (k \in \mathbb{N}).$$

Les premières solutions sont :

$$(0,0),\quad (3,2),\quad (20,14),\quad (119,84),\quad (696,492),\quad (4059,2870),$$
$$(23660,16730),\quad (137903,97512),\quad (803760,568344),\quad (4684659,3312554).$$

Et on a bien, par exemple :

$$\frac{3\times 4}{2} = 2\times\frac{2\times 3}{2},\quad \frac{20\times 21}{2} = 2\times 3\times 5\times 7 = 2\times\frac{14\times 15}{2},\quad \text{etc.}$$

**3°** On veut résoudre dans $\mathbb{N}$ l'équation

$$\frac{m(m+1)}{2} = n^2. \tag{2}$$

Comme pour l'équation précédente, on a :

$$\begin{aligned}
(2) \iff{} & 4m^2 + 4m - 2\cdot 4n^2 = 0\\
\iff{} & (2m+1)^2 - 2(2n)^2 = 1.
\end{aligned}$$

D'après la description des inversibles de $\mathbb{Z}[\sqrt{2}]$, il existe un exposant *pair*, donc de la forme $2k$, tel que

$$2m+1+2n\sqrt{2} = (1+\sqrt{2})^{2k}.$$

Coup de chance, $u_{2k}$ est impair et $v_{2k}$ pair. Les solutions sont donc de la forme :

$$m = \frac{u_{2k}-1}{2} \quad \text{et} \quad n = \frac{v_{2k}}{2} \qquad (k \in \mathbb{N}).$$

Les premières solutions sont :

$$(0,0),\quad (1,1),\quad (8,6),\quad (49,35),\quad (288,204),\quad (1681,1189),$$
$$(9800,6930),\quad (57121,40391),\quad (332928,235416),\quad (1940449,1372105).$$

Par exemple :

$$\frac{1\times 2}{2} = 1^2,\quad \frac{8\times 9}{2} = (2\times 3)^2 = 6^2,\quad \frac{49\times 50}{2} = (5\times 7)^2 = 35^2,\quad \text{etc.}$$