UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Corrigé de l'examen terminal (première session)

Dans ce qui suit, le terme « poly » désigne la version du poly d'AR3 disponible au début du cours : rappelons que cette version a été régulièrement mise à jour au cours du semestre et que les deux versions (initiales et révisées) sont disponibles sur la page web du cours.

Exercice 1

Posons, pour tout $n \in \mathbf{N}$, $u_n = n + (-1)^n$. On définit ainsi bien une suite $(u_n)_{n\geqslant 0}$ à valeurs réelles.

Soit $n \in \mathbf{N}$. On a $u_{2\,n} = 2\,n + 1$ et $u_{2\,n+1} = 2\,n + 1 + (-1) = 2\,n$. Comme on a $1 > 0$, on a $2\,n + 1 > 2\,n$, d'où $u_{2\,n} > u_{2\,n+1}$. Ainsi on a bien, pour tout $n \geqslant 0$, $u_{2\,n} > u_{2\,n+1}$.

Montrons que $(u_n)_{n\geqslant 0}$ tend vers $+\infty$. Soit $n \in \mathbf{N}$. On a $(-1)^n \in \{-1, 1\}$, donc en particulier $(-1)^n \geqslant -1$. Ainsi on a $n + (-1)^n \geqslant n - 1$, soit $u_n \geqslant n - 1$. On a donc montré

$$\forall n \in \mathbf{N}, \quad u_n \geqslant n - 1.$$

Soit M un réel. De la propriété précédente, il découle aussitôt que pour tout entier naturel n satisfaisant $n \geqslant M + 1$, on a $u_n \geqslant M$. Par définition, ceci montre que $(u_n)_{n\geqslant 0}$ tend vers $+\infty$.

Commentaires : comme pour le reste du sujet, il ne fallait pas oublier de justifier ses réponses. Le « chapeau » du sujet était on ne peut plus clair à cet égard, n'oubliez pas de le lire.

Il y avait bien sûr de multiples exemples imaginables, celui qui est donné ici est sans doute l'un des plus simples. Pour la démonstration du fait que (u_n) tend vers $+\infty$, il était bien sûr licite d'utiliser les théorèmes de comparaison, mais on se trouve ici dans un cas où il est presque plus simple d'appliquer directement la définition.

Exercice 2

1. On se reportera au paragraphe 3.2 du poly d'AR1 (rappelons que le lien vers la page d'AR1 contenant le poly est donné dans le document de présentation d'AR3).
2. On se reportera à la démonstration du théorème 3.1 dans le poly.

Exercice 3

Voici la liste demandée, sous forme de couples (premier élément : un élément de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$, deuxième élément : son ordre)

$$(([0]_2, [0]_6), 1)\,;\ (([0]_2, [1]_6), 6)\,;\ (([0]_2, [2]_6), 3)\,;\ (([0]_2, [3]_6), 2)\,;\ (([0]_2, [4]_6), 3)\,;\ (([0]_2, [5]_6), 6)\,;$$

$$(([1]_2, [0]_6), 2)\,;\ (([1]_2, [1]_6), 6)\,;\ (([1]_2, [2]_6), 6)\,;\ (([1]_2, [3]_6), 2)\,;\ (([1]_2, [4]_6), 6)\,;\ (([1]_2, [5]_6), 6)$$

Le groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ est de cardinal $2 \times 6 = 12$. Il est donc cyclique si et seulement s'il possède un élément d'ordre 12. Or, d'après la liste précédente, il ne possède aucun élément d'ordre 12. Ainsi $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ n'est pas cyclique.

Commentaire : le théorème chinois énoncé dans le cours ne permet pas de répondre à la question, car il n'énonce qu'une condition suffisante pour qu'un groupe produit du type $\mathbf{Z}/M\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ soit cyclique ; l'objet d'un des exercices du deuxième examen partiel était de montrer que cette condition était également nécessaire ; ici il était inutile de faire appel à un tel résultat (qu'il aurait fallu en outre redémontrer, puisque ça n'est pas un résultat du cours)

Exercice 4

1. On se reportera au théorème 4.41 du poly.
2. On se reportera à la proposition 4.46 et au texte qui suit (pages 51 et 52, jusqu'à la fin de la section 4.4.2)

   Commentaire : l'adverbe « soigneusement » utilisé dans l'énoncé de la question indiquait clairement qu'un certain niveau de détail était attendu dans la rédaction.

Exercice 5

Commentaire général : pour traiter cet exercice, une bonne maîtrise des notions d'application et de quantificateurs logiques (vues en L1) était indispensable.

1. Par définition de l'ordre, σ est d'ordre r si et seulement si on a

   $$\sigma^r = \mathrm{Id} \quad \text{et} \quad \forall k \in \{1, \dots, r-1\}, \quad \sigma^k \neq \mathrm{Id}\,.$$

   Par définition de l'égalité de deux applications, cette dernière condition équivaut bien à la condition de l'énoncé.

   Commentaire : Pour mémoire, si A et B sont des ensembles et f et g sont des applications de A vers B, on a, par définition :

   $$f = g \iff \forall a \in A, \quad f(a) = g(a).$$

   On en déduit aussitôt, par application des règles de logique vues en L1, qu'on a également :

   $$f \neq g \iff \exists a \in A, \quad f(a) \neq g(a)$$

2. On va appliquer le critère donné par la question précédente.

   Soit c un r-cycle et $\{d_1, \dots, d_r\}$ une partie de cardinal r de $\{1, \dots, n\}$ telle qu'on puisse écrire, avec la notation vue en cours, $c = (d_1, d_2, \dots, d_r)$. En particulier, pour tout entier i compris entre 1 et $r-1$, on a $c(d_i) = d_{i+1}$ et $c(d_r) = d_1$. On en déduit par une récurrence finie qu'on a, pour tout entier i compris entre 1 et $r-1$, $c^i(d_1) = d_{i+1}$ et $c^r(d_1) = d_1$. En particulier, pour tout entier i compris entre 1 et $r-1$, on a $c^i(d_1) \neq d_1$.

   Soit i un entier compris entre 2 et r. On a

   $$c^r(d_i) = c^r(c^{i-1}(d_1)) = c^{r+i-1}(d_1) = c^{i-1}(c^r(d_1)) = c^{i-1}(d_1) = d_i$$

   donc $c^r(d_i) = d$. Finalement pour tout entier i compris entre 1 et r, on a $c^r(d_i) = d_i$

   Par ailleurs, pour tout élément d de $\{1, \dots, n\} \setminus \{d_1, \dots, d_r\}$, on a $c(d) = d$; on peut en déduire par récurrence qu'on a, pour tout entier m positif, $c^m(d) = d$, et en particulier $c^r(d) = d$.

   Si l'on récapitule, on a montré, d'une part que pour tout $d \in \{1, \dots, n\}$, on a $c^r(d) = d$, d'autre part que pour tout entier k compris entre 1 et $r-1$ on a $c^k(d_1) \neq d_1$

   On peut conclure grâce à la question précédente.

3. Soit $i \in \{1, \dots, s\}$. Montrons que pour tout d dans le support de c_i, on a $c_i(d) = \sigma(d)$, puis que l'ordre de c_i divise l'ordre de σ. Comme les cycles $c_1, \dots, c_s$ ont des supports deux à deux disjoints, on sait d'après le cours qu'ils commutent deux à deux, et ainsi quitte à changer la numérotation des cycles, on peut supposer que $i = 1$. Soit d dans le support de c_1.

Pour tout entier j compris entre 2 et s, le support de c_j ne contient pas d et donc $c_j(d) = d$. On en déduit, par une récurrence finie, qu'on a $(c_2 \dots c_s)(d) = d$. Ainsi on a

$$\sigma(d) = (c_1\, c_2 \dots c_s)(d) = c_1[(c_2 \dots c_s)(d)] = c_1(d).$$

Mais par ailleurs on sait que le support de c_1 est stable par c_1 (tout élément du support de c_1 est envoyé par c_1 sur un élément du support de c_1). Par récurrence, on déduit alors de l'égalité $\sigma(d) = c_1(d)$ qu'on a pour tout $m \in \mathbf{N}$ l'égalité $\sigma^m(d) = c_1^m(d)$.

Soit ρ l'ordre de σ. Montrons que l'ordre de c_1 divise ρ. D'après le cours (proposition 2.44), il suffit de montrer qu'on a $c_1^\rho = \mathrm{Id}$. Or pour tout élément d du support de c_1 on a d'après ce qui précède :

$$c_1^\rho(d) = \sigma^\rho(d) = \mathrm{Id}(d) = d.$$

Et pour tout élément d de $\{1, \dots, n\}$ qui n'est pas dans le support de c_1, on a $c_1(d) = d$, d'où (récurrence finie) $c_1^\rho(d) = d$.

Finalement, pour tout d élément de $\{1, \dots, n\}$, on a $c_1^\rho(d) = d$; donc $c_1^\rho = \mathrm{Id}$ et l'ordre de c_1 divise ρ.

Notons μ le ppcm des ordre des c_i. Comme pour tout entier i de $\{1, \dots, s\}$ l'ordre de c_i divise ρ, on déduit de la propriété fondamentale du ppcm que μ divise ρ.

Pour montrer que $\mu = \rho$, il suffit donc de montrer que ρ divise μ (il est à noter que μ et ρ sont des entiers positifs). Comme ρ est l'ordre de σ, il suffit d'après le cours (proposition 2.44) de montrer que $\sigma^\mu = \mathrm{Id}$. Comme les c_i commutent deux à deux, on peut écrire

$$\sigma^\mu = (c_1 \dots c_s)^\mu = c_1^\mu \dots c_s^\mu.$$

Or, pour tout élément $i \in \{1, \dots, s\}$, μ est par définition un multiple de l'ordre de c_i, et donc $c_i^\mu = \mathrm{Id}$. On en déduit qu'on a bien $\sigma^\mu = \mathrm{Id}$, ce qui, comme on l'a déjà expliqué, permet de conclure à l'égalité $\rho = \mu$.

Les cycles de $\mathfrak{S}_{10}$

$$c_1 = (1, 2), \quad c_1 = (3, 4, 5), \quad c_3 = (6, 7, 8, 9, 10)$$

sont visiblement à supports deux à deux disjoints. D'après le cours (ou la question 2), ils sont d'ordre respectif 2, 3 et 5. Ainsi d'après ce qui précède $\sigma = c_1 c_2 c_3$ est d'ordre $\mathrm{ppcm}(2, 3, 5) = 30$.

Commentaire : il y a dans la correction qui précède un certain nombre de récurrences qui n'ont pas été rédigées, ce qui dans l'absolu, est mal ; elles sont a priori sans difficulté, mais les rédiger en détail est toujours un exercice utile.

Exercice 6

1. On se reportera à la proposition 7.10 du poly
2. On se reportera à la définition 4.22 du poly.
3. Supposons qu'il existe $(a, b) \in \mathbf{Z}^2$ tel que $p = a^2 + b^2$ et montrons que p n'est pas irréductible dans $\mathbf{Z}[i]$. Il suffit de montrer qu'il existe des éléments z_1, z_2 de $\mathbf{Z}[i]$ tels qu'aucun d'entre eux n'est inversible et vérifiant $p = z_1\, z_2$. Prenons $z_1 = a + i\, b$ et $z_2 = a - i\, b$. Ce sont bien des éléments de $\mathbf{Z}[i]$ vérifiant $p = z_1\, z_2$. Par ailleurs $N(z_1) = N(z_2) = a^2 + b^2 = p$ en particulier les normes $N(z_1)$ et $N(z_2)$ ne sont pas égales à 1. D'après la question 1, z_1 et z_2 ne sont pas inversibles dans $\mathbf{Z}[i]$.

Supposons que p n'est pas irréductible dans $\mathbf{Z}[i]$. Comme p n'est ni nul, ni inversible (car on a $N(p) = p^2$ et $p^2 \neq 1$), cela signifie qu'il existe $z_1, z_2 \in \mathbf{Z}[i]$ non inversibles vérifiant $p = z_1 z_2$. En prenant la norme, on obtient $p^2 = N(z_1)N(z_2)$. Or $N(z_1)$ et $N(z_2)$ sont des entiers positifs, distincts de 1 d'après la question précédente. Compte tenu du fait que les diviseurs de p^2 sont 1, p et p^2 (p est premier), on a nécessairement $N(z_1) = N(z_2) = p$. Si on écrit $z_1 = a + i\,b$ avec $(a, b) \in \mathbf{Z}^2$, on a donc en particulier $p = a^2 + b^2$.