Corrigé de l'examen de mathématiques générales I du 18/12/23

Exercice 1 (6 points)

a) C'est vrai. Si T est un autre p-Sylow, on sait qu'il est conjugué de S ; l'hypothèse S distingué implique alors $S = T$ (1.5 point).

b) C'est faux. On a vu que le sous-groupe dérivé de $\mathcal{S}_3$ est $\mathcal{A}_3 \simeq \mathbf{Z}/3\mathbf{Z}$, qui est abélien. Pourtant $\mathcal{S}_3$ n'est pas abélien (1.5 point).

c) C'est faux. Par exemple $\mathbf{Z}$ admet tout $p\mathbf{Z}$ avec p premier comme idéal maximal (1.5 point).

d) C'est faux. Dans $\mathbf{Z}[X]$, le polynôme $2X$ est de degré 1 mais n'est pas irréductible (1.5 point).

Exercice 2 (8 points)

a) Considérons un commutateur $z = xyx^{-1}y^{-1}$ avec $x, y \in G$. Alors $f(z) = f(x)f(y)f(x)^{-1}f(y)^{-1}$ (parce que f est un morphisme), qui est égal à 1 car $\mathbf{C}^*$ est abélien (1 point). Ainsi le noyau de f contient tous les commutateurs, donc le sous-groupe qu'ils engendrent, donc ce noyau contient $D(G)$ (1 point).

b) Tout d'abord Φ est un morphisme car si $f, g \in \widehat{G^{\mathrm{ab}}}$ et $x \in G$, alors

$$(\Phi(fg))(x) = (fg)(\bar{x}) = f(\bar{x})g(\bar{x}) = (\Phi(f))(x).(\Phi(g))(x) = (\Phi(f)\Phi(g))(x),$$

d'où $\Phi(fg) = \Phi(f)\Phi(g)$. Le noyau de Φ est réduit au neutre car si $\Phi(f)$ est l'application constante égale à 1, on a (pour tout x de G) $\Phi(f)(x) = 1$ soit $f(\bar{x}) = 1$, ce qui montre que f est constante égale à 1. Enfin, si $g \in \widehat{G}$, on a vu en a) que le noyau de G contient $D(G)$, donc g se factorise en un morphisme $\bar{g} : G/D(G) \to \mathbf{C}^*$. On a alors par définition $\Phi(\bar{g}) = g$. Finalement, Φ est surjective (1.5 point).

c) Comme vu en cours, le sous-groupe dérivé de $S := \mathcal{S}_n$ est $\mathcal{A}_n$, et on a donc $S^{\mathrm{ab}} \simeq \mathbf{Z}/2\mathbf{Z}$. D'après b), on est donc ramené à déterminer $\widehat{(\mathbf{Z}/2\mathbf{Z})}$. Un morphisme de $\mathbf{Z}/2\mathbf{Z}$ dans $\mathbf{C}^*$ doit envoyer $\bar{1}$ sur un élément x vérifiant

$x^2 = 1$, donc sur 1 ou -1 (et bien sûr $\bar{0}$ sur 1). Réciproquement, on voit que les deux possibilités donnent bien des morphismes, donc $\widehat{S}$ est d'ordre 2, il est donc isomorphe à $\mathbf{Z}/2\mathbf{Z}$ (1.5 point).

d) On peut supposer $G = \mathbf{Z}/n\mathbf{Z}$. Fixons une racine primitive n-ième de l'unité ζ ; alors l'application f_0 de G dans $\mathbf{C}^*$ qui envoie $\bar{r}$ sur ζ^r est bien définie (parce que $\zeta^n = 1$), et c'est clairement un morphisme de groupes. Par ailleurs, si $f : G \to \mathbf{C}^*$ est un morphisme, alors $f(\bar{1})^n = 1$, donc $f(\bar{1})$ (qui est une racine n-ième de l'unité) s'écrit ζ^m avec $m \in \mathbf{N}$. On a alors

$$f(\bar{r}) = f(r\bar{1}) = f(\bar{1})^r = \zeta^{mr} = f_0(\bar{r})^m,$$

ce qui montre que $f = f_0^m$. Ainsi, f_0 engendre $\widehat{G}$, qui est donc cyclique d'ordre n comme demandé (2 points).

e) Soient A et B deux groupes. Soit $f : A \times B \to \mathbf{C}^*$ un morphisme. Alors

$$f(x, y) = f((x, 1).(1, y)) = f(x, 1)f(1, y).$$

On définit un morphisme u de $\widehat{A} \times \widehat{B}$ dans $(\widehat{A \times B})$ par

$$(f_1, f_2) \mapsto [(x, y) \mapsto f_1(x)f_2(y)].$$

L'égalité qui précède montre que u est surjectif (un antécédent de f s'obtient en prenant $f_1(x) = f(x, 1)$ et $f_2(y) = f(1, y)$). De plus u est injectif car si $u(f_1, f_2)$ est trivial, alors f_1 et f_2 sont triviaux (prendre $y = 1$ puis $x = 1$ dans la définition de u). Finalement $(\widehat{A \times B})$ et $\widehat{A} \times \widehat{B}$ sont isomorphes. Par récurrence sur r, on obtient que $(A_1 \times \widehat{A_2 \times} ...A_n)$ est isomorphe à $\widehat{A_1} \times ... \times \widehat{A_r}$ pour toute famille finie de groupes $(A_1, ...A_r)$. On obtient alors le résultat via d) et le fait que tout groupe abélien est isomorphe à un produit de groupes cycliques (2 points).

Exercice 3 (7 points)

a) Si x ou y est nul, c'est clair. Sinon on a x/y ou y/x dans A, ce qui signifie que y divise x ou x divise y (1 point).

b) Soient $x \in M$ et $a \in A$. Alors, si ax était inversible dans A, on aurait un $b \in A$ tel que $bax = 1$, donc x aurait pour inverse ba et ne serait pas dans M. Si maintenant x et y sont dans M, alors on a par exemple y divise x via a) ; on peut donc écrire $y = cx$ avec $c \in a$, d'où $x + y = (1 + c)x$, qui est bien dans M d'après ce qui précède vu que $(1 + c) \in A$. Par ailleurs, 0 et $-x$ sont bien dans M (toujours d'après ce qui précède). Finalement, M est un idéal de A (1.5 point).

c) Si I est un idéal de A autre que A, alors il ne peut contenir d'élément inversible dans A, donc $I \subset M$. Ainsi M contient tout idéal de A autre que A, ce qui implique immédiatement que c'est le seul idéal maximal de A (1 point).

d) Déjà $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$: il contient clairement 0 et 1, est stable par soustraction (en effet $a/b - c/d = (ad - bc)/bd$ et p ne divise pas bd s'il ne divise ni b ni d) et par multiplication (via $(a/b)(c/d) = (ac/bd)$). Comme on a clairement $\mathbf{Z} \subset \mathbf{Z}_{(p)} \subset \mathbf{Q}$ avec $\mathbf{Q}$ corps des fractions de $\mathbf{Z}$, $\mathbf{Q}$ est bien l'ensemble des x/y avec x, y dans $\mathbf{Z}_{(p)}$ et $y \neq 0$, c'est donc le corps des fractions de $\mathbf{Z}_{(p)}$. Enfin, si $z \in \mathbf{Q}$, on peut l'écrire $z = a/b$ avec a et b premiers entre eux. En particulier p ne divise pas a ou p ne divise pas b. Dans le premier cas, on a $z^{-1} \in A$, dans le deuxième $z \in A$ (1.5 point).

e) D'après b), on peut par exemple supposer que a divise b, soit $b = ac$ avec $c \in A$. Alors tout élément de (a, b) s'écrit $xa + yb$ avec $x, y \in A$, soit $xa + yac = a(x + yc)$, ce qui montre qu'on a en fait $(a, b) = (a)$ (1 point).

f) Par récurrence sur r, e) donne que pour tout entier $r > 0$, un idéal engendré par r éléments est principal. Si A est noethérien, tout idéal est engendré par un nombre fini d'éléments, donc est principal. Ainsi l'anneau intègre A est principal (1 point).