Université Paris Diderot
Licence de Mathématiques

Algèbre
Année 2015-16
M. Livernet, L. Merel

Esquisse de corrigé de l'examen du 8 Janvier 2016

I

1. On a $2016 = 2^5 \times 3^2 \times 7$.
2. Le groupe $D_4 \times \mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2 \times \mathbf{Z}/7\mathbf{Z}$ n'est pas abélien puisque le groupe diédral D_4 n'est pas abélien. Mais il est d'ordre 2016 puisque D_4 est d'ordre 8.
3. Un groupe abélien fini G est isomorphe au produit de ses composantes p-primaires, qui sont d'ordre 32 pour $p = 2$, d'ordre 9 pour $p = 3$, d'ordre 7 pour $p = 7$, et qui sont triviales pour les autres valeurs du nombre premier p.
4. Le groupe $(\mathbf{Z}/2\mathbf{Z})^5 \times (\mathbf{Z}/3\mathbf{Z})^2 \times \mathbf{Z}/7\mathbf{Z}$ est d'ordre 2016 et non cyclique.
5. Le groupe $(\mathbf{Z}/2016\mathbf{Z})^\times$ est d'ordre $\phi(2016) = \phi(2^5)\phi(9)\phi(7) = 16 \times 6 \times 6 = 576$, où ϕ est la fonction indicatrice d'Euler.
6. Le groupe $(\mathbf{Z}/7\mathbf{Z})^\times$ est cyclique d'ordre 6, car il est engendré par $\bar{3}$ (qui est d'ordre 6). Le groupe $(\mathbf{Z}/9\mathbf{Z})^\times$ est cyclique d'ordre 6 car il est engendré par $\bar{2}$, qui est d'ordre 6. Le groupe $(\mathbf{Z}/32\mathbf{Z})^\times$ est engendré par $\{\bar{5}, -\bar{1}\}$ en effet $\bar{5}$ est d'ordre 8 et $-\bar{1}$ est d'ordre 2. Comme $-\bar{1}$ n'appartient pas au sous-groupe engendré par $\bar{5}$, le groupe $(\mathbf{Z}/32\mathbf{Z})^\times$ est isomorphe au produit d'un sous-groupe d'ordre 8 et d'un sous-groupe d'ordre 2.
7. Le groupe $(\mathbf{Z}/2016\mathbf{Z})^\times$ est isomorphe au produit $(\mathbf{Z}/32\mathbf{Z})^\times \times (\mathbf{Z}/9\mathbf{Z})^\times \times (\mathbf{Z}/7\mathbf{Z})^\times$ par le théorème des restes chinois. D'après la question précédente, on a les isomorphismes de groupes $(\mathbf{Z}/7\mathbf{Z})^\times \simeq \mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ et de même $(\mathbf{Z}/9\mathbf{Z})^\times \simeq \mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. On a de plus $(\mathbf{Z}/32\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. En somme, le groupe $(\mathbf{Z}/2016\mathbf{Z})^\times$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^3 \times \mathbf{Z}/8\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2$.
8. Dans $(\mathbf{Z}/2\mathbf{Z})^3 \times \mathbf{Z}/8\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2$, l'élément $(0, 0, 0, 1, 1, 1)$ est d'ordre 24.
9. Considérons les cycles c_1, c_2,..., c_k de $\mathcal{S}_n$ donnés par $c_i = ((m_i+1)(m_i+2)...(m_i+n_i))$, avec $m_i = n_1+n_2+...+n_{i-1}$. Le cycle c_i est d'ordre n_i. Ces cycles sont à support disjoints. Ils commutent donc. On a donc un isomorphisme de groupes $(\mathbf{Z}/n_1\mathbf{Z}) \times (\mathbf{Z}/n_2\mathbf{Z}) \times ... \times (\mathbf{Z}/n_k\mathbf{Z}) \to \mathcal{S}_n$ donné par $(\bar{a_1}, \bar{a_2}, ..., \bar{a_k}) \mapsto c_1^{a_1} c_2^{a_2} ... c_k^{a_k}$.
10. On applique le résultat de obtenu par la question 9 à $n_1 = n_2 = n_3 = 2$, $n_4 = 8$, $n_5 = n_6 = 3$, en utilisant la question 7.

II

1. On a $\rho^2 = \rho + 1 \in A$.
2. On a $1 \in A$. Soient $u, v, u', v' \in \mathbf{Z}$. On a $(u+v\rho)+(u'+v'\rho) = (u+u')+(v+v')\rho \in A$, $(u+v\rho)(u'+v'\rho) = uu' + vv' + (uv' + vu' + vv')\rho \in A$ et $-(u+v\rho) = -u + (-v)\rho$. Ainsi A est non vide, stable par addition, passage à l'opposé, multiplication et contient 1. C'est donc un sous-anneau de $\mathbf{R}$. On démontre par la même méthode et à l'aide des mêmes formules que K est un sous-anneau de $\mathbf{R}$.
3. L'application ϕ respecte l'addition et on a $\phi(1) = 1$. Montrons qu'elle respecte la multiplication. On a $\phi((u+v\rho)(u'+v'\rho)) = \phi(uu' + vv' + (uv' + vu' + vv')\rho) = uu' + 2vv' +$

$uv'+uv'+vu'-(uv'+u'v+vv')\rho = ((u+v)-v\rho)(u'+v'-v'\rho) = \phi((u+v\rho))\phi((u'+v'\rho))$. L'application ϕ est bijective car elle vérifie $\phi \circ \phi = \mathrm{Id}$. Donc ϕ est bien un isomorphisme d'anneaux.
4. Calcul direct. On a donc $\mathrm{N}(aa') = aa'\phi(aa') = a\phi(a)a'\phi(a') = \mathrm{N}(a)\mathrm{N}(a')$.
5. Si a est inversible dans A, on a $1/a \in A$ et donc $\mathrm{N}(a)\mathrm{N}(1/a) = \mathrm{N}(a.1/a) = \mathrm{N}(1) = 1$. Donc $\mathrm{N}(a)$ est inversible dans $\mathbf{Z}$. Donc $\mathrm{N}(a) \in \{-1, 1\}$.
6. On a $\mathrm{N}(a) = a\phi(a)$ et donc $1/a = \phi(a)/\mathrm{N}(a)$. Le membre de droite est égal à $\phi(a)$ ou $-\phi(a)$. Donc $1/a \in A$.
7. On a $1/\rho = \rho - 1 \in A$. Donc ρ est inversible. Comme $A^\times$ est un groupe, il contient toutes les puissances entières de ρ.
8. Puisque $A^\times$ est un sous-groupe de $\mathbf{R}^\times$, dont les seuls éléments d'ordre fini sont -1 et 1, les seuls éléments d'ordre fini de $A^\times$ sont -1 et 1.
9. On déduit de ce qui précède que ρ est d'ordre infini (puisque ρ est inversible et distinct de 1 et -1) dans $A^\times$. Donc $A^\times$ est d'ordre infini.
10. Soit $u + v\rho \in K$, avec u, $v \in \mathbf{Q}$ non tous deux nuls. On a $(u^2 + uv - v^2) = (u + v\rho)(u + v - v\rho)$ qui est non nul puisque ρ est irrationnel. On a $1/(u + v\rho) = (u + v)/(u^2 + uv - v^2) - (v/(u^2 + uv - v^2))\rho \in K$. Donc $u + v\rho$ est inversible dans K. Tout sous-corps de $\mathbf{R}$ contenant A contient K, puisque tout élément de K est le rapport deux éléments de A. Par propriété universelle du corps des fractions, il existe un morphisme injectif d'anneaux $\iota : \mathrm{Frac}(A) \to K$. Son image est un corps qui contient A. Elle contient donc K. Donc ι est un isomorphisme d'anneaux.
11. Soit $P = X^2 - X - 1 \in \mathbf{Z}[X]$. On a $P(\rho) = 0$ d'après 1. Par ailleurs P est de degré 2. Il serait scindé sur $\mathbf{Q}$ s'il était réductible sur $\mathbf{Q}$. Or P possède une racine non rationnelle. Il n'est donc pas scindé sur $\mathbf{Q}$ et donc irréductible.
12. C'est le morphisme d'évaluation.
13. Le morphisme ψ est surjectif puisque $u + v\rho$ a pour antécédent $u + vX$ (u, $v \in \mathbf{Q}$). Son noyau est un idéal principal engendré par le polynôme minimal de ρ sur $\mathbf{Q}$. D'après la question 10, ce polynôme minimal est $X^2 - X - 1$.