UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Corrigé Examen terminal, session 1, 5 Mai 2017

Exercice 1
1. $\mathbf{Z}$, $\mathbf{R}[X]$, $\mathbf{Z}[i]$ sont des anneaux principaux. (Les corps sont aussi des anneaux principaux, mais ce sont des exemples "assez mauvais"...)
2. X est irréductible dans $\mathbf{R}[X]$ (car de degré 1), 3 est irréductible dans $\mathbf{Z}[i]$ (car n'est pas somme de deux carrés). On peut aussi se servir de l'énoncé du problème ci-dessous : d'après la toute fin, $2, 3, 7, 13$ sont des exemples d'irréductibles dans $\mathbf{Z}[\omega]$, qui est principal.

Questions de cours
1. Soit $(I_n)_{n\geq 0}$ une suite croissante (au sens de l'inclusion) d'idéaux d'un anneau commutatif unitaire A. Soit $J = \cup_{n\geq 0} I_n$. J est non vide car I_0 est non vide. Soient $x, y \in J$.Donc il existe n, m deux entiers avec $x \in I_n, y \in I_m$. Quitte à intervertir x et y, on peut supposer que $n \geq m$. Donc $y \in I_m \subset I_n$ par croissance, et donc $x - y \in I_n$ comme différence de deux éléments de I_n. Donc $x - y \in I_n \subset J$. Soit maintenant $x \in J$ et $a \in A$. Il existe n tel que $x \in I_n$. Comme I_n est absorbant, $ax \in I_n \subset J$. Ce qui prouve que J est un idéal de A.

1 Soit $(I_n)_{n\geq 0}$ une suite croissante (au sens de l'inclusion) d'idéaux d'un anneau principal A. On pose $J = \cup_{n\geq 0} I_n$. D'après la question 1, c'est un idéal, et comme A est principal, il existe $x \in A$ avec $J = Ax$. Comme $x \in J$, il existe m tel que $x \in I_m$. On a donc par absorption, pour tout $n \geq m$,

$$Ax \subset I_m \subset I_n \subset J = Ax.$$

Par double inclusion, $I_m = I_n = J$.

Exercice 2
1.
$$\sigma = (1, 2, 4, 8)(3, 6, 12, 9)(5, 10)(7, 13, 11).$$

2. L'ordre de σ est le ppcm de la longueur des cycles, à savoir $ppcm(4, 4, 2, 3) = 12$. Sa signature est $(-1) * (-1) * (-1) * 1 = -1$.
3. Comme $2017 = 12 * 168 + 1 \equiv 1\,[12]$, on a $\sigma^{2017} = \sigma$.

Exercice 3
1. $\overline{29} * \overline{2} = \overline{58} = \overline{0}\,[58]$, donc A n'est pas intègre.
2. On calcule l'indicatrice d'Euler $\varphi(58) = \varphi(2 * 29) = (2 - 1) * (29 - 1) = 28$, le cardinal de $A^\times$ est donc 28.
3. Comme le groupe $(A^\times, *)$ est d'ordre 28, l'odre de $\overline{3}$ divise $28 = 2^2 * 7$ par le

théorème de Lagrange. C'est donc soit $1, 2, 4, 7, 14$ ou 28. On calcule donc

$$\bar{3}^1 = \bar{3} \neq \bar{1},\ \bar{3}^2 = \bar{9} \neq \bar{1},\ \bar{3}^4 = \overline{81} = \overline{23} \neq \bar{1},$$

$$\bar{3}^7 = \bar{3}^4 * \bar{3}^2 * \bar{3} = \overline{23} * \overline{27} = \overline{621} = \overline{580} + \overline{41} = -\overline{17} \neq \bar{1},$$

$$\bar{3}^{14} = (\bar{3}^7)^2 = \overline{17}^2 = \overline{289} = \overline{5 * 58 - 1} = -\bar{1} \neq \bar{1}.$$

D'après les calculs précédents, l'ordre n'est pas $1, 2, 4, 7$ ni 14, c'est donc 28.
4. Oui, le groupe est cyclique, car il est fini et $\bar{3}$ est un générateur (son ordre est celui du groupe).

Problème

Soit $\omega = \frac{1+\sqrt{5}}{2}$. On note

$$K = \{a + b\omega \ :\ (a, b) \in \mathbf{Q}^2\},$$

et

$$\mathcal{O} = \{a + b\omega \ :\ (a, b) \in \mathbf{Z}^2\}.$$

1. $1 = 1 + 0\omega$ donc $1 \in K$. Soient $(x, y) \in K^2$, il existe a, b, c, d des rationnels tels que $x = a + b\omega$, $y = c + d\omega$. On a alors

$$x - y = (a + b\omega) - (c + d\omega) = (a - c) + (b - d)\omega \in K,$$

car $a - c$ et $b - d$ sont bien des rationnels. Enfin,

$$xy = (a + b\omega)(c + d\omega) = ac + (bc + ad)\omega + bd\omega^2,$$

on calcule donc

$$\omega^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1 + 5 + 2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \omega.$$

On a ainsi

$$xy = (ac + bd) + (bc + ad + bd)\omega,$$

et comme $ac+bd$ et $bc+ad+bd$ sont rationnels, $xy \in K$. L'ensemble K contient 1, est stable par différence et produit, c'est donc un sous-anneau de $\mathbf{R}$. Comme $\mathbf{R}$ est intègre, K aussi.

2. On procède de même. $1 = 1 + 0\omega$ donc $1 \in \mathcal{O}$. Soient $(x, y) \in \mathcal{O}^2$, il existe a, b, c, d des entiers relatifs tels que $x = a + b\omega$, $y = c + d\omega$. On a alors

$$x - y = (a + b\omega) - (c + d\omega) = (a - c) + (b - d)\omega \in \mathcal{O},$$

car $a - c$ et $b - d$ sont dans $\mathbf{Z}$. Enfin,

$$xy = (ac + bd) + (bc + ad + bd)\omega,$$

et comme $ac + bd$ et $bc + ad + bd$ sont dans $\mathbf{Z}$ (somme et produit d'entiers relatifs), $xy \in \mathcal{O}$.

3. Soit $x \in K$ et a, b, a', b' deux écritures

$$x = a + b\omega = a' + b'\omega.$$

Alors

$$(a - a') + \frac{1}{2}(b - b') = \frac{\sqrt{5}}{2}(b' - b),$$

ou encore

$$\sqrt{5}(b' - b) = 2(a - a') + (b - b').$$

Si $b \neq b'$, alors

$$\sqrt{5} = \frac{2(a - a') + (b - b')}{b' - b},$$

qui est un rationnel car a, a', b, b' le sont. C'est absurde. Donc $b = b'$, et comme $a + b\omega = a' + b\omega$, on a aussi $a = a'$. D'où l'unicité de l'écriture.
Attention : Il est faux de penser qu'un nombre s'écrit de façon unique comme somme d'un rationnel et d'un irrationnel !! (contrexemple ?)
4.

$$\omega' = \frac{1 - \sqrt{5}}{2} = 1 - \omega \in \mathcal{O}.$$

5. Tout d'abord,

$$\sigma(1) = \sigma(1 + 0.\omega) = 1 + 0.\omega' = 1.$$

Soient $(x, y) \in K^2$. Par définition de K, il existe $(a, b, c, d) \in \mathbf{Q}^4$ avec $x = a + b\omega$, $y = c + d\omega$.

$$\sigma(x + y) = \sigma((a + c) + (b + d)\omega) = (a + c) + (b + d)\omega'.$$

D'un autre côté, on a

$$\sigma(x) + \sigma(y) = (a + b\omega') + (c + d\omega') = \sigma(x + y).$$

Pour le produit,

$$\sigma(xy) = \sigma((ac + bd) + (bc + ad + bd)\omega) = (ac + bd) + (bc + ad + bd)\omega',$$

et

$$\sigma(x)\sigma(y) = (a + b\omega')(c + d\omega') = ac + (bc + ad)\omega' + bd\omega'^2,$$

et on doit alors calculer

$$\omega'^2 = \left(\frac{1 - \sqrt{5}}{2}\right)^2 = \frac{1 + 5 - 2\sqrt{5}}{4} = \frac{3 - \sqrt{5}}{2} = 1 + \omega'.$$

Ainsi

$$\sigma(x)\sigma(y) = (ac + bd) + (bc + ad + bd)\omega' = \sigma(xy).$$

Ce qui prouve que σ est un morphisme d'anneaux. Pour montrer que c'est une involution, on calcule

$$\sigma(\sigma(x)) = \sigma(\sigma(a + b\omega)) = \sigma(a + b\omega') = \sigma(a + b(1 - \omega)) = \sigma((a + b) - b\omega),$$

$$\sigma(\sigma(x)) = (a + b) - b\omega' = (a + b) - b(1 - \omega) = a + b\omega = x.$$

Donc $\sigma^2 = Id_K$, c'est bien une involution.

6. On procède d'abord par condition nécessaire. Soit ψ un morphisme d'anneau de K dans K. Comme $\psi(1) = 1$, on a $\psi(n) = n$ pour tout entier n, et par suite pour tout entiers p, q, on a $q\psi(p/q) = \psi(p) = p$, et donc ψ est l'identité sur $\mathbf{Q}$. Comme

$$\psi(a + b\omega) = \psi(a) + \psi(b)\psi(\omega) = a + b\psi(\omega),$$

il suffit de connaître $\psi(\omega)$ pour connaître ψ. Or,

$$\omega^2 - \omega - 1 = 0,$$

Donc

$$\psi(\omega)^2 - \psi(\omega) - 1 = 0,$$

car ψ est un morphisme d'anneaux. Le nombre $\psi(\omega)$ est donc l'une des deux racines de $X^2 - X - 1$, qui sont justement ω et ω'. Si $\psi(\omega) = \omega$, alors ψ est simplement l'identité sur K. Sinon, $\psi(\omega) = \omega'$, et alors

$$\psi(a + b\omega) = a + b\omega' = \sigma(a + b\omega).$$

On en conclut donc que ψ est nécessairement soit Id_K, soit σ. Réciproquement, ce sont bien deux morphismes d'anneaux de K dans K.

7. Pour $x = a + b\omega$, $(a, b) \in \mathbf{Q}^2$, on calcule

$$N(x) = (a + b\omega)(a + b\omega') = a^2 + b^2\omega\omega' + ab(\omega + \omega'),$$

et on calcule $\omega\omega' = \frac{1+\sqrt{5}}{2}\frac{1-\sqrt{5}}{2} = \frac{1-5}{4} = -1$, $\omega + \omega' = \frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2} = 1$. Ainsi,

$$N(x) = a^2 + ab - b^2,$$

qui est bien un rationnel car a, b le sont. Si a, b sont entiers relatifs, $a^2 + ab - b^2$ également.

8. Montrons que K est un corps, càd que tout $x \in K$ non nul a un inverse dans K. Soit donc $x = a + b\omega$, avec a, b deux rationnels qui ne sont pas tous les deux nuls. On a

$$x\sigma(x) = N(x),$$

et donc

$$x\frac{\sigma(x)}{N(x)} = 1,$$

pourvu que $N(x) \neq 0$. Or, $\sigma(x) \neq 0$ car σ est une involution (sinon on aurait $x = \sigma(\sigma(x)) = \sigma(0) = 0$). Donc on a bien $N(x) = x\sigma(x) \neq 0$.
Il suffit donc de voir que $\frac{\sigma(x)}{N(x)} \in K$ pour conclure que x est inversible. Or,

$$\frac{\sigma(x)}{N(x)} = \frac{a - b}{a^2 + ab - b^2} - \frac{b}{a^2 + ab - b^2}\omega,$$

qui est bien à coefficients rationnels car a, b le sont, et donc dans K.

9. Soient $(x, y) \in K^2$, on a $N(xy) = xy\sigma(xy) = xy\sigma(x)\sigma(y) = N(x)N(y)$.

10. Soient $(a, b) \in \mathbf{Q}^2$ avec $|a| \leq 1/2$, $|b| \leq 1/2$. On a

$$|N(a + b\omega)| = |a^2 + ab - b^2| \leq |a|^2 + |ab| + |b^2| \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} \leq \frac{3}{4} < 1.$$

11. Soient x, y deux éléments de $\mathcal{O}$, avec y non nul. Comme K est un corps, x/y est dans K, de la forme $u + v\omega$, avec u, v deux rationnels. On choisit deux entiers relatifs c, d avec $|u - c| \leq 1/2$, $|v - d| \leq 1/2$, et on pose

$$q = c + d\omega \in \mathcal{O},\ r = x - qy \in \mathcal{O}.$$

D'après la question 10, $|N(r/y)| = |N((u - c) + (v - d)\omega)| < 1$. Donc

$$|N(r)| < |N(y)|,$$

et

$$x = qy + r.$$

ce qui donne une division euclidienne de x par y, dans $\mathcal{O}$.

12. Soient $(a, b) \in \mathbf{Z}^2$.

$$(a - 2b)^2 = a^2 + 4b^2 - 4ab \equiv a^2 - b^2 + ab \equiv N(a + b\omega) \bmod 5.$$

13. D'après la question précédente, l'entier $N(x)$ est un carré modulo 5 (le carré de $a - 2b$). Les carrés modulo 5 étant $0, 1, 4$, ce ne peut être 2 ni 3.

14. On procède par condition nécessaire et suffisante. Soit $x \in \mathcal{O}$ un inversible. Alors il existe $y \in \mathcal{O}$ avec $xy = 1$. En prenant la norme,

$$N(xy) = 1,$$

d'où $N(x)N(y) = 1$. Mais c'est un produit dans $\mathbf{Z}$, donc $N(x)$ est inversible dans $\mathbf{Z}$ donc -1 ou 1.
Réciproquement, soit x de norme 1 ou -1. On peut le réinterpréter comme

$$x\sigma(x) = \pm 1.$$

donc l'inverse de x est $\pm\sigma(x)$.

15. Soit p un entier premier (de $\mathbf{Z}$) congru à 2 ou 3 modulo 5. Soit $p = uv$, avec $u, v \in \mathcal{O}^2$, une décomposition de p comme produit. On veut montrer que u ou v est inversible, càd de norme ± 1. Prenons les normes:

$$N(p) = N(u)N(v),$$

ou encore

$$p^2 = N(u)N(v).$$

Ce produit a lieu dans $\mathbf{Z}$, donc les possibilités pour le couple $\{N(u), N(v)\}$ sont $\{\pm 1, \pm p^2\}$ ou $\{\pm p, \pm p\}$. Mais ce dernier cas ne peut se produire, car

$$N(u) \equiv \pm p \equiv \pm 3 \equiv \mp 2\,[5]$$

n'a pas de solution d'après la question 13. Donc soit $N(u)$, soit $N(v)$ vaut ± 1, et u ou v est inversible d'arpès la question 14. Donc p est irréductible dans $\mathcal{O}$.

Complément culturel : La réciproque est également vraie, mais un peu plus dure à établir : si p est congru à 1 ou 4 modulo 5, p n'est pas irréductible.