Contrôle continu n° 1

Tous les anneaux considérés sont commutatifs. Si A est un anneau, la notation $A^\times$ désigne l'ensemble des éléments inversibles de A, et pour tout $a \in A$, la notation (a) désigne l'idéal de A engendré par a.

Exercice.

Soient k un corps de caractéristique 0 et n un entier naturel non nul.

1. Dans $k[X]$, montrer que $X-1$ divise X^n-1 mais que $(X-1)^2$ ne divise pas X^n-1.
2. Montrer que le polynôme X^n+Y^n-1 est irréductible dans $k[X,Y]$.

Correction :

1. *1 est racine de X^n-1 donc $X-1$ divise X^n-1. Si $(X-1)^2$ divisait X^n-1, alors $X-1$ diviserait le polynôme dérivé nX^{n-1}, ce qui n'est pas le cas.*
2. *Le polynôme $X-1$ est de degré 1, donc irréductible dans $k[X]$. On peut alors appliquer le critère d'Eisenstein à Y^n+X^n-1 dans $k[X][Y]$ avec $X-1$.*

Problème : un anneau principal non euclidien.

Dans toute la suite, on pose $\alpha = \dfrac{1+i\sqrt{19}}{2}$ et $\bar{\alpha} = \dfrac{1-i\sqrt{19}}{2}$.

I. Un critère d'euclidianité

1. Soient A, B deux anneaux non nuls et $\phi : A \to B$ un morphisme d'anneaux.
   (a) Montrer que $\phi(A^\times) \subset B^\times$.
   (b) En déduire que si la restriction de ϕ à $A^\times \cup \{0\}$ est surjective, alors B est un corps.
2. Soit A un anneau euclidien non nul.
   (a) Montrer que $x \in A$ est non inversible si et seulement si l'anneau quotient $A/(x)$ est non nul.
   (b) Montrer qu'il existe un élément non inversible $x \in A$ tel que la restriction de la projection canonique $\pi : A \to A/(x)$ à $A^\times \cup \{0\}$ est surjective (si A n'est pas un corps, on pourra utiliser en la justifiant l'existence d'un élement non nul, non inversible de stathme minimal).
   (c) Soit $x \in A$ un élément comme ci-dessus. Montrer que l'idéal (x) est maximal.

Correction :

1. (a) $\phi(1_A) = 1_B$ *par définition. Si* $a \in A^\times$*, alors il existe* $b \in A$ *tel que* $ab = 1_A$*, et donc* $\phi(a)\phi(b) = \phi(ab) = \phi(1_A) = 1_B$*. En particulier* $\phi(a)$ *est inversible dans* B *d'inverse* $\phi(b)$*.*

   (b) *Clair puisqu'alors* $B \setminus \{0\} = \phi(A^\times) \subset B^\times$*. Tout élément non nul de* B *est donc inversible.*

2. (a) *Si* x *est inversible alors* $(x) = A$*, donc* $A/(x)$ *est l'anneau nul.*
   Réciproquement, si $A/(x)$ *est l'anneau nul alors* $(x) = A$*, donc* $1 \in (x)$*, donc il existe* $y \in A$ *tel que* $1 = xy$*, et* x *est bien inversible.*

   (b) *Si* A *est un corps, on peut prendre* $x = 0$ *: alors* $A/(x) = A$ *et* π *est l'identité, et comme* A *est un corps on a* $A^\times \cup \{0\} = A$*, donc la restriction de* π *est évidemment surjective.*

   Si A *n'est pas un corps : comme* A *est euclidien, il existe une application* $\nu : A \setminus \{0\} \to \mathbb{N}$*, tel que pour tout* $(a, b) \in A^2$ *avec* $b \neq 0$*, il existe* $(q, r) \in A^2$ *tel que* $a = bq + r$ *et* $r = 0$ *ou* $\nu(r) < \nu(b)$*.*
   A n'étant pas un corps, l'ensemble $\{\nu(a) \mid a \in A \setminus (A^\times \cup \{0\})\}$ *est une partie non vide de* $\mathbb{N}$*, et admet donc un plus petit élément. On prend alors* $x \in A \setminus (A^\times \cup \{0\})$ *tel que* $\nu(x) = \min\{\nu(a) \mid A \setminus (A^\times \cup \{0\})\}$*.*
   Soit z *un élément de* $A/(x)$ *; par définition, il existe* $a \in A$ *tel que* $z = \pi(a)$ *avec* π *la projection* $A \to A/(x)$*. On écrit la division euclidienne :* $a = qx + r$ *avec* $r = 0$ *ou* $\nu(r) < \nu(x)$*. On a forcément* $r \in A^\times \cup \{0\}$*, sinon on aurait* $\nu(r) \geq \nu(x)$ *par définition de* x*. Or* $z = \pi(a) = \pi(qx + r) = \pi(r)$*, donc tout élément de* $A/(x)$ *a bien un antécédent dans* $A^\times \cup \{0\}$*.*

   (c) *Si* x *non inversible est tel que la restriction du morphisme d'anneau* $\pi : A \to A/(x)$ *à* $A^\times \cup \{0\}$ *est surjective, alors* $A/(x)$ *est non nul car* x *non inversible, et c'est un corps d'après 1b, donc l'idéal* (x) *est maximal.*

II. L'anneau $\mathbb{Z}\left[\dfrac{1 + i\sqrt{19}}{2}\right]$

3. Montrer que l'anneau $\mathbb{Z}[\alpha]$ est isomorphe à $\mathbb{Z}[X]/(X^2 - X + 5)$, puis que $\mathbb{Z}[\alpha] = \{a + b\alpha \mid (a, b) \in \mathbb{Z}^2\}$.
4. Pour tout $z = a + b\alpha \in \mathbb{Z}[\alpha]$, on pose $\bar{z} = a + b\bar{\alpha}$ et $N(z) = a^2 + ab + 5b^2$.
   (a) Pour tout $z \in \mathbb{Z}[\alpha]$, montrer que $\bar{z}$ appartient à $\mathbb{Z}[\alpha]$ et que $N(z) = z\bar{z}$.
   (b) En utilisant des propriétés de N que l'on justifiera, déterminer l'ensemble $\mathbb{Z}[\alpha]^\times$ des inversibles de $\mathbb{Z}[\alpha]$.
5. Montrer que $\mathrm{Frac}(\mathbb{Z}[\alpha]) = \{u + v\alpha \mid (u, v) \in \mathbb{Q}\}$.

Correction :

3. *On considère le morphisme d'anneaux* $\psi : \mathbb{Z}[X] \to \mathbb{C}$ *qui à* P *associe* $P(\alpha)$*. Son image est clairement* $\mathbb{Z}[\alpha]$*, et on vérifie aisément que* $X^2 - X + 5$ *appartient à son noyau (car* $\alpha^2 = \alpha + 5$*), i.e.* $(X^2 - X + 5) \subset \ker\psi$*.*
   Maintenant si $P \in \ker\psi$*, alors on écrit la division euclidienne dans* $\mathbb{Z}[X]$ *par le polynôme* $X^2 - X + 5$ *(possible car il est unitaire) :* $P = (X^2 - X + 5)Q + R$ *avec* $\deg R < 2$*, donc* $R = a + bX$ *avec* $a, b \in \mathbb{Z}$*. En évaluant en* α*, il vient* $R(\alpha) = 0$*; si* R *est non nul on en déduit que* $\alpha = -a/b$ *donc est dans* $\mathbb{Q}$*, contradiction. Par suite* $R = 0$*, donc* P *appartient à* $(X^2 - X + 5)$*, et finalement* $\ker\psi = (X^2 - X + 5)$*. On en conclut que* $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(X^2 - X + 5)$ *par le théorème d'isomorphisme.*

Ensuite, si $z \in \mathbb{Z}[\alpha]$, alors $z = P(\alpha)$ pour un certain $P \in \mathbb{Z}[X]$. Division euclidienne : il existe $Q, R \in \mathbb{Z}[X]$ tels que $P = (X^2 - X + 5)Q + R$ et $\deg R < 2$, donc R de la forme $a + bX$ où $a, b \in \mathbb{Z}$. Par suite $z = P(\alpha) = R(\alpha) = a + b\alpha$.

4. *(a) On obtient facilement $\alpha\bar{\alpha} = 5$ et $\bar{\alpha} = 1 - \alpha$, donc si z est dans $\mathbb{Z}[\alpha]$ alors $\bar{z}$ est aussi dans $\mathbb{Z}[\alpha]$. Un calcul simple donne ensuite $(a + b\alpha)(a + b\bar{\alpha}) = a^2 + ab + 5b^2$.*

   (b) $z \mapsto \bar{z}$ est la restriction à $\mathbb{Z}[\alpha]$ de la conjugaison complexe, donc on a $\overline{zz'} = \overline{z}.\overline{z'}$ pour tout $(z, z') \in \mathbb{Z}[\alpha]^2$. On en déduit que $N(zz') = zz'\overline{zz'} = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = N(z)N(z')$, i.e. l'application $N : \mathbb{Z}[\alpha] \to \mathbb{Z}$ est multiplicative. Par ailleurs $N(z) \geq 0$ pour tout $z \in \mathbb{Z}[\alpha]$ (restriction du carré du module complexe), donc N est en fait une application multiplicative $\mathbb{Z}[\alpha] \to \mathbb{N}$.
   On peut aussi obtenir la positivité de N en observant que $a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2$.

   Mainteant si $z = a + b\alpha \in \mathbb{Z}[\alpha]^\times$, alors il existe z' tel que $zz' = 1$, donc $N(z)N(z') = N(zz') = N(1) = 1$. Comme N est à valeurs dans $\mathbb{N}$, on en déduit que nécessairement $N(z) = 1$, donc $a^2 + ab + 5b^2 = 1$, donc $(a + b/2)^2 + 19b^2/4 = 1$. Mais si $b \neq 0$ alors $19b^2/4 > 1$, impossible ; donc $b = 0$ et $a^2 = 1$, i.e. $z = \pm 1$. Par ailleurs 1 et -1 sont évidemment inversibles, donc $\mathbb{Z}[\alpha]^\times = \{1, -1\}$.

5. *Par double inclusion. Si $u = a/b$ et $v = c/d$ sont deux éléments de $\mathbb{Q}$, alors $u + v\alpha = \frac{ad+bc\alpha}{bd+0\alpha} \in Frac(\mathbb{Z}[\alpha])$. Réciproquement, si z, z' sont deux éléments de $\mathbb{Z}[\alpha]$ avec $z \neq 0$, alors $\frac{z'}{z} = \frac{z'\overline{z}}{z\overline{z}}$. Or $z'\overline{z}$ est un élément de $\mathbb{Z}[\alpha]$, qu'on peut donc écrire comme $a + b\alpha$ avec $a, b \in \mathbb{Z}$, et donc $\frac{z'}{z} = \frac{a}{N(z)} + \frac{b}{N(z)}\alpha$.*

III. Non-euclidianité

6. Montrer que le polynôme $X^2 - X + 5$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$ et dans $\mathbb{Z}/3\mathbb{Z}[X]$
7. À l'aide de la question précédente, montrer qu'il n'existe pas de morphisme d'anneaux de $\mathbb{Z}[\alpha]$ dans $\mathbb{Z}/2\mathbb{Z}$ ni de $\mathbb{Z}[\alpha]$ dans $\mathbb{Z}/3\mathbb{Z}$.
8. En déduire que $\mathbb{Z}[\alpha]$ n'est pas euclidien.

Correction :

6. *On vérifie que X^2+X+1 ($= X^2-X+5 \bmod 2$) n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$, et que X^2-X-1 ($= X^2 - X + 5 \bmod 3$) n'a pas de racines dans $\mathbb{Z}/3\mathbb{Z}$.*
7. *Par l'absurde, on suppose qu'il existe $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/2\mathbb{Z}$. Comme ϕ envoie 1 sur (la classe de) 1, la restriction de ϕ à $\mathbb{Z} \subset \mathbb{Z}[\alpha]$ est forcément la réduction modulo 2, c'est-à-dire la projection canonique $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.*
   Par conséquent $0 = \phi(0) = \phi(\alpha^2 - \alpha + 5) = \phi(\alpha)^2 + \phi(\alpha) + 1$, autrement dit $\phi(\alpha)$ est une racine dans $\mathbb{Z}/2\mathbb{Z}$ de $X^2 + X + 1$, en contradiction avec la question précédente.
   L'argument est exactement le même pour $\mathbb{Z}/3\mathbb{Z}$.
8. *Par l'absurde, supposons $\mathbb{Z}[\alpha]$ euclidien. Alors d'après I. il existe $x \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}[\alpha]^\times$ tel que la restriction à $\mathbb{Z}[\alpha]^\times \cup \{0\}$ de $\pi : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/(x)$ est surjective. Or d'après 4, on a $\mathbb{Z}[\alpha]^\times \cup \{0\} = \{-1, 0, 1\}$, donc $\mathbb{Z}[\alpha]/(x)$ a au plus trois éléments ; comme $\mathbb{Z}[\alpha]/(x)$ est non nul il est isomorphe soit à $\mathbb{Z}/2\mathbb{Z}$, soit à $\mathbb{Z}/3\mathbb{Z}$. Il existe donc un morphisme d'anneaux de $\mathbb{Z}[\alpha]$ dans $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$, ce qui est impossible d'après la question précédente.*

IV. Pseudo-division euclidienne

On étend la définition de N à $\mathrm{Frac}(\mathbb{Z}[\alpha])$ en posant, pour tout $u, v \in \mathbb{Q}$, $N(u+v\alpha) = (u+v\alpha)(u+v\bar{\alpha}) = u^2 + uv + 5v^2$.

9. Soient $z_1, z_2 \in \mathbb{Z}[\alpha]$ avec $z_2 \neq 0$, et $u, v \in \mathbb{Q}$ tels que $z_1/z_2 = u + v\alpha$ (cf. question 5). On note $\lfloor u \rceil$ et $\lfloor v \rceil$ les entiers les plus proches de u et v.
   Montrer que si $|v - \lfloor v \rceil| \leq 1/3$ alors $N(z_1/z_2 - (\lfloor u \rceil + \lfloor v \rceil \alpha)) < 1$.
10. Prouver que si $|v - \lfloor v \rceil| > 1/3$, alors $N(2z_1/z_2 - (\lfloor 2u \rceil + \lfloor 2v \rceil \alpha)) < 1$.
11. En déduire que pour tout $(z_1, z_2) \in \mathbb{Z}[\alpha]^2$ tel que $z_2 \neq 0$, il existe un couple $(q, r) \in \mathbb{Z}[\alpha]^2$ tel que :
    — $N(r) < N(z_2)$,
    — $z_1 = qz_2 + r$ ou $2z_1 = qz_2 + r$.

Correction :

9. Comme $|u - \lfloor u \rceil| \leq 1/2$ et $|v - \lfloor v \rceil| \leq 1/3$, on a

$$\begin{aligned} N\left(z_1/z_2 - (\lfloor u \rceil + \lfloor v \rceil \alpha)\right) &= N\left((u - \lfloor u \rceil) + (v - \lfloor v \rceil)\alpha\right) \\ &= (u - \lfloor u \rceil)^2 + (u - \lfloor u \rceil)(v - \lfloor v \rceil) + 5(v - \lfloor v \rceil)^2 \\ &\leq \frac{1}{2^2} + \frac{1}{2.3} + 5\frac{1}{3^2} = \frac{35}{36} < 1 \end{aligned}$$

10. On note $n = \lfloor v \rfloor$ la partie entière de v. Si $|v - \lfloor v \rceil| > 1/3$, cela signifie que $n + 1/3 < v < n + 2/3$. En multipliant par 2 on a $2n + 2/3 < 2v < 2n + 4/3$, soit $-1/3 < 2v - (2n+1) < 1/3$. Autrement dit, $\lfloor 2v \rceil = 2n + 1$ et $|2v - \lfloor 2v \rceil| < 1/3$. On peut alors raisonner comme en 9. en remplaçant z_1/z_2, u et v par $2z_1/z_2$, $2u$ et $2v$.

11. On pose $z_1/z_2 = u + v\alpha$, puis on raisonne par cas :
— *Si $|v - \lfloor v \rceil| \leq 1/3$, on pose $q = \lfloor u \rceil + \lfloor v \rceil \alpha \in \mathbb{Z}[\alpha]$, de sorte que $N(z_1/z_2 - q) < 1$. On pose aussi $r = z_1 - qz_2 \in \mathbb{Z}[\alpha]$. On a alors évidemment $z_1 = qz_2 + r$, et $N(r) = N(z_1 - qz_2) = N(z_1/z_2 - q)N(z_2) < N(z_2)$.*
— *Si $|v - \lfloor v \rceil| > 1/3$, on pose $q = \lfloor 2u \rceil + \lfloor 2v \rceil \alpha \in \mathbb{Z}[\alpha]$, de sorte que $N(2z_1/z_2 - q) < 1$. On pose aussi $r = 2z_1 - qz_2 \in \mathbb{Z}[\alpha]$. On a alors évidemment $2z_1 = qz_2 + r$, et $N(r) = N(2z_1 - qz_2) = N(2z_1/z_2 - q)N(z_2) < N(z_2)$.*

Remarquons qu'on a utilisé ici implicitement que :
• *N est encore multiplicative sur $\mathrm{Frac}(\mathbb{Z}[\alpha])$, ce qui se montre comme en 4b ;*
• *$N(z_2) \neq 0$ si $z_2 \neq 0$, ce qui peut se montrer à partir de l'expression $N(a + b\alpha) = (a + b/2)^2 + 19b^2/4$, ou en passant par le module complexe.*

V. Principalité

12. Démontrer que l'anneau quotient $\mathbb{Z}[\alpha]/(2)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1)$.
    En déduire que l'idéal $(2) \subset \mathbb{Z}[\alpha]$ est maximal.
13. Soit I un idéal non nul de $\mathbb{Z}[\alpha]$ et $w \in I \setminus \{0\}$ tel que $N(w) = \min\{N(z) \mid z \in I \setminus \{0\}\}$.
    Soit x un élément quelconque de I. On note $q, r \in \mathbb{Z}[\alpha]$ deux éléments comme en question 11., c'est-à-dire tels que $x = qw + r$ ou $2x = qw + r$, et $N(r) < N(w)$.
    (a) On suppose dans un premier temps que $2x = qw + r$. Montrer que $r = 0$, puis que $2|q$ ou $2|w$.

(b) Si $2 \nmid q$, alors $2|w$, et il existe donc $w' \in \mathbb{Z}[\alpha]$ tel que $2w' = w$.

i. Montrer que dans ce cas $(2, q) = \mathbb{Z}[\alpha]$, puis qu'il existe $\lambda, \mu \in \mathbb{Z}[\alpha]$ tels que $2\lambda + \mu q = 1$.

ii. Montrer que $\lambda w + \mu x = w'$, puis que $w' \in I$.

iii. Comparer $N(w')$ et $N(w)$. Que peut-on en conclure ?

(c) Si $2|q$, montrer que $x \in (w)$.

(d) On suppose maintenant que $x = qw + r$. Montrer que $x \in (w)$.

14. Montrer que $\mathbb{Z}[\alpha]$ est principal.

Correction :

12. On utilise la question 3 :

$$\mathbb{Z}[\alpha]/(2) \simeq (\mathbb{Z}[X]/(X^2 - X + 5))/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5)$$
$$\simeq (\mathbb{Z}[X]/(2))/(X^2 - X + 5) \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1).$$

Comme $X^2 + X + 1$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, le quotient est un corps, donc l'idéal (2) est maximal.

13. (a) $r = 2x - qw \in I$, donc si r est non nul on a $N(w) \leq N(r)$ par définition de w, contradiction. Donc $2x = qw$, ce qui implique $qw \in (2)$. Or l'idéal (2) est maximal, donc premier, donc $q \in (2)$ ou $w \in (2)$, i.e. $2|q$ ou $2|w$.

(b) i. $q \notin (2)$ donc l'idéal $(2, q)$ contient strictement l'idéal (2). Or (2) est maximal, donc $(2, q) = \mathbb{Z}[\alpha]$. En particulier $1 \in (2, q)$, d'où l'existence de λ et μ.

ii. En multipliant par w', on a $2\lambda w' + \mu q w' = w'$. Or $2w' = w$, et comme $2x = qw = 2qw'$, on a $x = qw'$ (par intégrité), d'où l'égalité $\lambda w + \mu x = w'$. Et puisque w et x sont dans l'idéal I on a bien $w' \in I$.

iii. $N(w) = N(2w') = N(2)N(w') = 4N(w')$. Or $w \neq 0$, donc $w' \neq 0$, donc $N(w)$ et $N(w')$ sont des entiers strictement positifs et par suite $N(w) > N(w')$, ce qui est en contradiction avec la définition de w et le fait que $w' \in I \setminus \{0\}$.

On en conclut donc que l'hypothèse $2 \nmid q$ était fausse, i.e. $2|q$.

(c) Comme $2x = qw$, si $q = 2q'$ alors $x = q'w \in (w)$.

(d) $r = x - qw \in I$, donc si r est non nul on a $N(w) \leq N(r)$ par définition de w, contradiction. Donc $x = qw$, ce qui implique $x \in (w)$.

14. On a montré à la question précédente que pour tout idéal I non nul de $\mathbb{Z}[\alpha]$, on avait $I \subset (w)$ où $w \in I \setminus \{0\}$ est tel que $N(w) = \min\{N(z) \mid z \in I \setminus \{0\}\}$. L'inclusion réciproque étant évidente, on a $I = (w)$, autrement tout idéal non nul de $\mathbb{Z}[\alpha]$ est principal, donc $\mathbb{Z}[\alpha]$ est principal.