UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Corrigé de l'examen final (première session)

Exercice 1

Supposons $x \leqslant 0$, de sorte que $|x-1| = 1-x$ et $|x| = -x$. L'inéquation se réécrit donc $1-2\,x < 3$ ce qui équivaut à $2\,x > -2$ soit encore $x > -1$.

Supposons $0 < x \leqslant 1$ de sorte que $|x-1| = 1-x$ et $|x| = x$. L'inéquation se réécrit donc $1 < 3$ ce qui est toujours vérifié quel que soit la valeur de x.

Supposons $x > 1$, de sorte que $|x-1| = x-1$ et $|x| = x$. L'inéquation se réécrit donc $2\,x - 1 < 3$ ce qui équivaut à $2\,x < 4$ soit encore $x < 2$.

Ainsi l'ensemble des solutions de l'inéquation est la réunion des trois ensembles $]-1,0]$, $]0,1]$ et $]1,2[$: c'est donc $]-1,2[$.

Exercice 2

1 On a $\sigma = (1,4)\,(2,6,5,7)$ et $\sigma^{-1} = (1,4)\,(7,5,6,2)$.

2 On a $\sigma^2 = (1,4)^2\,(2,6,5,7)^2 = (2,5)\,(6,7)$ et $\sigma^4 = (\sigma^2)^2 = (2,5)^2\,(6,7)^2 = \mathrm{Id}$. L'ordre de σ divise donc 4, or $\sigma \neq \mathrm{Id}$ et $\sigma^2 \neq \mathrm{Id}$ donc l'ordre de σ est 4.

3 On a $\sigma^3 = \sigma^{-1} = (1,4)\,(7,5,6,2)$. Pour $n \geqslant 1$, soit $n = 4\,q + r$ la division euclidienne de n par 4. On a alors

$$\sigma^n = \sigma^{4\,q}\,\sigma^r = (\sigma^4)^q\,\sigma^r = \mathrm{Id}^q\ \sigma^r = \sigma^r.$$

On en déduit

$$\sigma^n = \begin{cases} \mathrm{Id} & \text{si } n \equiv 0\,[4] \\ \sigma = (1,4)\,(2,6,5,7) & \text{si } n \equiv 1\,[4] \\ \sigma^2 = (2,5)\,(6,7) & \text{si } n \equiv 2\,[4] \\ \sigma^3 = (1,4)\,(7,5,6,2) & \text{si } n \equiv 3\,[4] \end{cases}$$

Exercice 3

1 On a

$$\frac{3+5\,i}{3+3\,i} = \frac{(3+5\,i)(3-3\,i)}{3^2+3^2} = 1 + \frac{1}{3} + \frac{1}{3}i.$$

On constate alors que $N\left(\frac{3+5\,i}{3+3\,i} - 1\right) < 1$. Ainsi $3+5\,i = 1.(3+3\,i)+2\,i$ est une division euclidienne de $3+5\,i$ par $3+3\,i$ (quotient 1, reste $2\,i$).

On a

$$\frac{3+3\,i}{2\,i} = \frac{(3+3\,i).(-2\,i)}{2^2} = 1 - 2\,i + \frac{1}{2} + \frac{1}{2}i.$$

On constate alors que $N\left(\frac{3+3\,i}{2\,i} - (1-2\,i)\right) < 1$. Ainsi $3+3\,i = (1-2\,i).2\,i + (-1+i)$ est une division euclidienne de $3+3\,i$ par $2\,i$ (quotient $1-2\,i$, reste $-1+i$).

On a

$$\frac{2\,i}{-1+i} = \frac{2\,i.(-1-i)}{2} = 1 - i \in \mathbf{Z}[i].$$

Ainsi $2\,i = (1-i).(-1+i) + 0$ est une division euclidienne de $2\,i$ par $-1+i$ (quotient $1-i$, reste 0). Un pgcd de $3+5\,i$ et $3+3\,i$ est donné par le dernier reste non nul, soit $-1+i$ (les autres pgcd de $3+5\,i$ et $3+3\,i$ sont $-1-i$, $1+i$ et $1-i$).

2 z est non nul (car $N(z) \neq 0$) et non inversible (car $N(z) \neq 1$). Si on a $z = z_1\, z_2$ avec z_1, $z_2 \in \mathbf{Z}[i]$, on en déduit $N(z) = N(z_1\, z_2)$ soit $p = N(z_1)\, N(z_2)$. Comme p est premier et que $N(z_1)$ et $N(z_2)$ sont des entiers positifs, cette dernière égalité entraîne nécessairement $N(z_1) = 1$ ou $N(z_2) = 1$, soit $z_1 \in \mathbf{Z}[i]^\times$ ou $z_2 \in \mathbf{Z}[i]^\times$. Ainsi z est bien irréductible.
3 Par hypothèse on a $z' = u\, z$ avec $u \in \mathbf{Z}[i]$, d'où $N(z') = N(u)\, N(z)$ Comme z et z' sont non nuls, $N(z) = N(z')$ est non nul et on en déduit $N(u) = 1$. Ainsi $u \in \mathbf{Z}[i]^\times$, d'où le résultat.
4 Par hypothèse, $a^2 + b^2 = N(a + i\, b) = p$ donc $a + i\, b$ est irréductible. Par ailleurs l'égalité $a^2 + b^2 = \alpha^2 + \beta^2$ se réécrit

$$(a + i\, b)(a - i\, b) = (\alpha + i\, \beta)\, (\alpha - i\, \beta).$$

En particulier l'élément irréductible $a + i\, b$ divise le produit $(\alpha + i\, \beta)\, (\alpha - i\, \beta)$. On en déduit que $a + i\, b$ divise soit $\alpha + i\, \beta$, soit $\alpha - i\, \beta$.
5 Soit $(\alpha, \beta) \in \mathbf{Z}^2$ vérifiant $\alpha^2 + \beta^2 = p$. D'après la question précédente, $a + i\, b$ divise soit $\alpha + i\, \beta$, soit $\alpha - i\, \beta$. Supposons que $a + i\, b$ divise $\alpha + i\, \beta$. Comme $N(a + i\, b) = N(\alpha + i\, \beta) = p$, d'après la question 3, il existe $u \in \mathbf{Z}[i]^\times$ tel que $\alpha + i\, \beta = u\, (a + i\, b)$ Comme $\mathbf{Z}[i]^\times = \{1, -1, i, -i\}$, on en déduit facilement qu'on a soit $(|\alpha|\,, |\beta|) = (|a|\,, |b|)$, soit $(|\alpha|\,, |\beta|) = (|b|\,, |a|)$. La même conclusion vaut si $a + i\, b$ divise $\alpha - i\, \beta$.

Réciproquement, si (α, β) vérifie soit $(|\alpha|\,, |\beta|) = (|a|\,, |b|)$, soit $(|\alpha|\,, |\beta|) = (|b|\,, |a|)$, il est clair qu'on a $\alpha^2 + \beta^2 = a^2 + b^2 = p$.

Finalement l'ensemble des solutions de l'équation $\alpha^2 + \beta^2 = p$ est

$$\{(a, b),\, (-a, b),\, (a, -b),\, (-a, -b), (b, a),\, (-b, a),\, (b, -a),\, (-b, -a)\}$$

Il y a donc 8 solutions (rappelons que p est supposé impair, donc nécessairement $|a| \neq |b|$).

Exercice 4
1 Si $[n]_N \in (\mathbf{Z}/N\mathbf{Z})^\times$, il existe $m \in \mathbf{Z}$ tel que $[n]_N[m]_N = [1]_N$ soit $[n.m]_N = [1]_N$ soit $[n.m - 1]_N = [0]_N$ soit N divise $n.m - 1$. Il existe donc $q \in \mathbf{Z}$ tel que $n.m + N.q = 1$, donc n et N sont premiers entre eux.

Si n et N sont premiers entre eux, il existe $(m, q) \in \mathbf{Z}^2$ tel que $n.m + N.q = 1$, d'où $[n.m + N.q]_N = [1]_N$, d'où $[n]_N[m]_N = [1]_N$. Ainsi $[n]_N \in (\mathbf{Z}/N\mathbf{Z})^\times$.
2 D'après la question précédente, on a $(\mathbf{Z}/4\mathbf{Z})^\times = \{[1]_4, [3]_4\}$. C'est un groupe d'ordre 2, en particulier c'est un groupe cyclique.
3 D'après la question 1, on a $(\mathbf{Z}/9\mathbf{Z})^\times = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$. C'est un groupe d'ordre 6. On constate que $[2]_9$, $[4]_9 = [2]_9^2$ et $[8]_9 = [2]_9^3$ sont tous distincts de $[1]_9$. Ainsi l'ordre de $[2]_9$, qui doit diviser 6, est 6 et $(\mathbf{Z}/9\mathbf{Z})^\times$ est cyclique. On pouvait alternativement invoquer le résultat du cours qui dit que tout groupe d'ordre 6 commutatif est cyclique.
4 p ne divise pas $1 + p$ (sinon p diviserait 1) et a fortiori p^2 ne divise pas $1 + p$. Comme 1, p et p^2 sont les diviseurs positifs de p^2, on a $\mathrm{pgcd}(1 + p, p^2) = 1$ donc $x \in (\mathbf{Z}/p^2\mathbf{Z})^\times$ d'après la question 1.

D'après la formule du binôme de Newton, on a $(1+p)^p = 1+p.p+\sum_{k=2}^{p} \binom{p}{k} p^k$ d'où on déduit aussitôt $(1 + p)^p \equiv 1\ [p^2]$ ce qui se réécrit $x^p = [1]_{p^2}$. Ainsi l'ordre de x divise p. Mais comme p est premier et qu'on a visiblement $x \neq [1]_{p^2}$ (p^2 ne divise pas p), l'ordre de x est p.
5 Par hypothèse p et n sont premiers entre eux. En particulier ni p ni a fortiori p^2 ne divisent n. On en déduit aussitôt que p^2 et n sont premiers entre eux, donc $[n]_{p^2} \in (\mathbf{Z}/p^2\mathbf{Z})^\times$.

Soit $k \geqslant 1$ tel que $[n]_{p^2}^k = [1]_{p^2}$. Ainsi p^2 divise $n^k - 1$, donc p divise $n^k - 1$, donc $[n]_p^k = [1]_p$. De cette dernière égalité on déduit que r divise k. En particulier r divise l'ordre de $[n]_{p^2}$.
6 On sait que le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est d'ordre $p - 1$ et cyclique. Il existe donc $n \in \mathbf{Z}$ tel que $[n]_p$ est d'ordre $p - 1$ dans $(\mathbf{Z}/p\mathbf{Z})^\times$. D'après la question précédente, $y = [n]_{p^2}$ convient.

7 Le sous-groupe G de $(\mathbf{Z}/p^2\mathbf{Z})^\times$ engendré par y est un groupe cyclique de cardinal l'ordre de y. Cet ordre est divisible par $p-1$. D'après le résultat rappelé en préambule, G possède un élément d'ordre $p-1$, donc $(\mathbf{Z}/p^2\mathbf{Z})^\times$ également.

Alternativement on pouvait donner l'argument suivant (qui revient en fait à redémontrer le résultat rappelé en préambule) : écrivons l'ordre de y sous la forme $k\,(p-1)$, avec k entier positif. Alors il est clair que $(y^k)^{p-1} = y^{k\,(p-1)} = [1]_{p^2}$ et que pour tout $1 \leqslant \ell < k$ on a $(y^\ell)^{p-1} = y^{\ell\,(p-1)} \neq [1]_{p^2}$ car $\ell\,(p-1) < k\,(p-1)$. Ainsi $z = y^k$ est un élément d'ordre $p-1$.

8

1. Ceci découle aussitôt de la relation $(g^n)^{d_1} = (g^{d_1})^n = e$.
2. On a
$$(g\,h)^{d_1\,d_2} = g^{d_1\,d_2} h^{d_1\,d_2} = \left(g^{d_1}\right)^{d_2} \left(h^{d_2}\right)^{d_1} = e^{d_2}\,e^{d_1} = e$$
ce qui montre le résultat.
3. On a $g^n = h^{-n}$. Soit r l'ordre de cet élément. D'après la question 8.1, r en tant qu'ordre de g^n divise d_1 et en tant qu'ordre de h^{-n} divise d_2. Comme d_1 et d_2 sont premiers entre eux, on a $r = 1$.
4. Soit $n \geqslant 1$ tel que $(g\,h)^n = g^n\,h^n = 1$. D'après la question précédente, g^n et h^n sont d'ordre 1, donc $g^n = e$ et $h^n = e$. Ainsi d_1 divise n et d_2 divise n. En particulier d_1 et d_2 divisent l'ordre de $g\,h$. Comme d_1 et d_2 sont premiers entre eux, $d_1\,d_2$ divisent l'ordre de $g\,h$. D'après la question 8.2, $g\,h$ est d'ordre $d_1\,d_2$

9 D'après la question 4, $(\mathbf{Z}/p^2\mathbf{Z})^\times$ possède un élément x d'ordre p. D'après la question 7, $(\mathbf{Z}/p^2\mathbf{Z})^\times$ possède un élément y d'ordre $p-1$. Or $p-1$ et p sont premiers entre eux. Comme $(\mathbf{Z}/p^2\mathbf{Z})^\times$ est commutatif, d'après la question 8, $x\,y$ est d'ordre $p\,(p-1)$.

10 D'après la question précédente, il suffit de montrer que le cardinal de $(\mathbf{Z}/p^2\mathbf{Z})^\times$ est $p.(p-1)$. Or on a
$$\#(\mathbf{Z}/p^2\mathbf{Z})^\times = \{n \in \{0,1,\ldots,p^2-1\}, \quad \mathrm{pgcd}(n,p^2) = 1\}.$$
Les diviseurs positifs de p^2 étant 1, p et p^2, on voit que pour $n \in \{0,1,\ldots,p^2-1\}$ la condition $\mathrm{pgcd}(n,p^2) = 1$ équivaut à « p ne divise pas n ». Or
$$\{n \in \{0,1,\ldots,p^2-1\}, \quad p|n\} = \{k\,p, \quad k \in \{0,\ldots,p-1\}\}$$
et
$$\#(\mathbf{Z}/p^2\mathbf{Z})^\times = p^2 - \#\{k\,p, \quad k \in \{0,\ldots,p-1\}\} = p^2 - p = p.(p-1)$$
d'où le résultat.