UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Corrigé de l'examen final (seconde session)

Exercice 1

Un des exemples les plus simples est certainement le suivant : posons, pour tout $x \in \mathbf{R}$, $f(x) = |x|$. Alors f est une fonction de $\mathbf{R}$ dans $\mathbf{R}$, continue sur $\mathbf{R}$. Cependant f n'est pas dérivable en 0. En effet dire que f est dérivable en 0 équivaut à dire que la quantité (définie pour $x \neq 0$)

$$\frac{f(x) - f(0)}{x - 0} = \frac{|x|}{x}$$

admet une limite quand x tend vers 0. Or pour $x > 0$ on a $\frac{|x|}{x} = 1$ donc

$$\lim_{\substack{x \to 0 \\ x > 0}} \frac{|x|}{x} \text{ existe et vaut } 1.$$

Pour $x > 0$ on a $\frac{|x|}{x} = -1$ donc

$$\lim_{\substack{x \to 0 \\ x < 0}} \frac{|x|}{x} \text{ existe et vaut } -1.$$

Comme $1 \neq -1$, on en déduit que $\frac{|x|}{x}$ n'admet pas de limite quand x tend vers 0.

Exercice 2

1 On a

$$\sigma = (1, 2, 7)\,(3, 5)$$

et (par exemple)

$$\sigma = (1, 7)\,(1, 2)\,(3, 5).$$

Comme σ s'écrit comme le produit d'un nombre impair de transpositions, on a $\varepsilon(\sigma) = -1$.

2 C'est une question de cours. La formule de conjugaison nous dit qu'on a

$$\tau\sigma\tau^{-1} = (\tau(1), \tau(2), \tau(7))\,(\tau(3), \tau(5))$$

3 Si τ est une transposition, on a $\tau^2 = \mathrm{Id}$ d'où $\tau = \tau^{-1}$ et l'égalité $\tau\sigma = \sigma\tau$ équivaut à $\tau\sigma\tau^{-1} = \sigma$. D'après les questions précédentes, ceci équivaut à

$$(1, 2, 7)\,(3, 5) = (\tau(1), \tau(2), \tau(7))\,(\tau(3), \tau(5)).$$

Par unicité de la décomposition en produit de cycles à supports disjoints, ceci équivaut à

$$(1, 2, 7) = (\tau(1), \tau(2), \tau(7)) \text{ et } (3, 5) = (\tau(3), \tau(5)) \quad (*)$$

On a en particulier $\{3, 5\} = \{\tau(3), \tau(5)\}$, donc soit $\tau(3) = 5$ et $\tau(5) = 3$, soit $\tau(3) = 3$ et $\tau(5) = 5$. Dans le premier cas, comme τ est une transposition, on a $\tau = (3, 5)$ et $(*)$ est alors vérifiée. Dans le deuxième cas, on utilise le fait que $(*)$ entraîne également $\{1, 2, 7\} = \{\tau(1), \tau(2), \tau(7)\}$. Premier sous-cas : τ fixe les trois éléments 1, 2 et 7. Comme τ est une transposition, on a nécessairement

$\tau = (4,6)$, et dans ce cas $(*)$ est vérifiée. Deuxième sous-cas : au moins un des éléments 1, 2 ou 7 n'est pas fixé par τ. Dans ce cas τ permute nécessairement deux éléments parmi 1, 2 et 7 et fixe le troisième. Mais on vérifie alors aussitôt que l'égalité $(1,2,7) = (\tau(1), \tau(2), \tau(7))$ n'est *pas* vérifiée (par exemple $\tau = (2,7)$, or $(1,2,7) \neq (1,7,2)$)

Conclusion : les transpositions τ qui commutent à σ sont $(3,5)$ et $(4,6)$.

Exercice 3

1 On a

$$\frac{113}{15+i} = \frac{113(15-i)}{15^2+1^2} = \frac{1695-113\,i}{226} = 7 - i + \frac{1}{2} + \frac{1}{2}i.$$

On constate alors que $N\left(\frac{113}{15+i} - (7-i)\right) < 1$. Ainsi $113 = (7-i)(15+i) + 7 + 8\,i$ est une division euclidienne de 113 par $15+i$ (quotient $7-i$, reste $7+8\,i$).

On a

$$\frac{15+i}{7+8\,i} = \frac{(15+i)(7-8\,i)}{7^2+8^2} = \frac{113-113\,i}{113} = 1-i$$

Ainsi $15 + i = (7+8\,i)(1-i)$ est une division euclidienne de $15+i$ par $7+8\,i$ (quotient $1-i$, reste 0).

Un pgcd de 113 et $15+i$ est donné par le dernier reste non nul, soit $7+8\,i$.

2 On a $113 \equiv 1\,[4]$. En calculant la norme du pgcd trouvé à la question précédente, on sait donc qu'on obtient une décomposition de 113 en somme de deux carrés, plus précisément $113 = 7^2 + 8^2$ (relation qui apparaissait déjà dans les calculs de la question précédente).

3 On a $113 = 2^4.7 + 1$. On commence par calculer 2^7 modulo 4. Pour cela, on peut utiliser l'écriture binaire $7 = 2^2 + 2 + 1$. On a $2^2 \equiv 4\,[113]$ et $(2^2)^2 \equiv 4^2 \equiv 16\,[113]$, d'où $2^7 = (2^2)^2.2^2.2 \equiv 16.4.2 \equiv 128 \equiv 15\,[113]$. On a donc $2^7 \neq 1\,[113]$. On calcule alors 15^2 modulo 113 et on trouve $15^2 \equiv -1\,[113]$.

4 Si $z \in \mathbf{Z}[i]$ s'écrit $a + i\,b$ avec $a, b \in \mathbf{Z}$ on a $N(z) = a^2 + b^2$. On constate donc aussitôt que les éléments de $\mathscr{C}_2$ sont exactement les éléments de $\mathbf{N}$ qui s'écrivent $N(z)$ avec $z \in \mathbf{Z}[i]$. Comme le produit de deux éléments de $\mathbf{Z}[i]$ en est encore un ($\mathbf{Z}[i]$ est un sous-anneau de $\mathbf{C}$), la relation $N(z_1\,z_2) = N(z_1)\,N(z_2)$ pour $z_1, z_2 \in \mathbf{Z}[i]$ donne le premier résultat.

Par ailleurs si on écrit $z_1 = a + i\,b$ et $z_2 = c + i\,d$, avec $a, b, c, d \in \mathbf{Z}$, on a

$$z_1\,z_2 = (ac - bd) + i\,(bc + ad)$$

et la relation $N(z_1\,z_2) = N(z_1)N(z_2)$ s'écrit

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

5 On a $565 = 5.113$ avec $5 = 2^2 + 1^2$ et $113 = 7^2 + 8^2$. Ainsi

$$565 = (2^2+1^2)(7^2+8^2) = (2.7 - 1.8)^2 + (1.7 + 2.8)^2 = 6^2 + 23^2$$

6 Par une récurrence immédiate, on déduit de la question 4 que le produit d'un nombre fini d'éléments de $\mathscr{C}_2$ est encore dans $\mathscr{C}_2$. Soit à présent n un entier comme dans l'énoncé et $\mathscr{P}_n$ l'ensemble des diviseurs premiers de n. La décomposition en facteurs premiers de n s'écrit

$$n = \prod_{p \in \mathscr{P}_n} p^{v_p(n)} \quad (*)$$

Pour $p \in \mathscr{P}_n$ tel que $p = 2$ ou $p \equiv 1\,[4]$, on sait (cours) que $p \in \mathscr{C}_2$ et donc $p^{v_p(n)} \in \mathscr{C}_2$.

Pour $p \in \mathscr{P}_n$ tel que $p \equiv 3\,[4]$, par hypothèse $v_p(n)$ est pair. Ainsi $p^{v_p(n)}$ est le carré d'un entier, et le carré d'un entier est dans $\mathscr{C}_2$ ($a^2 = a^2 + 0^2$!). $(*)$ exprime donc n comme le produit d'un nombre fini d'éléments de $\mathscr{C}_2$, et ainsi $n \in \mathscr{C}_2$.

7 Indication : utiliser la description des éléments irréductibles de $\mathbf{Z}[i]$ et la décomposition en éléments irréductibles dans $\mathbf{Z}[i]$ (*cf.* TD)

Exercice 4

1 On a

$$(x + \alpha\, a)^2 - \alpha^2\, \Delta = x^2 + 2\,\alpha\, a\, x + \alpha^2\, a^2 - \alpha^2\, \Delta = x^2 + a\, x + (2\,\alpha)^2\, b = x^2 + a\, x + b.$$

L'équation $x^2 + a\, x + b = 0$ équivaut donc à $[x + \alpha\, a]^2 = \alpha^2\, \Delta$ ou encore $[2(x + \alpha\, a)]^2 = \Delta$. Si elle admet une solution x, on voit donc aussitôt que Δ est un carré dans $\mathbf{F}_p$.

Réciproquement, si $\Delta = \delta^2$, l'équation équivaut à $[x + \alpha\, a]^2 = (\alpha\, \delta)^2$, en particulier tout x vérifiant $x + \alpha\, a = \alpha\, \delta$ est solution. Ainsi il y a au moins une solution, à savoir $x = \alpha(\delta - a)$.

2 Pour $p = 2$, on a $-3 \equiv 1\,[2]$ soit $-3 \equiv 1^2\,[2]$. Pour $p = 3$, on a $-3 \equiv 0\,[3]$ soit $-3 \equiv 0^2\,[3]$.

3 Comme 3 est premier, $\mathbf{F}_p^\times$ admet un élément x d'ordre 3 si et seulement si il existe $x \in \mathbf{F}_p \backslash \{[1]_p\}$ vérifiant $x^3 = [1]_p$ si et seulement si (d'après l'identité de l'énoncé) il existe $x \in \mathbf{F}_p \backslash \{[1]_p\}$ vérifiant $x^2 + x + [1]_p = 0$.

Or, comme on a $p \neq 3$, $[1]_p$ n'est pas solution de l'équation $x^2 + x + [1]_p = 0$. Ainsi il existe $x \in \mathbf{F}_p \backslash \{[1]_p\}$ vérifiant $x^2 + x + [1]_p = 0$ si et seulement si il existe $x \in \mathbf{F}_p$ vérifiant $x^2 + x + [1]_p = 0$

Pour l'équation $x^2 + x + [1]_p = 0$, on a $\Delta = [-3]_p$. D'après la première question, comme on a $p \neq 2$, $\mathbf{F}_p^\times$ admet un élément x d'ordre 3 si et seulement si -3 est un carré modulo p.

Par ailleurs, $\mathbf{F}_p^\times$ étant un groupe cyclique (d'ordre $p - 1$), il admet un élément d'ordre 3 si et seulement si 3 divise son ordre si et seulement si p est congru à 1 modulo 3.

Exercice 5

1 g est d'ordre fini si et seulement si il existe $n \geqslant 1$ tel que $g^n = e$. L'ordre de g est alors le plus petit élément de la partie de $\mathbf{N}$ non vide $\{n \in \mathbf{N},\, n \geqslant 1,\, g^n = e\}$.

Alternativement on peut éventuellement prendre comme définition (mais dans le cours c'était vu comme une propriété) : g est d'ordre fini si le sous-groupe engendré par g est fini ; l'ordre de g est alors le cardinal du sous-groupe engendré par g.

2 Dans toute la suite de l'exercice, on considère un élément $g \in G$ d'ordre fini α. Soit $m \in \mathbf{Z}$. Montrer qu'on a $g^m = e$ si et seulement si α divise m.

Si $m = n\,\alpha$ avec $n \in \mathbf{Z}$ alors $g^m = (g^\alpha)^n = e^n = e$.

Si $g^m = e$, soit $m = q\,\alpha + r$ la division euclidienne de m par α (on a $\alpha \neq 0$). On a alors $e = g^m = g^{q\,\alpha + r} = (g^\alpha)^q\, g^r = e^q\, g^r = g^r$. On a donc $g^r = e$ avec $0 \leqslant r < \alpha$ et par définition de l'ordre $r = 0$. Ainsi α divise m.

3 On a $(g^n)^{\frac{\alpha}{\operatorname{pgcd}(n,\alpha)}} = g = g^{\operatorname{ppcm}(n,\alpha)}$. D'après la question précédente, $g^{\operatorname{ppcm}(n,\alpha)} = e$. Ainsi g est d'ordre fini et toujours d'après la question précédente son ordre β divise $\frac{\alpha}{\operatorname{pgcd}(n,\alpha)}$.

4 On a $e = (g^n)^\beta = g^{n\,\beta}$. D'après la question 2, α, l'ordre de g, divise donc $n\,\beta$. On en déduit que $\frac{\alpha}{\operatorname{pgcd}(n,\alpha)}$ divise $\frac{n}{\operatorname{pgcd}(n,\alpha)}\,\beta$. Comme $\frac{\alpha}{\operatorname{pgcd}(n,\alpha)}$ et $\frac{n}{\operatorname{pgcd}(n,\alpha)}$ sont premiers entre eux, le lemme de Gauss permet de conclure que $\frac{\alpha}{\operatorname{pgcd}(n,\alpha)}$ divise β.

Comme d'après la question précédente on a aussi que β divise $\frac{\alpha}{\operatorname{pgcd}(n,\alpha)}$, on en déduit bien qu'on a $\beta = \frac{\alpha}{\operatorname{pgcd}(n,\alpha)}$.