Corrigé Contrôle continu Arithmétique et algèbre commutative mercredi 26 février 2014
10h00–12h00

1. Soit $\mathbf{Z}[\mathbf{i}] = \{\, a + \mathbf{i}b \mid a, b \in \mathbf{Z} \,\}$ (avec $\mathbf{i}^2 = -1$), l'anneau des entiers de Gauss et soit $A = \mathbf{Z}[\mathbf{i}]/(1+3\mathbf{i})$ où $(1 + 3\mathbf{i})$ est l'idéal engendré par $1 + 3\mathbf{i}$.

a. Montrer que dans A on a $\mathbf{i} \equiv 3 \pmod{1 + 3\mathbf{i}}$ et $10 \equiv 0 \pmod{1 + 3\mathbf{i}}$.

√ *Par définition $a \equiv b \pmod{1 + 3\mathbf{i}}$ veut dire que $a - b$ est divisible (dans $\mathbf{Z}[\mathbf{i}]$) par $1 + 3\mathbf{i}$. Or $\mathbf{i} - 3 = \mathbf{i}(1 + 3\mathbf{i})$ est clairement divisible par $1 + 3\mathbf{i}$, et $10 - 0 = 10 = (1 + 3\mathbf{i})(1 - 3\mathbf{i})$ aussi.*

b. En déduire que dans A tout élément est la classe d'un entier.

√ *D'après la première congruence $a + \mathbf{i}b \equiv a + 3b \pmod{1 + 3\mathbf{i}}$, donc la classe de $a + \mathbf{i}b$ est la même que celle de $a + 3b$, qui est un entier.*

c. Calculer le noyau du morphisme naturel $\mathbf{Z} \to A$.

√ *On a vue que $10 \in (1 + 3\mathbf{i})$, donc le noyau contient 10. En considérant la "norme" $N(z) = |z|^2$, qui est multiplicatif $\mathbf{Z}[\mathbf{i}] \to \mathbf{Z}$, on voit que 2 et 5 ne peuvent pas être dans l'idéal $(1+3\mathbf{i})$ (dont les éléments z ont tous $10 \mid N(z)$). Le générateur du noyau doit diviser 10, donc le noyau est $10\mathbf{Z}$.*

d. Montrer que A est isomorphe à un anneau de la forme $\mathbf{Z}/n\mathbf{Z}$ où n est un entier à déterminer.

√ *L'image du morphisme naturel $\mathbf{Z} \to A$ est isomorphe à $\mathbf{Z}/10\mathbf{Z}$. Comme tout élément de A est une classes représentée par un entier (question b) cette image est A tout entier.*

2. Soit $n > 0$ un entier.

a. Montrer que n est inversible dans l'anneau $A = \mathbf{Z}[X]/(nX - 1)$.

√ *Comme $nX \equiv 1 \pmod{nX - 1}$, l'image de X dans le quotient est l'inverse de (l'image de) n.*

b. Montrer que A est isomorphe à un sous-anneau de $\mathbf{Q}$ que l'on déterminera.

√ *Par la propriété des anneaux de polynômes, il existe un morphisme $f : \mathbf{Z}[X] \to \mathbf{Q}$ qui est l'identité sur $\mathbf{Z}$ et tel que $f(X) = \frac{1}{n}$. Comme $f(nX - 1) = nf(X) - 1 = \frac{n}{n} - 1 = 0$, le noyau $\ker(f)$ contient $nX - 1$, et si l'on peut montrer que $\ker(f) = (nX - 1)$, alors le théorème d'isomorphisme montrera que $\mathbf{Z}[X]/(nX-1)$ est isomorphe à l'image de f, qui est le sous-anneau $\mathbf{Z}[\frac{1}{n}]$ de $\mathbf{Q}$. Pour montrer que $\ker(f) \subseteq (nX-1)$ (l'autre inclusion étant claire) supposons le contraire, et considérons $P \in \ker(f) \setminus (nX - 1)$ de degré minimal. Le coefficient dominant de P n'est pas divisible par n, car sinon il existerait un polynôme $Q \in (nX - 1)$ avec le même terme dominant, et $P - Q$ contredirait le choix de P. Donc si cX^d est le terme dominant de P son image $f(cX^d) = \frac{c}{n^d}$ n'est pas un multiple entier de $\frac{1}{n^{d-1}}$. Mais tous les termes de $f(cX^d - P)$ sont des multiples entiers de $\frac{1}{n^{d-1}}$, et donc $f(cX^d - P)$ aussi, contredisant $f(cX^d - P) = f(cX^d) - f(P) = f(cX^d)$. Cela établit $\ker(f) = (nX - 1)$. Le sous-anneau $\mathbf{Z}[\frac{1}{n}]$ de $\mathbf{Q}$ est celui de toutes les factions pouvant être écrit avec une puissance de n comme dénominateur.*

3. Soit R un sous-anneau de $\mathbf{Q}$. On veut montrer que R est un anneau principal.

a. Chaque $\alpha \in R$ est un nombre rationnel, qu'on peut donc écrire comme une fraction *irréductible* $\alpha = \frac{p}{q}$. En utilisant des coefficients de Bezout pour $1 = \operatorname{pgcd}(p, q)$, montrer que $\frac{1}{q} \in R$ aussi.

√ *Si $s, t \in \mathbf{Z}$ sont tels que $1 = sp + tq$, alors $\frac{1}{q} = \frac{sp+tq}{q} = s\alpha + t \in R$.*

b. Pour un idéal I de R, montrer que $I \cap \mathbf{Z}$ est un idéal de $\mathbf{Z}$.

√ *Comme R est un anneau de caractéristique 0, il contient $\mathbf{Z}$ comme sous-anneau. L'intersection $I \cap \mathbf{Z}$ est à la fois un sous-groupe additif de R (car intersection de deux tels sous-groupes) et fermé pour la multiplication par tout élément de $\mathbf{Z}$ (car I et $\mathbf{Z}$ le sont chacun: $\mathbf{Z}$ parce que c'est un anneau, et I parce qu'il est même fermé pour la multiplication par tout élément de R). Un autre argument est que $I \cap \mathbf{Z}$ est le noyau d'un morphisme composé $\mathbf{Z} \to R \to R/I$, donc un idéal de $\mathbf{Z}$.*

c. Soit I un idéal de R, et $\alpha \in I$ un élément non nul. Montrer que $I \cap \mathbf{Z} \neq \{0\}$, et que α est un multiple dans R du plus petit élément $d > 0$ de $I \cap \mathbf{Z}$.

√ *Si $\alpha = \frac{p}{q}$ avec $p \neq 0$, alors $I \cap \mathbf{Z}$ contient l'entier strictement positif $|p| = |q\alpha|$, et n'est donc pas réduit à $\{0\}$. Comme tout idéal non nul de $\mathbf{Z}$, il est engendré par son plus petit élément strictement positif d, avec donc $p \mid d$. On a vu que $\frac{1}{q} \in R$, et on a $\alpha = \frac{1}{q}p = \frac{1}{q}(p/d)d$, un multiple dans R de d.*

d. En déduire que dans cette situation $I = dR$, et conclure que R est un anneau principal.

√ *On vient de montrer que tout élément non nul de I est multiple dans R de d (qui était choisi de façon indépendante de α), et c'est évidemment aussi le cas de 0, donc $I \subseteq dR$. Mais par construction $d \in I$, donc aussi $dR \subseteq I$, et $dR = I$. Cela montre que tout idéal autre que $\{0\}$ est principal, et $\{0\} = 0R$ l'est naturellement aussi. Cela prouve que R est une anneau principal.*

4. Soit $\mathbf{D}$ le sous-anneau de $\mathbf{Q}$ des nombres décimaux : ceux qui s'écrivent sous la forme $\frac{n}{10^k}$ avec $n \in \mathbf{Z}$ et $k \in \mathbf{N}$.

a. Décrire le groupe $\mathbf{D}^\times$ des éléments inversibles de $\mathbf{D}$.

√ *Les inversibles de $\mathbf{D}$ sont des fractions non nulles $\frac{n}{10^k}$ dont l'inverse (dans $\mathbf{Q}$) $\frac{10^k}{n}$ est aussi dans $\mathbf{D}$, c'est-à-dire dont n divise une puissance de 10 (de sorte que l'inverse puisse être écrit avec un tel dénominateur). C'est le cas si n n'a pas d'autres facteurs premiers que 2 et 5, c'est-à-dire si $n = 2^l 5^m$ pour certains $l, m \in \mathbf{N}$. Aussi correct : $\mathbf{D}^\times = \{\, \frac{p}{q} \mid p, q \in M \,\}$ où $M = \{\, 2^l 5^m \mid l, m \in \mathbf{N} \,\}$.*

b. Pour $d \in \mathbf{D}$ on définit $n(d) \in \mathbf{Z}$ ainsi. Si $d = 0$ on pose $n(d) = 0$. Sinon on écrit $d = n \times 10^i$ avec $n \in \mathbf{Z}$ et $i \in \mathbf{Z}$ (l'exposant peut donc être positif ou négatif) et où on exige que n *ne soit pas divisible* par 10 ; alors $n(d)$ est défini comme le nombre n dans cette écriture. Montrer que pour tout d l'entier $n(d)$ est bien défini, et que $n(d) = xd$ pour un élément inversible $x \in \mathbf{D}^\times$.

√ *Pour que $n(d)$ soit bien défini pour $d \in \mathbf{D} \setminus \{0\}$, il faut qu'une écriture comme indiquée existe et soit unique. Par définition de $\mathbf{D}$ il existe des entiers $m \in \mathbf{Z}, k \in \mathbf{N}$ avec $d = \frac{m}{10^k}$. Si l est le plus grand nombre naturel tel que 10^l divise m (qui existe car $d \neq 0$) alors $n = m/10^l$ est entier et non divisible par 10, donc l'écriture $d = n \times 10^{l-k}$ convient. Pour l'unicité, si $d = n_1 \times 10^{i_1} = n_2 \times 10^{i_2}$ sont deux telles écritures avec $i_1 < i_2$, alors $n_1 = 10^{i_2 - i_1} n_2$, ce qui contredit que n_1 n'est pas divisible par 10, donc on ne peut pas avoir deux telles écritures différentes. Avec l'unique telle écriture $d = n \times 10^i$ on voit que $n(d) = n = d \times 10^{-i} = xd$, où on a bien que $x = 10^{-i} \in \mathbf{D}^\times$.*

On veut montrer que $\mathbf{D}$ admet une division euclidienne dans le sens suivant : pour tout $a, b \in \mathbf{D}$ avec $b \neq 0$ il existe un quotient $q \in \mathbf{D}$ et un reste $r \in \mathbf{D}$ tels que $a = qb + r$ et $|n(r)| < |n(b)|$.

c. Montrer, un utilisant la division euclidienne dans $\mathbf{Z}$, que cet énoncé est vrai dans le cas particulier où a, b sont des *entiers* et en plus b n'est pas divisible par 10.

√ *Le fait que b n'est pas divisible par 10 assure que $n(b) = b$. On peut alors prendre les mêmes quotient q et reste r que dans la division euclidienne de a par b dans $\mathbf{Z}$: on obtient $n(r)$ de l'entier r en divisant zéro ou plus fois par 10, d'où $|n(r)| \leq |r| < |b| = |n(b)|$.*

d. Montrer ensuite le cas général de l'énoncé, en se servant du quotient et du reste pour la division dans $\mathbf{D}$ de $n(a)$ par $n(b)$, division qui relève du cas particulier considéré dans le point précédent.

√ *D'après le point précédent il existe q_0, r_0 avec $n(a) = q_0 n(b) + r_0$ et $|n(r_0)| < |n(n(b))| = |n(b)|$. Avec $x, y \in \mathbf{D}^\times$ tels que $n(a) = xa$ et $n(b) = yb$, on a $a = x^{-1} n(a) = x^{-1}(q_0 n(b) + r_0) = q_0 x^{-1} y b + x^{-1} r_0$, donc on peut prendre $q = q_0 x^{-1} y$ et $r = x^{-1} r_0$, car x^{-1} étant une puissance de 10 on a $n(r) = n(x^{-1} r_0) = n(r_0)$ et donc $|n(r)| < |n(b)|$.*

Fin.