Révisions

Exercice 1

Posons $A = \{a + ib\sqrt{5} \in \mathbf{C}/a, b \in \mathbf{Z}\}$.
1. Montrer que c'est un anneau.
2. Montrer que l'application $A \to \mathbf{R}$ qui à z associe $z\bar{z}$ est à valeurs dans $\mathbf{Z}$ et multiplicative.
3. Déterminer A^*.
4. Montrer que les éléments 2, 3, $1 + i\sqrt{5}$, $1 - i\sqrt{5}$ sont irréductibles dans A.
5. Montrer que 6 admet deux décompositions en produits d'irréductibles. L'anneau A est-il factoriel ?

Exercice 2

Soit K un corps. Soit A un anneau factoriel qui n'est pas un corps.
1. Montrer que l'idéal de $K[X, Y]$ engendré par X et Y n'est pas prinicipal.
2. En déduire que l'anneau $K[X, Y]$ est factoriel mais pas principal.
3. Soit a un élément non nul et non inversible de A. Montrer que l'idéal de l'anneau $A[X]$ engendré par a et X n'est pas principal.
4. En déduire que l'anneau $A[X]$ est factoriel mais pas principal.

Exercice 3

1. Déterminer les polynômes irréductibles de degré ≤ 2 sur $\mathbf{F}_2$.
2. En déduire que le polynôme $X^5 + X^3 + 1$ est irréductible sur $\mathbf{F}_2$.
3. En déduire que le polynôme $X^5 + 5X^3 + 5 \in \mathbf{Z}[X]$ est irréductible sur $\mathbf{Z}$.
4. Montrer cette dernière irréductibilité sans utiliser la question 2.

Exercice 4

Soit K un corps de caractéristique différente de 2 et 3. Considérons le polynôme $P = X^3 + pX + q \in K[X]$. Supposons-le scindé et notons α, β et γ ses racines. On se propose de déterminer ces racines en fonctions de p et q. On suppose que K contient une racine cubique primitive de l'unité j.
1. Soit $Q \in K[X]$ de degré 3. Montrer qu'il existe $a \in K^*$ et $b \in K$ tel que $Q(aX + b)$ ait un coefficient du second degré nul.
2. Posons $R_j(X_1, X_2, X_3) = (X_1 + jX_2 + j^2X_3)^3 \in K[X_1, X_2, X_3]$. Montrer que l'orbite de R_j sous l'action du groupe symétrique $\mathcal{S}_3$ contient deux éléments : R_j et un autre élément qu'on notera R_{j^2}.
3. Montrer que les polynômes $R_j + R_{j^2}$ et $Q = (X_1 + jX_2 + j^2X_3)(X_1 + j^2X_2 + jX_3)$ sont symétriques. Exprimer $R_j + R_{j^2}$ et $R_jR_{j^2} = Q^3$ en fonction des polynômes symétriques élémentaires.
4. Posons $u = R_j(\alpha, \beta, \gamma) \in K$ et $v = R_{j^2}(\alpha, \beta, \gamma) \in K$. Exprimer $u + v$ et uv en fonction de p et q.
5. Exprimer α, β et γ en fonction de u et v.

Exercice 5

Lesquels des groupes abéliens suivants sont isomorphes entre eux: $\mathbf{Z}/2008\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}\times\mathbf{Z}/251\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}\times\mathbf{Z}/502\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/251\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/1004\mathbf{Z}$?

Exercice 6

Soit K un corps. Soit E un K-espace vectoriel. Soit u un endomorphisme de E.
1. Rappeler comment u fait de E un $K[X]$-module.
2. Montrer que si E est de dimension finie comme K espace vectoriel, E est de type fini comme $K[X]$-module. Notons alors $\mu(X)$ le polynôme minimal de u. Montrer que E est un $K[X]/(\mu(X))$-module et que c'est un $K[X]$-module de torsion.

3. Posons $E = K[T]$. Considérons le cas où u est la multiplication par T. Montrer que E est un $K[X]$-module libre.
4. Posons $E = K[T]$. Considérons le cas où u est la dérivation dans $K[T]$. Montrer que E n'est pas de type fini comme $K[X]$-module (on pourra montrer que, si c'était le cas, il existerait des polynômes $P_1, \ldots, P_r \in K[T]$ tels que tout élément de $K[T]$ soit combinaison K-linéaire des dérivées successives de $P_1, \ldots, P_r$). Montrer que tout élément de E est de torsion.

Exercice 7

Soit L un corps contenant $\mathbf{F}_2$. Soient x et y des éléments de L vérifiant $x^2 + x + 1 = 0$ et $y^3 + y + 1 = 0$. Considérons les sous-corps $\mathbf{F}_2(x)$, $\mathbf{F}_2(y)$ et $\mathbf{F}_2(x, y)$ de L.
1. Montrer que les racines des polynômes $X^2 + X + 1$ dans L sont x et $x^2 = x + 1$, puis que les racines des polynômes $X^3 + X + 1$ dans L sont y et y^2 et $y^4 = y^2 + y$.
2. Montrer que les extensions $\mathbf{F}_2(x)|\mathbf{F}_2$, $\mathbf{F}_2(y)|\mathbf{F}_2$ et $\mathbf{F}_2(x, y)|\mathbf{F}_2$ sont de degrés 2, 3 et 6 respectivement. En déduire que les corps $\mathbf{F}_2(x)$, $\mathbf{F}_2(y)$ et $\mathbf{F}_2(x, y)$ ont respectivement 4, 8 et 64 éléments.
3. Déterminer le polynôme minimal sur $\mathbf{F}_2$ de $x + y$.
4. Démontrer que tout élément de $\mathbf{F}_2(x, y)^*$ est d'ordre divisant 63.
5. Montrer que x et y sont d'ordre 3 et 7 respectivement dans $\mathbf{F}_2(x, y)^*$. En déduire l'ordre de xy.

Exercice 8

Considérons les polynômes $X^3 - 3X + 1$ et $X^4 - 3 \in \mathbf{Q}[X]$.
1. Ces polynômes sont-il irréductibles sur $\mathbf{Q}$?
2. En déterminer un corps de rupture de $X^4 - 3$ dans $\mathbf{R}$. Quel est son degré ?
3. Ce polynôme admet-il un corps de décomposition dans $\mathbf{R}$?
4. Quel est le degré d'un corps de décomposition de $X^4 - 3$ sur $\mathbf{Q}$?
5. Soit a une racine de $X^3 - 3X + 1$ dans $\mathbf{C}$.
6. Quel est le degré d'un corps de décomposition de $X^3 - 3X + 1$ sur $\mathbf{Q}$?

Exercice 9

Soit K un corps de caractéristique 0 ou > 3. Soit $P = X^3 + aX + b \in K[X]$. Soit L un corps de décomposition de P sur K. Notons α_1, α_2 et α_3 les racines de P dans L. Posons $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in L$ et $\Delta = \delta^2$. On a $\Delta = -4a^3 - 27b^2$.
1. Montrer que P est irréductible sur K si et seulement si P est sans racine dans K.
2. Montrer que $L|K$ est galoisienne.
3. Rappeler comment $\mathrm{Gal}(L/K)$ s'identifie à un sous-groupe du groupe symétrique $\mathcal{S}_3$. Soit $\sigma \in \mathrm{Gal}(L/K)$. Montrer que $\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$, où $\mathrm{sgn}(\sigma)$ est la signature de σ.
4. Supposons P irréductible sur K. Si $\delta \in K$, montrer que $\mathrm{Gal}(L/K)$ est d'ordre 3. En déduire que $L|K$ est de degré 3 puis que $L = K(\alpha_1) = K(\alpha_2) = K(\alpha_3)$.
5. Supposons P irréductible sur K. Si $\delta \notin K$, montrer que $\mathrm{Gal}(L/K)$ contient un élément d'ordre 2. En déduire que $\mathrm{Gal}(L/K)$ n'est pas d'ordre 2. Conclure que $\mathrm{Gal}(L/K)$ est d'ordre 6.
6. Quels sont les groupes de Galois des polynômes $X^3 - 3X + 1$ et $X^3 - X + 1 \in \mathbf{Q}[X]$?

Exercice 10

On se propose de montrer que le corps $\mathbf{C}$ est algébriquement clos. On admettra que tout polynôme à coefficients réels de degré impair possède un zéro dans $\mathbf{R}$.
1. Montrer que si toute extension finie de $\mathbf{C}$ est égale à $\mathbf{C}$, le corps $\mathbf{C}$ est algébriquement clos.
2. Montrer que tout nombre complexe possède une racine carrée. En déduire que tout polynôme de degré 2 admet une racine dans $\mathbf{C}$, puis que $\mathbf{C}$ ne possède pas d'extension de degré 2.
3. Soit K_0 une extension finie de $\mathbf{C}$. Montrer qu'il existe une extension finie $K|K_0$ telle que l'extension $K|\mathbf{R}$ soit galoisienne.

4. Notons alors G le groupe de Galois de l'extension $K|\mathbf{R}$. Soit H un 2-sous-groupe de Sylow de G. Notons L le sous-corps de K formé par les éléments invariants par H. En termes des ordres des groupes G et H, quel est l'ordre de l'extension $L|\mathbf{R}$?
5. Montrer qu'il existe $\alpha \in L$ tel que $L = \mathbf{R}(\alpha)$ et α racine d'un polynôme irréductible de degré impair de $\mathbf{R}[X]$.
6. En déduire que $\alpha \in \mathbf{R}$ puis que G est un 2-groupe.
7. Montrer que l'extension $K|\mathbf{C}$ est galoisienne. Notons G_1 son groupe de Galois. Montrer que c'est un 2-groupe.
8. Soit G_2 un sous-groupe d'indice 2 de G_1. Notons L_2 le sous-corps de K formé par les éléments invariants par G_2. Quel est le degré de l'extension $L_2|\mathbf{C}$? En déduire que G_1 n'a pas de sous-groupe d'indice 2. Conclure.