Algèbre avancée
Examen final (durée : 3 heures)

NB : L'usage du cours est autorisé (mais pas les TD).

Exercice 1

Soit p un nombre premier impair et $\zeta_p = e^{\frac{2i\pi}{p}}$. On pose $\alpha = \zeta_p + \zeta_p^{-1}$.

1. Montrer que ζ_p est de degré 2 sur $\mathbf{Q}(\alpha)$ et en déduire que α est algébrique de degré $\frac{p-1}{2}$ sur $\mathbf{Q}$.
2. Déterminer le polynôme minimal de α sur $\mathbf{Q}$ lorsque $p = 5$ et $p = 7$.
3. Montrer que l'extension $\mathbf{Q}(\alpha)/\mathbf{Q}$ est galoisienne et que $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ est un groupe cyclique d'ordre $\frac{p-1}{2}$.
4. Combien le corps $\mathbf{Q}(\zeta_{37})$ possède-t-il de sous-corps ?
5. Pour tout nombre premier ℓ, montrer qu'il existe une infinité d'extensions finies galoisiennes $K/\mathbf{Q}$ non isomorphes telles que $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/\ell\mathbf{Z}$.

Exercice 2

Le but de cet exercice est de montrer le théorème de la base normale : si L/K est une extension finie galoisienne, alors il existe $a \in L$ tel que l'ensemble des conjugués de a sur K est une K-base de L. On pose $[L : K] = n$ et $G = \mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$, avec $\sigma_1 = \mathrm{id}_L$.

1. Montrer qu'il existe une unique application K-linéaire $\varphi : L \otimes_K L \to L^n$ telle que $\varphi(x \otimes y) = (x\sigma_i(y))_{1 \leq i \leq n}$ pour tous $x, y \in L$.
2. Montrer que φ est un isomorphisme (on pourra utiliser le lemme d'indépendance des caractères de Dedekind).

Dans les questions 3 à 5, on suppose K infini.

Soit $t = \sum_{k=1}^r x_k \otimes y_k \in L \otimes_K L$ tel que $\varphi(t) = (1, 0, \ldots, 0)$. On définit une fonction polynomiale $P : L^r \to L$ par

$$P(\lambda_1, \ldots, \lambda_r) = \det\Big(\sum_{k=1}^r \lambda_k \sigma_j^{-1}\sigma_i(y_k)\Big)_{1 \leq i,j \leq n}.$$

3. Montrer que $P(x_1, \ldots, x_r) = 1$.
4. Montrer qu'il existe $\lambda_1, \ldots, \lambda_r \in K$ tels que $P(\lambda_1, \ldots, \lambda_r) \neq 0$ (on pourra montrer par récurrence sur r qu'une fonction polynomiale $L^r \to L$ s'annulant sur K^r est nécessairement nulle).
5. On pose $a = \sum_{k=1}^r \lambda_k y_k$. Montrer que $(\sigma(a))_{\sigma \in G}$ est une K-base de L.

Dans les questions 6 et 7, on suppose $K = \mathbf{F}_q$ et $L = \mathbf{F}_{q^n}$. On note $F : L \to L$ l'endomorphisme de Frobenius, défini par $F(x) = x^q$.

6. Montrer que F est K-linéaire et déterminer son polynôme minimal μ.

On munit L d'une structure de $K[X]$-module par $P(X) \cdot x = P(F)(x)$ pour tout $P \in K[X]$ et $x \in L$.

7. À l'aide du théorème de structure des $K[X]$-modules de type fini, montrer l'isomorphisme de $K[X]$-modules $L \cong K[X]/(\mu)$, et en déduire le théorème de la base normale pour L/K.

Exercice 3

Soit A un anneau commutatif et $u : M \to N$ un morphisme de A-modules. On note $M_\mathfrak{p}$ (resp. $N_\mathfrak{p}$) le localisé de M (resp. N) en un idéal premier $\mathfrak{p}$ de A.

1. Soit $\mathfrak{p}$ un idéal premier de A. En utilisant la propriété universelle du localisé, montrer qu'il existe une unique application $A_\mathfrak{p}$-linéaire $u_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ telle que $u_\mathfrak{p}(x) = u(x)$ pour tout $x \in M$.
2. Montrer que les conditions suivantes sont équivalentes :
   (a) u est injectif ;
   (b) pour tout idéal premier $\mathfrak{p}$ de A, $u_\mathfrak{p}$ est injectif ;
   (c) pour tout idéal maximal $\mathfrak{m}$ de A, $u_\mathfrak{m}$ est injectif.
3. Montrer la même chose en remplaçant « injectif » par « surjectif ».

Exercice 4

1. Soit $n \geq 1$ un entier et p un nombre premier. Calculer le localisé $M_{(p)}$ du $\mathbf{Z}$-module $M = \mathbf{Z}/n\mathbf{Z}$ en l'idéal premier $p\mathbf{Z}$.
2. En déduire que tout groupe abélien fini, vu comme $\mathbf{Z}$-module, est isomorphe à la somme directe de ses localisés.
3. Montrer que deux groupes abéliens de type fini M et N sont isomorphes si et seulement si $M_{(p)} \cong N_{(p)}$ pour tout nombre premier p.
4. Soit M un groupe abélien fini. Déterminer les diviseurs élémentaires des groupes abéliens $M \otimes_\mathbf{Z} M$, $\mathrm{Sym}^2 M$ et $\bigwedge^2 M$ en fonction de ceux de M. (On pourra commencer par le cas où M est cyclique.)

Exercice 5

Soit A un anneau commutatif et M un A-module de type fini. Montrer que tout endomorphisme surjectif $u : M \to M$ est un isomorphisme.

Indications : on pourra se ramener au cas local, montrer que le relèvement d'une base de $\frac{M}{\mathfrak{m}M}$ engendre M, et s'inspirer de l'astuce du déterminant.