Algèbre avancée
Corrigé de l'examen final

Exercice 1

1. Le polynôme $X^2 - \alpha X + 1$ annule ζ_p qui est donc de degré 1 ou 2 sur $\mathbf{Q}(\alpha)$. Or on ne peut avoir $\zeta_p \in \mathbf{Q}(\alpha)$ puisque $\mathbf{Q}(\alpha) \subset \mathbf{R}$ et $\zeta_p \notin \mathbf{R}$ ($p \geq 3$). Donc ζ_p est de degré 2 sur $\mathbf{Q}(\alpha)$.
   Puisque ζ_p est de degré $p-1$ sur $\mathbf{Q}$ (cours) et $\alpha = \zeta_p + \zeta_p^{-1} \in \mathbf{Q}(\zeta_p)$ il vient
   $$p - 1 = [\mathbf{Q}(\zeta_p) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \zeta_p) : \mathbf{Q}(\alpha)] \cdot [\mathbf{Q}(\alpha) : \mathbf{Q}] = 2[\mathbf{Q}(\alpha) : \mathbf{Q}]$$
   et donc α est de degré $\frac{p-1}{2}$ sur $\mathbf{Q}$.
2. Soit $p = 5$. On a $\alpha^2 = \zeta_5^2 + \zeta_5^{-2} + 2$. La somme des racines 5^{e} de l'unité étant nulle, il vient $\alpha^2 + \alpha - 1 = 0$. Donc $X^2 + X - 1$ annule α et d'après la question 1, c'est le polynôme minimal de α sur $\mathbf{Q}$.
   Soit $p = 7$. On a $\alpha^2 = \zeta_7^2 + \zeta_7^{-2} + 2$ et $\alpha^3 = \zeta_7^3 + \zeta_7^{-3} + 3(\zeta_7 + \zeta_7^{-1})$. Par la même méthode, on trouve que $X^3 + X^2 - 2X - 1$ est le polynôme minimal de α sur $\mathbf{Q}$.
3. D'après le cours $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ est galoisienne et $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$. Comme tous les sous-groupes de $(\mathbf{Z}/p\mathbf{Z})^\times$ sont distingués, la correspondance de Galois entraîne que $\mathbf{Q}(\alpha)/\mathbf{Q}$ est galoisienne. De plus $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ s'identifie à un quotient de $(\mathbf{Z}/p\mathbf{Z})^\times$. Comme le quotient d'un groupe cyclique est cyclique et $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \frac{p-1}{2}$, on en déduit le résultat.
4. D'après la correspondance de Galois, les sous-corps de $\mathbf{Q}(\zeta_{37})$ sont en bijection avec les sous-groupes de $(\mathbf{Z}/37\mathbf{Z})^\times$ qui est cyclique d'ordre 36. Ces sous-groupes sont eux-mêmes en bijection avec l'ensemble des diviseurs positifs de $36 = 2^2 \cdot 3^2$. Il y a donc $(2+1) \times (2+1) = 9$ sous-corps de $\mathbf{Q}(\zeta_{37})$ (en comptant $\mathbf{Q}$ et $\mathbf{Q}(\zeta_{37})$).
5. On utilise le fait qu'il existe une infinité de nombres premiers $p \equiv 1 \pmod{\ell}$. Soit p un tel nombre premier. Puisque $\ell | p - 1$, il existe (par les mêmes arguments que précédemment) un unique sous-corps $K_p \subset \mathbf{Q}(\zeta_p)$ tel que $\mathrm{Gal}(K_p/\mathbf{Q}) \cong \mathbf{Z}/\ell\mathbf{Z}$. Montrons que les corps K_p sont deux à deux non isomorphes. Par l'absurde, supposons $K_p \cong K_{p'}$ avec $p \neq p'$. Puisque $K_p/\mathbf{Q}$ (resp. $K_{p'}/\mathbf{Q}$) est galoisienne, l'image de K_p (resp. $K_{p'}$) dans $\mathbf{C}$ ne dépend pas du choix du plongement $K_p \hookrightarrow \mathbf{C}$ (resp. $K_{p'} \hookrightarrow \mathbf{C}$) et est incluse dans $\mathbf{Q}(\zeta_p)$ (resp. $\mathbf{Q}(\zeta_{p'})$). On en déduit $\mathbf{Q}(\zeta_p) \cap \mathbf{Q}(\zeta_{p'}) \neq \mathbf{Q}$ ne qui contredit le fait que $\mathbf{Q}(\zeta_p)$ et $\mathbf{Q}(\zeta_{p'})$, vus comme sous-corps de $\mathbf{C}$, sont linéairement disjointes sur $\mathbf{Q}$.

Exercice 2

1. L'application $\psi : L \times L \to L^n$ définie par $\psi(x,y) = (x\sigma_i(y))_{1\leq i\leq n}$ est K-bilinéaire (chaque σ_i est K-linéaire). On conclut par la propriété universelle de $L \otimes_K L$.
2. Les K-espaces vectoriels $L \otimes_K L$ et L^n sont de même dimension n^2. Il suffit donc de montrer que φ est injective. Soit $(e_i)_{1\leq i\leq n}$ une K-base de L. D'après le cours les $e_i \otimes e_j$ forment une K-base de $L \otimes_K L$ et il suffit de montrer que les $\varphi(e_i \otimes e_j)$ sont linéairement indépendants sur K. Par l'absurde, supposons $\sum_{i,j=1}^n \lambda_{i,j}\varphi(e_i \otimes e_j) = 0$ avec $\lambda_{i,j} \in K$. Pour tout $\sigma \in G$, on a donc
$$\sum_{i,j=1}^{n} \lambda_{i,j} e_i \sigma(e_j) = 0.$$
Posons $e'_j = \sum_{i=1}^n \lambda_{i,j} e_i \in L$, de sorte que $\sum_{j=1}^n e'_j \sigma(e_j) = 0$ pour tout $\sigma \in G$. D'après le lemme d'indépendance des caractères de Dedekind, les éléments de G forment une famille L-libre du L-espace vectoriel $\mathrm{End}_K(L)$. On a un isomorphisme de L-espaces vectoriels $\mathrm{End}_K(L) \cong L^n$ donné par $f \mapsto (f(e_1), \ldots, f(e_n))$. Comme $\mathrm{card}(G) = n$, les éléments de G forment une base de ce L-espace vectoriel. Or, la relation précédente indique que les éléments de G appartiennent tous au sous-L-espace vectoriel
$$H = \Big\{(x_1, \ldots, x_n) \in L^n \Big| \sum_{j=1}^{n} e'_j x_j = 0\Big\}.$$
La seule possibilité est donc $e'_1 = \ldots = e'_n = 0$ d'où $\lambda_{i,j} = 0$ pour tout i, j.
3. Par définition de t, on a $\sum_{k=1}^r x_k \sigma_j^{-1}\sigma_i(y_k) = \delta_{i,j}$ d'où $P(x_1, \ldots, x_r) = 1$.
4. Montrons par récurrence sur $r \geq 1$ que toute fonction polynomiale $L^r \to L$ s'annulant sur K^r est nulle sur L^r. Pour $r = 1$ cela résulte du fait qu'un polynôme ayant une infinité de racines est nul. Supposons le résultat au rang r et montrons-le au rang $r+1$. Soit $Q \in L[X_1, \ldots, X_{r+1}]$ tel que la fonction polynomiale associée à Q est nulle sur K^{r+1}. Posons $Q = \sum_{i=0}^d Q_i \cdot X_{r+1}^i$ avec $Q_i \in L[X_1, \ldots, X_r]$. Pour tout $\lambda_1, \ldots, \lambda_r \in K$, le polynôme $\sum_{i=0}^d Q_i(\lambda_1, \ldots, \lambda_r) X_{r+1}^i \in L[X_{r+1}]$ admet une infinité de racines, donc est nul c'est-à-dire $Q_i(\lambda_1, \ldots, \lambda_r) = 0$ pour tout i. Par hypothèse de récurrence $Q_i = 0$ pour tout i et donc $Q = 0$.
D'après la question 3, on en déduit que P n'est pas identiquement nulle sur K^r. Il existe donc $\lambda_1, \ldots, \lambda_r \in K$ tels que $P(\lambda_1, \ldots, \lambda_{r+1}) \neq 0$.
5. Notons $M \in \mathrm{GL}_n(L)$ la matrice définie par $M_{i,j} = \sum_{k=1}^r \lambda_k \sigma_j^{-1}\sigma_i(y_k) = \sigma_j^{-1}\sigma_i(a)$ pour $1 \leq i, j \leq n$. Il suffit de montrer que la famille $(\sigma_i(a))_{1\leq i\leq n}$ est K-libre. Par l'absurde, supposons $\sum_{i=1}^n \mu_i \sigma_i(a) = 0$ avec $\mu_i \in K$. En appppliquant σ_j^{-1}, il vient $\sum_{i=1}^n \mu_i M_{i,j} = 0$ pour tout j, c'est-à-dire qu'une combinaison linéaire des lignes de M est nulle. Comme $\det(M) \neq 0$, il vient $\mu_i = 0$ pour tout i.
6. Posons $q = p^m$ avec p premier et $m \geq 1$. Comme on est en caractéristique p, on a $(x+y)^p = x^p + y^p$ pour tout $x, y \in L$. Une application répétée de cette identité montre $F(x+y) = F(x) + F(y)$ pour tout $x, y \in L$. De plus

pour tout $\lambda \in \mathbf{F}_q$ et $x \in L$ on a $F(\lambda x) = (\lambda x)^q = \lambda^q x^q = \lambda x^q = \lambda F(x)$. Ainsi F est K-linéaire. **Attention** : si q n'est pas premier, alors $\binom{q}{k}$ n'est en général pas divisible par q. Par exemple $\binom{4}{2} = 6$.

On sait que $F^n = \mathrm{id}_L$, donc $X^n - 1 \in K[X]$ annule F. De plus, supposons que $Q = \sum_{i=0}^{n-1} a_i X^i \in K[X]$ annule F. Alors en posant $R = \sum_{i=0}^{n-1} a_i T^{q^i}$, on a $R(x) = 0$ pour tout $x \in L$. Comme $\mathrm{card}(L) = q^n > \deg(R)$, on en déduit $R = 0$ et donc $Q = 0$. Par suite le polynôme minimal μ de F sur K est égal à $X^n - 1$.

7. L est un K-espace vectoriel de dimension finie donc a fortiori un $K[X]$-module de type fini. D'après le théorème de structure, on a un isomorphisme de $K[X]$-modules $L \cong K[X]^r \oplus \bigoplus_{i=1}^{s} K[X]/(P_i)$ avec $r \geq 0$ et $P_1 | \cdots | P_s$ polynômes unitaires non constants. Puisque $\dim_K L < +\infty$ il vient $r = 0$. De plus, par définition du polynôme minimal d'un endomorphisme, on a $P_s = \mu$. Enfin, la comparaison des dimensions donne $s = 1$, d'où un isomorphisme $L \cong K[X]/\mu$.
   Soit maintenant $a \in L$ l'élément correspondant à la classe de 1 via cet isomorphisme. Alors pour tout $k \geq 0$, la classe de X^k correspond à $F^k(a) \in L$. On en déduit que $a, F(a), \ldots, F^{n-1}(a)$ sont linéairement indépendants sur K. D'après le cours $G = \mathrm{Gal}(L/K)$ est cyclique d'ordre n engendré par F. Donc $(\sigma(a))_{\sigma \in G}$ est une base normale de L/K.

Exercice 3

1. Notons ρ_M (resp. ρ_N) l'application A-linéaire canonique $M \to M_\mathfrak{p}$ (resp. $N \to N_\mathfrak{p}$). La propriété universelle du localisé $M_\mathfrak{p}$ appliquée à l'application A-linéaire $\rho_N \circ u : M \to N_\mathfrak{p}$ donne le résultat.
2. Montrons (a) $\Rightarrow$ (b). Soit $\mathfrak{p}$ idéal premier de A. Soit $\frac{x}{s} \in \ker(u_\mathfrak{p})$ avec $x \in M$ et $s \notin \mathfrak{p}$. Alors $0 = u_\mathfrak{p}(\frac{x}{s}) = \frac{u(x)}{s}$ donc il existe $t \notin \mathfrak{p}$ tel que $tu(x) = 0$. Donc $u(tx) = 0$ puis $tx = 0$ ce qui entraîne $\frac{x}{s} = 0$.
   L'implication (b) $\Rightarrow$ (c) est évidente.
   Montrons (c) $\Rightarrow$ (a). Soit $x \in \ker(u)$. Posons $I = \{a \in A : ax = 0\}$. C'est un idéal de A. Supposons par l'absurde $I \neq A$. Alors il existe $\mathfrak{m}$ idéal maximal de A tel que $I \subset \mathfrak{m}$. Utilisons l'injectivité de $u_\mathfrak{m}$. Comme $u_\mathfrak{m}(\frac{x}{1}) = \frac{u(x)}{1} = 0$. Donc $\frac{x}{1} = 0$ dans $M_\mathfrak{m}$ et il existe $s \notin \mathfrak{m}$ tel que $sx = 0$, d'où $s \in I$, contradiction.
3. Montrons (a) $\Rightarrow$ (b). Soit $\mathfrak{p}$ idéal premier de A. Soit $\frac{y}{s} \in N_\mathfrak{p}$ avec $y \in N$ et $s \notin \mathfrak{p}$. Comme u est surjectif, il existe $x \in M$ tel que $y = u(x)$. Alors $u_\mathfrak{p}(\frac{x}{s}) = \frac{1}{s} \cdot u_\mathfrak{p}(\frac{x}{1}) = \frac{1}{s} \cdot \frac{u(x)}{1} = \frac{y}{s}$.
   L'implication (b) $\Rightarrow$ (c) est évidente.
   Montrons (c) $\Rightarrow$ (a). Soit $y \in N$. Posons $I = \{a \in A : ay \in u(M)\}$. C'est un idéal de A. Supposons par l'absurde $I \neq A$. Alors il existe $\mathfrak{m}$ idéal maximal

de A tel que $I \subset \mathfrak{m}$. Utilisons la surjectivité de $u_{\mathfrak{m}}$. On a $\frac{y}{1} = u_{\mathfrak{m}}(\frac{x}{s})$ avec $x \in M$ et $s \notin \mathfrak{m}$. Alors $\frac{y}{1} = \frac{u(x)}{s}$ donc il existe $t \notin \mathfrak{m}$ tel que $tsy = tu(x) = u(tx) \in u(M)$. Donc $ts \in I$, ce qui contredit $ts \notin \mathfrak{m}$.

Exercice 4

1. D'après le cours $(\mathbf{Z}/n\mathbf{Z})_{(p)} \cong (\mathbf{Z}/n\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Z}_{(p)} \cong \mathbf{Z}_{(p)}/n\mathbf{Z}_{(p)}$. Posons $n = p^{\alpha}m$ avec $\alpha \geq 0$ et $p \nmid m$. Comme m est inversible dans $\mathbf{Z}_{(p)}$ on a $n\mathbf{Z}_{(p)} = p^{\alpha}\mathbf{Z}_{(p)}$. Si $\alpha = 0$ alors $(\mathbf{Z}/n\mathbf{Z})_{(p)} = 0$. Si $\alpha \geq 1$ alors $\mathbf{Z}/n\mathbf{Z}$ et $\mathbf{Z}/p^{\alpha}\mathbf{Z}$ ont même localisé en p. Mais $\mathbf{Z}/p^{\alpha}\mathbf{Z}$ est déjà local d'idéal maximal $p(\mathbf{Z}/p^{\alpha}\mathbf{Z})$, de sorte que $(\mathbf{Z}/p^{\alpha}\mathbf{Z})_{(p)} \cong \mathbf{Z}/p^{\alpha}\mathbf{Z}$. Dans tous les cas $(\mathbf{Z}/n\mathbf{Z})_{(p)} \cong \mathbf{Z}/p^{\alpha}\mathbf{Z}$ avec $\alpha = v_p(n)$.
2. Soit G un groupe abélien fini. Par le théorème de structure G est somme directe de groupes cycliques. Puisque la localisation commute aux sommes directes, il suffit de montrer le résuitat pour $G = \mathbf{Z}/n\mathbf{Z}$. Or $\mathbf{Z}/n\mathbf{Z} \cong \bigoplus_{p|n} \mathbf{Z}/p^{v_p(n)}\mathbf{Z}$. On conclut grâce à la question 1.
3. L'implication directe est immédiate. Dans l'autre sens, soit M et N des groupes abéliens de type fini tels que $M_{(p)} \cong N_{(p)}$ pour tout p premier. Par le théorème de structure, on a $M \cong \mathbf{Z}^r \oplus G$ et $N \cong \mathbf{Z}^s \oplus H$ avec $r, s \geq 0$ et G, H groupes abéliens finis. Localisons en p ces isomorphismes. On obtient un isomorphismes de $\mathbf{Z}_{(p)}$-modules $\mathbf{Z}_{(p)}^r \oplus G_{(p)} \cong \mathbf{Z}_{(p)}^s \oplus H_{(p)}$. Comme $\mathbf{Z}_{(p)}$ est principal (c'est même un anneau de valuation discrète), l'unicité dans le théorème de structure donne $r = s$ et $G_{(p)} \cong H_{(p)}$ pour tout p premier. On conclut grâce à la question 2.
4. Dans cette question les diviseurs élémentaires d'un groupe abélien fini M désignent les entiers $d_1, \ldots, d_n \geq 2$, déterminés de manière unique, tels que $M \cong \bigoplus_{i=1}^n \mathbf{Z}/d_i\mathbf{Z}$ et $d_1 | \cdots | d_n$. Il est clair que $M \otimes_{\mathbf{Z}} M$ est un groupe abélien fini. Déterminons ses diviseurs élémentaires. Par distributivité du produit tensoriel par rapport aux sommes directes, on a

$$M \otimes_{\mathbf{Z}} M \cong \bigoplus_{i,j=1}^{n} M_{i,j}$$

avec $M_{i,j} \cong \mathbf{Z}/d_i\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/d_j\mathbf{Z} \cong \mathbf{Z}/d_{\min(i,j)}\mathbf{Z}$ (on le montre grâce à l'isomorphisme $G \otimes_{\mathbf{Z}} \mathbf{Z}/d\mathbf{Z} \cong G/dG$, valable pour tout groupe abélien G). Par suite les diviseurs élémentaires de $M \otimes_{\mathbf{Z}} M$ sont :

$$\underbrace{d_1, \ldots, d_1}_{2n-1}, \underbrace{d_2, \ldots, d_2}_{2n-3}, \ldots, \underbrace{d_i, \ldots, d_i}_{2n-2i+1}, \ldots, d_n.$$

Notons e_i le générateur canonique de $\mathbf{Z}/d_i\mathbf{Z} \subset M$. Remarquons que $e_i \otimes e_j$ est un générateur du groupe cyclique $M_{i,j}$.
Par définition $\mathrm{Sym}^2 M = (M \otimes_{\mathbf{Z}} M)/R$ où R est le sous-groupe de $M \otimes_{\mathbf{Z}} M$ engendré par les $x \otimes y - y \otimes x$ avec $x, y \in M$. On vérifie que R est engendré

par les $e_i \otimes e_j - e_j \otimes e_i$ avec $1 \leq i < j \leq n$. On en déduit

$$M \otimes_{\mathbf{Z}} M = \Big(\bigoplus_{1 \leq i \leq j \leq n} M_{i,j} \Big) \oplus R.$$

Les diviseurs élémentaires de $\mathrm{Sym}^2 M$ sont donc

$$\underbrace{d_1, \ldots, d_1}_{n}, \underbrace{d_2, \ldots, d_2}_{n-1}, \ldots, \underbrace{d_i, \ldots, d_i}_{n-i+1}, \ldots, d_n.$$

De même $\bigwedge^2 M = (M \otimes_{\mathbf{Z}} M)/R'$ où R' est le sous-groupe de $M \otimes_{\mathbf{Z}} M$ engendré par les $x \otimes x$ avec $x \in M$. On vérifie que R' est engendré par les $e_i \otimes e_i$ avec $1 \leq i \leq n$ et les $e_i \otimes e_j + e_j \otimes e_i$ avec $1 \leq i < j \leq n$. On en déduit

$$M \otimes_{\mathbf{Z}} M = \Big(\bigoplus_{1 \leq i < j \leq n} M_{i,j} \Big) \oplus R'.$$

Les diviseurs élémentaires de $\bigwedge^2 M$ sont donc

$$\underbrace{d_1, \ldots, d_1}_{n-1}, \underbrace{d_2, \ldots, d_2}_{n-2}, \ldots, \underbrace{d_i, \ldots, d_i}_{n-i}, \ldots, d_{n-1}.$$

Exercice 5

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

Première étape : réduction au cas local. D'après l'exercice 3 (question 2), il suffit de montrer que $u_{\mathfrak{m}}$ est injectif pour tout idéal maximal $\mathfrak{m}$ de A. Or $M_{\mathfrak{m}} = M \otimes_A A_{\mathfrak{m}}$ est un $A_{\mathfrak{m}}$-module de type fini, et toujours d'après l'exercice 3 (question 3), on sait que $u_{\mathfrak{m}}$ est surjectif. Par conséquent, si on connaît le résultat pour tout A local, on le déduit pour A quelconque. Dans la suite, on suppose donc A local. On note $\mathfrak{m}$ son unique idéal maximal et $k = A/\mathfrak{m}$.

Deuxième étape : lemme de Nakayama. Posons $\overline{M} = M/\mathfrak{m}M \cong M \otimes_A (A/\mathfrak{m})$. C'est un $A/\mathfrak{m}$-module de type fini, autrement dit un k-espace vectoriel de dimension finie. Soit $e_1, \ldots, e_n \in M$ tels que $(\overline{e_1}, \ldots, \overline{e_n})$ est une k-base de $\overline{M}$. Posons $N = M/(\sum_{i=1}^n Ae_i)$. Alors $N/\mathfrak{m}N \cong \overline{M}/(\sum_{i=1}^n k\overline{e_i}) = 0$. D'après lemme de Nakayama $N = 0$, donc $e_1, \ldots, e_n$ engendrent M comme A-module.

Troisième étape : astuce du déterminant. Posons $u(e_j) = \sum_{i=1}^n \lambda_{i,j} e_i$ avec $\lambda_{i,j} \in A$. Posons $B = (\lambda_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(A)$. Notons $\overline{u} : \overline{M} \to \overline{M}$ la réduction de u modulo $\mathfrak{m}M$. Alors $\overline{u} = u \otimes \mathrm{id}_k$ est k-linéaire surjective, donc est bijective. Or la matrice de $\overline{u}$ dans la base $(\overline{e_1}, \ldots, \overline{e_n})$ n'est autre que $\overline{B} \in \mathrm{GL}_n(k)$. Donc $\overline{\det(B)} = \det(\overline{B}) \in k^\times$. Comme A est local cela entraîne $\det(B) \in A^\times$. D'après l'astuce du déterminant, le polynôme $P(X) = \det(X \cdot I - B) \in A[X]$ vérifie $P(u) = 0$. Posons $P(X) = \lambda + XQ(X)$ avec $\lambda = (-1)^n \det(B) \in A^\times$. Finalement, soit $m \in M$ tel que $u(m) = 0$. Alors $0 = P(u)(m) = \lambda m + Q(u) \circ u(m) = \lambda m$ et donc $m = 0$.