Corrigé de l'examen d'algèbre de M1

Exercice 1 : Groupes (5 points)

a) On a $1 \in C_x$ car $x.1 = 1.x = x$. Si y, y' sont dans C_x, alors

$$x(yy') = (xy)y' = yxy' = y(y'x) = (yy')x,$$

donc $yy' \in C_x$. Finalement, si $y \in C_x$, alors $xy = yx$ d'où $x = yxy^{-1}$ et $y^{-1}x = xy^{-1}$, ce qui montre que $y^{-1} \in C_x$. Ainsi, C_x est un sous-groupe de G (1 point). On peut aussi directement dire que C_x est le stabilisateur de x pour l'action de G sur lui-même par conjugaison.

b) On sait que Z est distingué dans G, donc G/Z est un groupe, qui n'est pas cyclique dès que G n'est pas commutatif (lemme vu en cours). De ce fait, G/Z est de cardinal au moins 4 (vu que 2 et 3 sont des nombres premiers, tout groupe d'ordre 1, 2 ou 3 est cyclique), ce qui donne $g/|Z| \geq 4$, ou encore $|Z| \leq g/4$ (1.5 point).

c) Par définition de E et de C_x, on a

$$|E| = \sum_{x \in G} |C_x|.$$

Si $x \in Z$, alors $C_x = G$ d'où $|C_x| = g$, ce qui donne la formule en séparant les éléments de G en ceux qui sont dans Z et ceux qui ne sont pas dans Z. D'autre part, si $x \notin Z$, alors C_x est un sous-groupe strict de G, donc il est d'indice au moins 2, donc $|C_x| \leq g/2$ (1.5 point).

d) D'après c), on a

$$|E| \leq g|Z| + (g - |Z|)g/2,$$

d'où

$$|E|/g^2 \leq 1/2 + \frac{|Z|}{2g}.$$

D'après b), on a $\frac{|Z|}{2g} \leq 1/8$, d'où $|E|/g^2 \leq 1/2 + 1/8 = 5/8$ (1 point).

Exercice 2 : Anneaux (4 points)

a) C'est faux, il n'est même pas intègre vu que $52 = 13 \times 4$ n'est pas premier (1 point).

b) C'est faux, car il est divisible par 7, qui n'est pas inversible dans $\mathbf{Z}[X]$ (1 point).

c) C'est faux. Soit en effet $r_1, ..., r_s$ une famille finie d'éléments de $\mathbf{Q}$. Ecrivons chaque r_i sous la forme d'une fraction irréductible p_i/q_i avec $q_i \in \mathbf{N}^*$. Alors, tout élément de la $\mathbf{Z}$-algèbre A engendrée par les r_i s'écrit $P(r_1, ..., r_s)$ avec $P \in \mathbf{Z}[X]$, donc s'écrit sous forme d'une fraction irréductible n/d, avec d de la forme

$$d = q_1^{\alpha_1} ... q_r^{\alpha_r},$$

avec chaque α_i dans $\mathbf{N}$. Or, certains nombre rationnels ne sont pas de cette forme, par exemple $1/p$, où p est un nombre premier qui ne divise aucun des q_i, donc ne peut pas diviser d par unicité de la décomposition en facteurs premiers (2 points).

Exercice 3 : Modules (8 points)

a) Soit $\mathcal{B} = (e_1, ..., e_r)$ une base de L. Soit $e_i^* : L \to A$ la forme linéaire qui envoie e_i sur 1 et les autres e_j sur 0. Montrons que $\mathcal{B}^* := (e_1^*, ..., e_r^*)$ est une base de L^*. Soit $f : L \to A$ linéaire, alors f coïncide avec l'application linéaire $\sum_{j=1}^r f(e_j)e_j^*$, car les deux prennent les mêmes valeurs sur la base $\mathcal{B}$. Ainsi $\mathcal{B}^*$ est une famille génératrice de M^*. Si maintenant $\sum_{j=1}^r \alpha_j e_j^* = 0$ avec $\alpha_j \in A$, alors en évaluant sur chaque e_i on trouve que tous les α_i sont nuls, ce qui montre que $\mathcal{B}^*$ est une famille libre. Ainsi $\mathcal{B}^*$ est une base de M^*, qui est donc libre de rang r (1.5 point).

b) Soit $f : \mathbf{Q} \to \mathbf{Z}$ linéaire. Soit $x \in \mathbf{Q}$, alors pour tout $n \in \mathbf{N}^*$ on peut écrire $x = ny$ avec $y \in \mathbf{Q}$, donc $f(x) \in n\mathbf{Z}$ pour tout $n \in \mathbf{N}^*$, ce qui montre que $f(x) = 0$. Ainsi f est nulle et donc $M^* = 0$ (1 point).

c) Il est clair que i est injective car comme p est surjective, $f \circ p = 0$ implique $f = 0$. Par définition, le noyau de u est constitué des formes linéaires $g : L \to A$ dont la restriction à R est nulle. Si $g = i(f)$ avec $f \in M^*$, alors on a $g(x) = 0$ pour tout $x \in R$ car un tel x vérifie $p(x) = 0$ par définition d'une suite exacte. Réciproquement, si la restriction de g à R est nulle, alors g induit une forme linéaire f sur M via la formule $f(p(x)) = g(x)$ pour tout $x \in L$, qui a un sens car tout y de M s'écrit $p(x)$, et deux éléments x, x' qui s'envoient sur y par p vérifient $g(x) = g(x')$ puisqu'alors $(x - x') \in R$ et la restriction de g à R est nulle. On a alors bien $g = i(f)$. Finalement $\ker u = \operatorname{Im} i$ comme on voulait (2 points). Notons au passage que u n'est pas toujours surjective (prendre l'inclusion $\mathbf{Z} \to \mathbf{Q}$ et appliquer b).

d) Comme M est de type fini, on a une suite exacte comme en c) avec L libre de type fini. D'après c), M^* est isomorphe à un sous-module de L^*, lequel est libre de type fini d'après a). Comme A est noethérien, M^* est de type fini. Si A est de plus principal, on sait que M^* est libre (1.5 point).

e) Supposons M de torsion. Soit $f : M \to A$ une forme linéaire. Pour tout $x \in M$, il existe a non nul dans A tel que $ax = 0$ d'où $f(ax) = af(x) = 0$. Comme A est intègre, ceci implique $f(x) = 0$. Ainsi $M^* = 0$ (cette implication est vraie dans tout anneau intègre). Supposons maintenant que M ne soit pas de torsion. D'après le théorème de structure des modules de type fini sur un anneau principal, on peut écrire $M = L \oplus F$ avec L libre de type fini de rang au moins 1 (et F de torsion). D'après a), il existe une forme linéaire non nulle g sur L, et on obtient une forme linéaire non nulle g sur M en composant f avec la projection $M \to L$. Ainsi M^* est bien non nul. Par contre, l'exemple de b) montre que le résultat tombe en défaut si M n'est pas de type fini, car le $\mathbf{Z}$-module $M = \mathbf{Q}$ vérifie $M^* = 0$, bien qu'il ne soit pas de torsion, il est même sans torsion (2 points).

Exercice 4 : Théorie de Galois (5 points)

a) D'après la correspondance de Galois, il suffit de trouver un sous-groupe de G d'indice a, c'est-à-dire un p-Sylow de G. Or, on sait qu'un tel p-Sylow existe toujours (1 point).

b) Soient H, H' les sous-groupes respectifs associés à F, F' par la correspondance de Galois. La formule de conjugaison dans cette correspondance dit qu'on cherche $\sigma \in \mathrm{Gal}\,(L/K)$ tel que H' soit le conjugué de H par σ. Or, H et H' sont deux p-Sylow de G (cf. a), ils sont donc bien conjugués (1 point).

c) D'après le théorème de structure des groupes abéliens, G est isomorphe à $\prod_{i=1}^{r} \mathbf{Z}/d_i\mathbf{Z}$, où les d_i sont des entiers au moins égaux à 2 tels que $d_1|d_2|...|d_r$. Par définition de e, on a alors $e = d_r$. On observe alors que le quotient de G par le sous-groupe $\prod_{i=1}^{r-1} \mathbf{Z}/d_i\mathbf{Z}$ est isomorphe à $\mathbf{Z}/e\mathbf{Z}$. Comme d divise e, le groupe $\mathbf{Z}/e\mathbf{Z}$ admet à son tour un quotient isomorphe à $\mathbf{Z}/d\mathbf{Z}$ (le quotient par $d\mathbf{Z}/e\mathbf{Z}$), ce qui fait que G a un quotient isomorphe à $\mathbf{Z}/d\mathbf{Z}$. La correspondance de Galois dit alors qu'il existe une extension galoisienne E de K, avec $E \subset L$, telle que $\mathrm{Gal}\,(E/K) \simeq \mathbf{Z}/d\mathbf{Z}$ (2 points).

d) Non : prenons une extension galoisienne L de $\mathbf{Q}$ de groupe de Galois $G = \mathcal{S}_3$ (par exemple $L = \mathbf{Q}(j, \sqrt[3]{2})$). On a alors dans G des éléments d'ordre 1, 2 et 3, donc $e = 6$. Mais on n'a pas d'extension intermédiaire E avec $\mathrm{Gal}\,(E/\mathbf{Q})$ cyclique d'ordre 6, car cela impliquerait (pour raison de degré) que $E = L$, or $\mathcal{S}_3$ n'est pas isomorphe à $\mathbf{Z}/6\mathbf{Z}$ (1 point).