Algèbre, Master 1 **5 novembre 2018**
2018–2019

Examen partiel d'Algèbre

Correction

Problème 1 1. Comme $\mathbb{Z}$ est factoriel, tout polynôme irréductible de $\mathbb{Z}[X]$ l'est dans l'anneau $\mathbb{Q}[X]$.

2. Il faut montrer que $Q \mapsto \overline{Q}_p$ est compatible avec la somme des polynômes. Cela provient de l'égalité $\overline{a_n + b_n} = \overline{a}_n + \overline{b}_n$.
   Il faut enfin montrer que $Q \mapsto \overline{Q}_p$ est compatible avec la multiplication des polynômes. Cela provient, par le produit de Cauchy, de l'égalité

$$\overline{\sum_{k=0}^{n} a_k b_{n-k}} = \sum_{k=0}^{n} \overline{a_k}\,\overline{b_{n-k}}.$$

   Pour la dernière assertion, montrons la contraposée. Soit Q réductible sur $\mathbb{Z}[X]$, et donc $Q = ST$, avec S et T non inversibles dans $\mathbb{Z}[X]$. Alors, comme Q est unitaire, S et T le sont aussi (leur coefficient dominant est inversible) et donc, comme S et T non inversibles, cela signifie que leur degré est strictement positif. D'après la question précédente, $\overline{Q}_p = \overline{S}_p\overline{T}_p$. Comme S et T sont unitaires, $\overline{S}_p$ et $\overline{T}_p$ sont de même degré respectifs que S et T, donc de degré strictement positifs. Conclusion, $\overline{Q}_p$ est réductible.

3. Comme le polynôme $X^3 - X - 1$ est de degré 3, montrer qu'il est irréductible sur $\mathbb{F}_3$ revient à montrer qu'il n'a pas de racine sur $\mathbb{F}_3$. Or, 0 et ± 1 ne sont pas racine. D'où la première assertion.
   Comme $\overline{P}_3 = X^9 - X^3 - 1$, en remarquant que sur $\mathbb{F}_3$, $(a+b)^3 = a^3 + b^3$ (Frobenius !), on obtient $(X^3 - X - 1)^3 = X^9 - X^3 - 1$. D'où l'assertion, puisque $X^3 - X - 1$ est irréductible sur $\mathbb{F}_3$.

4. Supposons α dans $\mathbb{F}_4$ tel que $\alpha^4 + \alpha + 1 = 0$. Alors, comme $\alpha^4 = \alpha$, il vient, $0 = \alpha^4 + \alpha + 1 = 2\alpha + 1 = 1$, puisque l'on travaille en caractéristique 2. Impossible.
   Montrons que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$. Si, par l'absurde, il se décomposait sur $\mathbb{F}_2$, alors ce serait soit en facteurs de degré 1 et 3, soit en facteurs de degré 2 et 2. Dans le premier cas, il possèderait une racine dans $\mathbb{F}_2$, ce qui est clairement pas le cas. Dans le second cas, il se décomposerait en RS, avec R et S irréductibles de degré 2 sur $\mathbb{F}_2$. Or, $\mathbb{F}_2[X]/R$ serait un corps de rupture de R, et donc une extension de degré 2 sur $\mathbb{F}_2$. On aurait $\mathbb{F}_{2^2} = \mathbb{F}_4$. Conclusion, $X^4 + X + 1$ possèderait une racine dans $\mathbb{F}_4$, ce qui est impossible par ce qui précède.
   Comme $\overline{P}_2 = X^9 + X^8 + X^3 + X^2 + X + 1$, en remarquant que sur $\mathbb{F}_2$, $(a+b)^2 = a^2 + b^2$, on obtient

$$(X+1)(X^4 + X + 1)^2 = (X+1)(X^8 + X^2 + 1) = \overline{P}_2.$$

   D'où l'assertion, puisque $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

5. Supposons par l'absurde P réductible sur $\mathbb{Q}$, alors P est réductible sur $\mathbb{Z}$, par la question 1. Supposons qu'il se décompose en RS, avec R et S deux polynômes entiers de degré respectif r et s. Alors, $r+s=9$, avec $rs \neq 0$. En utilisant la question 2 et la question 3, on voit que, quitte à permuter R et S, on a $r=3$ et $s=6$. Par la question 4, on voit que $\mathbb{F}_2$ se décompose en 3 polynômes irréductibles de degré différent de 3 et 6, ce qui est impossible.

Problème 2

1. Tout élément de G peut s'écrire comme la classe de p/q et donc en le multipliant par q, on obtient la classe p donc 0 puisque p est entier.
2. Montrons la double inclusion. Il est clair que la classe de $\frac{p}{q}$ est dans le sous-groupe engendré par la classe de $\frac{1}{q}$. D'où la première inclusion. Pour montrer l'inclusion inverse, il suffit de voir que $up+vq=1$ pour u,v de $\mathbb{Z}$ par Bezout, puisque l'on a alors :
$$\overline{u\frac{p}{q}} = \overline{u\frac{p}{q}+v} = \overline{\frac{1}{q}},$$
ce qui prouve bien que $\overline{\frac{1}{q}}$ est dans le sous-groupe engendré par $\overline{\frac{p}{q}}$.
En déduire que, pour chaque entier $n \geq 1$, il existe un unique sous-groupe cyclique de G d'ordre n.
Il est clair que le sous-groupe engendré par $\overline{\frac{1}{n}}$ est d'ordre n. Pour l'unicité, soit G un groupe cyclique d'ordre n, alors il est engendré par un élément de la forme $\overline{\frac{m}{n}}$, avec m et n premiers entre eux. Par la question précédente, ce sous-groupe est engendré par $\overline{\frac{1}{n}}$. On a donc l'unicité.
3. On suppose que H est un sous-groupe de G engendré par les classes de $\frac{p}{q}$ et $\frac{p'}{q'}$. Soit d le pgcd de $q'p$ et qp' dans $\mathbb{Z}$, montrons que H est égal au sous-groupe cyclique engendré par la classe de $\frac{d}{qq'}$. Comme $q'p=ad$ pour un entier a, il vient $\frac{p}{q}=\frac{pq'}{qq'}=a\frac{d}{qq'}$ et de même pour $\frac{p'}{q'}$, ce qui prouve l'inclusion.
Pour l'inclusion inverse, il suffit d'écrire l'identité de Bezout $upq'+vq'p=d$, car $\mathbb{Z}$ est principal. Ceci donne $u\frac{p}{q}+v\frac{p'}{q'}=\frac{d}{qq'}$ et donc, on obtient l'inclusion inverse et H est cyclique.
Maintenant, si H est un sous-groupe de G de type fini, par récurrence sur le nombre de générateurs, on obtient donc que G est cyclique.
Montrons la dernière assertion. Tout sous-groupe d'ordre n de G est forcément de type fini, puisqu'il est fini ! Donc, il est cyclique et donc unique par la question qui précède.
4. On considère le sous-groupe de G engendré par les classes de $\frac{1}{p^n}$ avec p fixé et n dans $\mathbb{N}$. Ce groupe est distinct de G, puisque si q est premier distinct de p, une somme $\sum_{n=0}^{N}\frac{u_n}{p^n}=\frac{1}{q}+\mathbb{Z}$ est impossible. En effet, on multiplie par p^Nq et on voit que q divise p^N, ce qui est absurde.
Il est forcément infini car les classes de $\frac{1}{p^n}$ sont deux à deux distincts, en effet, les rationnels $\frac{1}{p^n}$ ne diffèrent pas d'un entier puisqu'ils sont tous dans $]0,1[$.
5. Supposons que pour tout pour tout p premier et $n \in \mathbb{N}$, contient un élément d'ordre p^n. Comme G est abélien, la somme d'un élément d'ordre m et un élément d'ordre m' est d'ordre mm' si m et m' sont premiers entre eux. Il en résulte que G contient

un élément pour tout ordre k dans $\mathbb{N}$, et donc tout $\frac{1}{k}$ par la question 2. Il contient donc tout G. Il en résulte qu'il existe p et n tel que G n'a pas d'élément d'ordre p^n. Donc, G/H contient la classe de $\frac{1}{p^N}$ pour tout $N \geq n$, il est donc infini car ceux-ci sont bien tous distincts. Vérifions-le quand même : si, par l'absurde, $\frac{1}{p^m}$ et $\frac{1}{p^{m'}}$, $n \leq m < m'$ sont dans la même classe modulo H, alors $\frac{1}{p^m} - \frac{1}{p^{m'}} = \frac{p^{m'-m}-1}{p^{m'}}$ serait d'ordre $p^{m'}$ (car $p^{m'}$ et $p^{m'-m}-1$ sont premiers entre eux) donc n'appartiennent pas à H, absurde.

Remarque. On gagne beaucoup en vision intérieure à considérer le groupe $\mathbb{Q}/\mathbb{Z}$ comme le sous-groupe U des racines de l'unité de $\mathbb{C}^*$. En effet, le morphisme qui envoie α dans $\mathbb{Q}$ sur $e^{2i\alpha\pi}$ a pour image U et pour noyau $\mathbb{Z}$ et fournit un isomorphisme $\mathbb{Q}/\mathbb{Z} \simeq U$. La cyclicité d'un sous-groupe fini provient alors d'un résultat classique sur les sous-groupes du groupe multiplicatif d'un corps, et l'unicité également. On obtient un sous-groupe infinité propre de U en prenant l'ensemble des racines 2^n-ièmes de l'unité pour tout n.

Problème 3

1. On veut montrer que $\sigma\Delta = \varepsilon(\sigma)\Delta$ pour tout σ. Comme ε est un morphisme il suffit de le montrer pour un système de générateur de S_n, disons les transpositions $(i, i+1)$. Or, il est clair que lorsque l'on échange i et $i+1$ dans Δ tous les facteurs restent inchangés sauf $(X_i - X_{i+1})$ qui est changé en son opposé. On a donc bien $(i, i+1)\Delta = -\Delta$ comme voulu.
2. On sait que $A = k[X_2, \cdots, X_n][X_1]$. On effectue la division euclidienne de P par le polynôme $(X_1 - X_2)$ dans l'anneau euclidien $k(X_2, \cdots, X_n)[X_1]$ et comme le polynôme $(X_1 - X_2)$ est unitaire, le reste et le quotient restent dans A.
3. (a) On évalue l'identité $P = Q \cdot (X_1 - X_2) + R$ en $X_1 = X_2$ pour obtenir que R est l'évaluation de A en $X_1 = X_2$, ce que l'on écrit $R = \mathrm{ev}_{(X_1=X_2)}(A)$. Or, l'évaluation de A en $X_1 = X_2$ ne change pas si l'on échange X_1 et X_2 dans A. C'est-à-dire, étant donné que $(12)A = -A$ par hypothèses :

$$R = \mathrm{ev}_{(X_1=X_2)}(A) = \mathrm{ev}_{(X_1=X_2)}(12)A = \mathrm{ev}_{(X_1=X_2)}(-A) = -R.$$

Comme on est en caractéristique différente de 2, on obtient bien $R = 0$.

(b) On voit donc que A est divisible par le polynôme $(X_1 - X_2)$. Or, ce polynôme est irréductible car de degré 1 en X_1 et de contenu 1 car unitaire en X_1. De même, A est divisible par le polynôme irréductible $(X_i - X_j)$, $1 \leq i < j \leq n$. Comme tous ces polynômes sont non associés et irréductibles, ils sont deux à deux premiers entre eux et A est divisible par leur produit, qui est égal à Δ.

Remarque. Le résultat final est faux dans le cas de la caractéristique 2. En effet, dans ce cas, $1 = -1$ et un polynôme antisymétrique est tout simplement symétrique. Or, si par exemple $n = 2$, X_1X_2 est antisymétrique (car symétrique) mais n'est pas divisible par $\Delta = (X_1 - X_2)$, puisque l'évaluation $X_1 = X_2$ ne l'annule pas.