TD n°2.

1 Groupes

Exercice 1. Soit X_n un polygone régulier à n sommets. On note $G(X_n)$ (resp. $G^+(X_n)$) le groupe des isométries (resp. isométries positives) de X_n.

a) Montrer que $G^+(X_n)$ est un sous-groupe distingué d'indice deux dans $G(X_n)$.
b) Montrer que $G^+(X_n)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
c) Décrire $G(X_n)$ comme produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 2. Soit p un nombre premier et G un groupe de cardinal p^n. On note $Z(G) := \{x \in G | \forall y \in G, xy = yx\}$. En considérant l'action de G sur lui-même par conjugaison, montrer que $Z(G) \neq \{1\}$.

Exercice 3. On dit qu'un groupe G est nilpotent s'il existe une suite de sous-groupes distingués de G :

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tel que pour tout i, G_{i+1}/G_i soit dans le centre de G/G_i.

a) montrer que tout sous-groupe et tout quotient d'un groupe nilpotent est nilpotent.
b) Montrer qu'un p-groupe est nilpotent.
c) Soit $U_n(k)$ l'ensemble des matrices (à coefficient dans un corps k) $n \times n$ triangulaires supérieures n'ayant que des 1 sur la diagonale. Montrer que $U_n(k)$ est un sous-groupe nilpotent de $GL_n(k)$.

Exercice 4. Soit G un groupe fini d'ordre n ayant pour tout nombre premier p un unique p-Sylow, noté G_p.

a) Soient p, q deux nombres premiers distincts. Soient $g \in G_p$ et $h \in G_q$. Montrer que $ghg^{-1}h^{-1} \in G_p \cap G_q = \{1\}$.
b) En déduire un isomorphisme $\prod_{p|n} G_p \to G$.

Exercice 5. Soit G un groupe simple (i.e. sans sous-groupe distingué différent de $\{1\}$ et G) de cardinal 60. Pour $p = 2, 3, 5$, on note n_p le nombre de p-Sylow de G.

a) Montrer que $n_5 = 6$. En déduire le nombre d'éléments d'ordre 5 dans G.
b) Montrer que $n_3 = 10$. En déduire le nombre d'éléments d'ordre 3 dans G.
c) Montrer que G ne contient pas d'élément d'ordre 6 ou 10.
d) Montrer que si H_1 et H_2 sont deux 2-Sylow de G, alors $H_1 \cap H_2 = \{1\}$ (on pourra considérer le commutateur d'un élément non trivial de l'intersection de $H_1 \cap H_2$).
e) Montrer que $n_2 = 5$.
f) Montrer que G est isomorphe à $\mathfrak{A}_5$.

2 Groupes abéliens

Exercice 6. (2.1.10) Soient X et Y deux groupes abéliens. On définit sur

$$\operatorname*{Hom}_{Ab}(X, Y) = \{\text{Morphismes de groupes abéliens } X \to Y\}$$

une addition par

$$\forall x \in X, \quad (f + g)(x) = f(x) + g(x).$$

Montrer que l'on définit ainsi une structure de groupe abélien sur $\mathrm{Hom}_{Ab}(X, Y)$.

Exercice 7. (2.2.6) Montrer qu'un groupe abélien A non trivial est simple si et seulement si il est cyclique d'ordre premier.

Exercice 8. (2.2.8) Soit A un groupe abélien et $n \geq 1$ un entier naturel. Montrer que si B est un quotient de A qui vérifie $B[n] = B$, alors B est un quotient de A/nA.

Exercice 9. (2.2.9) Soit A un groupe abélien fini. Si $B \subset A$ est un sous-groupe dont l'ordre est premier à celui de A/B, alors A est isomorphe à $B \oplus A/B$.

Exercice 10. (2.2.10) Soit A un groupe abélien fini. Montrer que

a) L'ensemble $I = \{m \in \mathbb{Z};\ mA = 0\}$ est un sous-groupe non nul de $\mathbb{Z}$. On appelle son générateur positif l'*exposant* de A.

b) L'exposant de A divise l'ordre de A.

c) L'exposant de A est le produit des exposants des composantes p-primaires $A(p)$ de A.

d) Il existe un élément $a \in A$ dont l'ordre est égal à l'exposant de A.

Exercice 11. (2.2.11) Dualité dans les groupes abéliens finis et théorème de structure. Soit A est un groupe abélien fini. On appelle *caractère* de A un homomorphisme de A dans le groupe $\mathbb{C}^*$ des nombres complexes non nuls. Notons n le cardinal de A et d son exposant.

a) Montrer que les caractères de G forment un groupe $\widehat{G}$ dont l'élément neutre est le *caractère trivial* **1** qui prend la valeur constante 1.

b) Montrer que l'exposant de $\widehat{A}$ divise d (celui de A).

c) Montrer que, si A est cyclique d'ordre n, $\widehat{A}$ est cyclique d'ordre n.

d) Montrer que, si A est une somme directe $B \oplus C$, on a $\widehat{A} \simeq \widehat{B} \oplus \widehat{C}$.

e) Pour tout $\alpha \in \mathrm{Hom}(A, B)$, on définit $\widehat{\alpha} : \widehat{B} \to \widehat{A}$ par

$$\forall \chi \in \widehat{B} = \mathrm{Hom}(B, \mathbb{C}^*), \quad \widehat{\alpha}(\chi) = \chi \circ \alpha \in \mathrm{Hom}(A, \mathbb{C}^*) = \widehat{A}.$$

Montrer que $\widehat{\alpha} \in \mathrm{Hom}(\widehat{B}, \widehat{A})$.

f) Montrer que si α est surjectif, $\widehat{\alpha}$ est injectif.

g)* Montrer que si α est injectif, $\widehat{\alpha}$ est surjectif.

h) D'après l'exercice précédent, il existe un élément a de A dont l'ordre est d. Notons B le groupe engendré par a et α l'inclusion de B dans A. Montrer qu'il existe un élément $\chi \in \widehat{A}$ tel que $\chi(a)$ soit d'ordre d. Montrer que l'on a $A \simeq B \oplus \mathrm{Ker}\,\chi$.

i) Montrer que tout groupe abélien fini est somme directe de groupes cycliques.

j) Pour $a \in A$, on note $a^\vee$ l'application définie sur $\widehat{A}$ par $a^\vee(\chi) = \chi(a)$. Montrer que $a \mapsto a^\vee$ est un isomorphisme (de *bidualité*, ou *canonique*) de A sur $\widehat{\widehat{A}}$.

Exercice 12. (2.2.13) Structure de $(\mathbb{Z}/n\mathbb{Z})^*$**.** Soient p un nombre premier et $n \geq 1$ un entier.

a) Montrer que si $p^n > 2$, alors on a

$$\forall x, y \in \mathbb{Z}, \quad (x + p^n y)^p \equiv x^p + p^{n+1} x^{p-1} y \pmod{p^{n+2}}.$$

b) Que se passe-t-il si $p^n = 2$?

c) Montrer que si $p^n > 2$, $m \geq 0$, $x \equiv 1 \pmod{p^n}$ et $x \not\equiv 1 \pmod{p^{n+1}}$, alors le groupe

$$\mathrm{Ker}((\mathbb{Z}/p^{n+m}\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*)$$

est cyclique d'ordre p^m. Il est engendré par la classe de x.

d) Montrer que si $p > 2$, alors le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique (voir 2.2.9).

e) Montrer que si $n \geq 2$, alors l'application

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{n-2}Z \to (\mathbb{Z}/2^n\mathbb{Z})^*, \quad (a, b) \mapsto (-1)^a 5^b \pmod{2^n}$$

est un isomorphisme de groupes.

f) Montrer que groupe $(\mathbb{Z}/m\mathbb{Z})^*$ est cyclique si et seulement si $m = 1$, 2, 4, ou m est le la forme p^n ou $2p^n$, où $p > 2$ est un nombre premier et $n \geq 1$.

Exercice 13. (2.3.6) Décrire (à isomorphisme près) tous les groupes abéliens Y d'ordre 8 et tous les groupes abéliens X d'ordre 16. Pour chaque X, dire quels Y sont (isomorphes à un) sous-groupe de X.

Exercice 14. (2.3.7) Soit X un groupe abélien d'ordre 216. Montrer qu'il existe deux entiers $a, b \in [1, 2, 3]$ tels que $|X[2]| = 2^a$ et $|X[3]| = 3^b$. Décrire la structure de X en termes de a et b. Que se passe-t-il si on remplace 216 par 432 ?

Exercice 15. (2.3.8) Soit X un groupe abélien d'ordre n, et d un diviseur de n. Montrer que X a moins un sous-groupe X^d d'ordre d et un quotient X_d d'ordre d. Montrer que X est cyclique si et seulement si X^d (respectivement X_d) est unique pour tout d divisant n.

Exercice 16. (2.3.9) Décrire tous les groupes abéliens X qui admettent un sous-groupe Y tel que $Y \simeq \mathbb{Z}/4\mathbb{Z}$ et $X/Y \simeq \mathbb{Z}/2\mathbb{Z}$. Même question pour $Y \simeq \mathbb{Z}/6\mathbb{Z}$ et $X/Y \simeq \mathbb{Z}/12\mathbb{Z}$.

Exercice 17. (2.3.10) Soit $(d_i)_{1\leq i\leq m}$ et $(e_i)_{1\leq i\leq n}$ deux familles d'entiers naturels tels que $1 < d_1|d_2|\dots|d_m$ et $1 < e_1|e_2|\dots|e_n$. On pose $X = \prod_{i=1}^{m} \mathbb{Z}/d_i\mathbb{Z}$ et $Y = \prod_{i=1}^{n} \mathbb{Z}/e_i\mathbb{Z}$. Indiquer sous quelles conditions X admet un sous-groupe (respectivement un quotient) isomorphe à Y.

Exercice 18. Soit A un groupe abélien fini. On pose $s = \sum_{x\in A} x$.

a) Montrer que $2s = 0$.

b) Soit $d_1|d_2|\dots|d_r$ les diviseurs élémentaires de A. Montrer que si d_{r-1} est impair et d_r pair, s est l'unique élément d'ordre 2 de A. Montrer que dans tous les autres cas $s = 0$.
Un élément x d'un groupe G est *caractéristique* si son orbite sous l'action de $\mathrm{Aut}(G)$ est réduite à un point.

c) Montrer que s est caractéristique.

d) Soit $n \geq 1$ un entier. Quels sont les éléments caractéristiques de $\mathbb{Z}/n\mathbb{Z}$?

e) Montrer que $(\mathbb{Z}/n\mathbb{Z})^2$ n'a pas d'autre élément caractéristique que 0.

f) Montrer que $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/2n\mathbb{Z})$ a exactement un élément caractéristique non nul.

g) Plus généralement, à quelles conditions sur $d_1, \dots, d_r$ le groupe A admet-il un autre élément caractéristique que 0 ? Montrer que cet élément t est alors unique.

Exercice 19.

a) Montrer que le groupe $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est naturellement isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$. En déduire qu'il est commutatif.

b) Expliciter $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Remarquer qu'il n'est pas commutatif.

c) Montrer que si d est un diviseur commun de m et n, l'application f

$$(x, y) \mapsto (x + \frac{n}{d}y, y)$$

est un automorphisme de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

d) Montrer que si A est un groupe abélien fini, $\mathrm{Aut}(A)$ est abélien si et seulement si A est cyclique.

3 Anneaux et idéaux

Si I, J sont deux idéaux de A, on note $(I : J) := \{a \in A, aJ \subset I\}$ (c'est un idéal de A).

Exercice 20. Soient A un anneau et I, J et L des idéaux de A. Montrer les assertions suivantes :

a) $I \cdot J \subset I \cap J$,
b) $(I \cdot J) + (I \cdot L) = I \cdot (J + L)$,
c) $(I \cap J) + (I \cap L) \subset I \cap (J + L)$,
d) si A est principal, alors $(I \cap J) + (I \cap L) = I \cap (J + L)$,
e) si J est contenu dans I, alors $J + (I \cap L) = I \cap (J + L)$,
f) supposons que $A = k[X, Y]$ avec k un corps et posons $I = (X)$, $J = (Y)$ et $L = (X + Y)$. Calculer $(I \cap J) + (I \cap L)$ et $I \cap (J + L)$, puis les comparer.

Exercice 21. Soient I et J deux idéaux d'un anneau A. On suppose que $I + J = A$ (deux tels idéaux sont dits comaximaux).

a) Montrer que $IJ = I \cap J$.
b) Montrer que $A \to A/I \times A/J$ est surjectif de noyau $I \cap J$.
c) Généraliser au cas de n idéaux comaximaux deux à deux.

Exercice 22. Soient I et J deux idéaux d'un anneau A. On suppose que $I + J = A$ (deux tels idéaux sont dits comaximaux), montrer que $I^n + J^n = A$.

Exercice 23. a) Soit I et J deux idéaux comaximaux de A (c'est-à-dire $I+J = A$). Montrer que $(I : J) = I$. Soit L un idéal tel que $I \cdot L \subset J$; montrer que $L \subset J$.

b) Soit $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers dont aucun n'est contenu dans l'autre. Montrer que $(\mathfrak{p} : \mathfrak{q}) = \mathfrak{p}$ et $(\mathfrak{q} : \mathfrak{p}) = \mathfrak{q}$. Donner un exemple de deux idéaux premiers dans $k[X, Y]$, où k est un corps, dont aucun n'est contenu dans l'autre et qui ne sont pas comaximaux.

c) Soit a un élément non diviseur de 0 d'un anneau A. Montrer que si (a) est premier, la relation $(a) = I \cdot J$ pour deux idéaux I et J, entraine $I = A$ où $J = A$.

Indice : Commencer par montrer que $I = (a)$ ou $J = (a)$.

Exercice 24. Montrer à l'aide d'un contre-exemple, que si I et J sont des idéaux tels que $I \cap J = I \cdot J$, I et J ne sont pas nécessairement comaximaux.

Exercice 25. Montrer qu'un anneau intègre A possédant un nombre fini d'idéaux est un corps.
Indice : prendre $x \in A$ et considérer les idéaux (x^n).

Exercice 26. Soit $A = A_1 \times \cdots \times A_n$ un produit d'anneaux et soit I un idéal de A.

a) Montrer que I est égal à un produit d'idéaux $I_1 \times \cdots \times I_n$.

b) Déterminer les idéaux premiers et maximaux de A.

c) Supposons que les A_i soient des corps, montrer que l'anneau A n'a qu'un nombre fini d'idéaux.

Exercice 27. Soit A l'anneau des fonctions continues à valeur réelles sur un espace topologique compact K.

a) Soit I un idéal strict de A. Montrer qu'il existe $x \in K$ tel que pour tout $f \in I$, on ait $f(x) = 0$.

b) Déterminer les idéaux maximaux de A.

Exercice 28. Montrer qu'il n'y a pas de morphisme d'anneaux :

a) de $\mathbb{C}$ dans $\mathbb{R}$,

b) de $\mathbb{R}$ dans $\mathbb{Q}$,

c) de $\mathbb{Q}$ dans $\mathbb{Z}$,

d) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$, pour tout $n > 0$.

Exercice 29. Montrer qu'il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n. Montrer que dans ce cas il existe un unique morphisme d'anneau.

Exercice 30. Soit A un anneau, montrer que l'ensemble R des éléments réguliers de A (c'est-à-dire non diviseurs de 0 dans A) est une partie multiplicative, c'est-à-dire : $1 \in R$ et si r et s sont des éléments de R alors $rs \in R$.

Exercice 31. Dans un anneau fini, tous les éléments réguliers sont inversibles.

Exercice 32. Soit A un anneau (commutatif unitaire) et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$.

a) Montrer que P est nilpotent si et seulement si pour tout $i \in \mathbb{N}$, a_i est nilpotent.

b) Soit x un élément nilpotent de A. Montrer que $1 + x$ est inversible.

c) Montrer que P est inversible dans $A[X]$ si et seulement si a_0 est inversible et pour tout $i \geq 1$, a_i est nilpotent.

Indice : si $Q = \sum_{i=0}^{m} b_i X^i$ est un inverse de P, on pourra commencer par montrer que que pour tout $r \geq 0$, $a_n^{r+1} b_{m-r} = 0$.

d) Montrer qu'un élément x de A appartient à tous les idéaux maximaux de A si et seulement si pour tout $a \in A$, $1 - ax$ est inversible.

e) Montrer que P est dans l'intersection de tous les idéaux maximaux si et seulement si P est nilpotent (c'est-à-dire, dans $A[X]$, le radical de Jacobson est égal au nilradical).

Exercice 33. Soit $f : A \to B$ un morphisme d'anneaux.
(i) Montrer que l'image réciproque d'un idéal premier est encore un idéal premier.
(ii) Est-ce encore vrai pour les idéaux maximaux ? Et si f est surjectif ?

Exercice 34. Soit A un anneau et I un idéal et soit $\pi : A \to A/I$. Montrer que :
(i) les idéaux de A/I sont en bijection avec les idéaux de A contenant I,
(ii) cette bijection induit une bijection sur les idéaux premiers et les idéaux maximaux.

Exercice 35. Déterminer tous les idéaux premiers de :
(i) $\mathbb{C}[X]$,
(ii) $\mathbb{R}[X]/(X^2+X+1)$,
(iii) $\mathbb{R}[X]/(X^3-6X^2+11X-6)$,
(iv) $\mathbb{R}[X]/(X^4-1)$.
(v) Déterminer tous les morphismes de $\mathbb{R}$-algèbre de ces anneaux dans $\mathbb{R}$ et $\mathbb{C}$.

Exercice 36. Soit $\mathfrak{p}$ un idéal premier d'un anneau A, et soient $(I_i)_{1\leq i\leq n}$ des idéaux de A. Supposons que

$$\mathfrak{p} \supset \prod_{i=1}^{n} I_i,$$

montrer que $\mathfrak{p}$ contient l'un des idéaux I_i.

Exercice 37. Soient $(\mathfrak{p}_i)_{1\leq i\leq n}$ des idéaux premiers d'un anneau A, et soit I un idéal de A tel que

$$I \subset \cup_{i=1}^{n} \mathfrak{p}_i.$$

Montrer que I est contenu dans l'un des $\mathfrak{p}_i$.

Exercice 38. Soit A un anneau et nil(A) l'ensemble des éléments nilpotents de A.
(i) Montrer que nil(A) est un idéal.
(ii) Montrer que si $\mathfrak{p}$ est un idéal premier, alors nil(A) $\subset \mathfrak{p}$.
(iii) Soit $s \notin$ nil(A) et $S = \{1, s, \cdots, s^n, \cdots\}$. Montrer que l'ensemble des idéaux de A disjoints de S contient un élément maximal $\mathfrak{p}$ (utiliser le lemme de Zorn). Montrer que $\mathfrak{p}$ est premier. En déduire que

$$\mathrm{nil(A)} = \bigcap_{\mathfrak{p}\ \text{idéal premier}} \mathfrak{p}.$$

Exercice 39. Montrer que dans un anneau principal A, les idéaux premiers sont maximaux.

Exercice 40. Montrer que l'anneau $\dfrac{\mathbb{C}[X,Y]}{(Y-X^2)}$ est principal.

Exercice 41. Soit $A = \dfrac{\mathbb{C}[X,Y]}{(XY-1)}$; on pose x l'image de X dans A.

a) Montrer que x est inversible et que tout élément a non nul de A peut s'écrire de façon unique sous la forme $a = x^m P(x)$ où $m \in \mathbb{Z}$ et P est un polynôme de terme constant non nul. On note $e(a) = \deg(P)$.
b) Soient $a, b \in A$ montrer qu'il existe $q, r \in A$ tels que $a = bq + r$ et : $r = 0$ ou $e(r) < e(b)$.
c) En déduire que A est principal.

Exercice 42. Soit k un corps et $A = k[X,Y]/(X^2, XY, Y^2)$.
(i) Déterminer les éléments inversibles de A.
(ii) Déterminer tous les idéaux principaux de A.
(iii) Déterminer tous les idéaux de A.

Exercice 43. Soit A un anneau intègre et $\mathfrak{p}$ un idéal premier principal non nul. Soit I un idéal principal de A contenant $\mathfrak{p}$. Montrer que $I = \mathfrak{p}$ ou $I = A$.

Exercice 44. Montrer qu'il n'existe pas d'homomorphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$.

Exercice 45. Soit $f : A \to B$ un homomorphisme d'anneaux. Pour tout idéal I de A on note $f_*(I)$ l'idéal de B engendré par $f(I)$ et on l'appelle extension de I dans B. Pour tout idéal J de B on appelle contraction de J l'idéal $f^{-1}(J)$. Soit I un idéal de A et J un idéal de B. Montrer que :

a) $I \subset f^{-1}\big(f_*(I)\big)$ et $J \supset f_*\big(f^{-1}(J)\big)$,
b) $f^{-1}(J) = f^{-1}\big[f_*\big(f^{-1}(J)\big)\big]$ et $f_*(I) = f_*\big[f^{-1}\big(f_*(I)\big)\big]$.
c) Soit $\mathcal{C}$ l'ensemble des idéaux de A qui sont des contractions d'idéaux de B et $\mathcal{E}$ l'ensemble des idéaux de B qui sont des extensions d'idéaux de A. Montrer que :
d) $\mathcal{C} = \big\{I : I = f^{-1}\big(f_*(I)\big)\big\}$ et $\mathcal{E} = \big\{J : J = f_*\big(f^{-1}(J)\big)\big\}$,
e) f_* définit une bijection de $\mathcal{C}$ sur $\mathcal{E}$; quel est son inverse ?
Soient I_1 et I_2 deux idéaux de A et J_1 et J_2 deux idéaux de B. Montrer que :

f) $f_*(I_1+I_2)=f_*(I_1)+f_*(I_2)$ et $f^{-1}(J_1+J_2)\supset f^{-1}(J_1)+f^{-1}(J_2)$,
g) $f_*(I_1\cap I_2)\subset f_*(I_1)\cap f_*(I_2)$ et $f^{-1}(J_1\cap J_2)=f^{-1}(J_1)\cap f^{-1}(J_2)$,
h) $f_*(I_1\cdot I_2)=f_*(I_1)\cdot f_*(I_2)$ et $f^{-1}(J_1\cdot J_2)\supset f^{-1}(J_1)\cdot f^{-1}(J_2)$,
i) $f_*(I_1:I_2)\subset (f_*(I_1):f_*(I_2))$ et $f^{-1}(J_1:J_2)\subset (f^{-1}(J_1):f^{-1}(J_2))$,
j) $f_*(\sqrt{I})\subset\sqrt{f_*(I)}$ et $f^{-1}(\sqrt{J})=\sqrt{f^{-1}(J)}$.

Exercice 46. Considérons l'homomorphisme d'anneau $\varphi : k[U,V]\longrightarrow k[X]$ défini par $\varphi(U)=X^3$ et $\varphi(V)=-X^2$ et tel que $\varphi(a)=a$ pour tout $a\in k$?

a) Quel est le noyau de φ ?
b) Quelle est l'image de φ ?
c) Montrer que A est intègre et que son corps des fractions est isomorphe à $k(X)$.

Exercice 47. Montrer que l'algèbre quotient $\mathbb{R}[X]/(X^2+X+1)$ est isomorphe à $\mathbb{C}$ et que l'algèbre $\mathbb{R}[X]/(X(X+1))$ est isomorphe à $\mathbb{R}^2$.

Exercice 48. Soit k un corps de caractéristique $p>0$ et A une k-algèbre. Montrer que le morphisme

$$F : A\to A$$

$$x\mapsto x^p$$

appelé morphisme de Frobenius est un morphisme d'anneaux.

Exercice 49. Soit k un corps et A une k-algèbre de dimension finie comme k-espace vectoriel.

a) Montrer qu'une algèbre *intègre* de dimension finie sur un corps est un corps [Montrer que l'application de multiplication par a non nul est injective puis surjective].
b) Soit $\mathfrak{p}\in\operatorname{Spec}(A)=\{\mathfrak{p}\ /\ \mathfrak{p}$ est un idéal premier$\}$.
Montrer que $A/\mathfrak{p}$ est de dimension finie sur k.
c) Montrer que $\mathfrak{p}$ est un idéal maximal.
Soient $\mathfrak{p}_i\in\operatorname{Spec}(A), i=1,\cdots,n$ des idéaux distincts.
d) Montrer que la flèche

$$A\to\bigoplus_{i=1}^{n} A/\mathfrak{p}_i$$

est surjective. En déduire l'inégalité $n\le\dim_k(A)$.
On suppose dorénavant A réduite (c'est-à-dire nil(A) = 0).
e) Montrer que la flèche

$$A\to\bigoplus_{\mathfrak{p}\in\operatorname{Spec}(A)} A/\mathfrak{p}$$

est un isomorphisme d'anneaux.
f) Considérons l'algèbre $A=\mathbb{R}[X]/((X^2+a)X(X+1))$ avec $a\in\mathbb{R}$.
À quelle condition sur $a\in\mathbb{R}$, l'algèbre A est elle réduite ?
g) Dans le cas où A est réduite, expliciter l'isomorphisme précédent.

Exercice 50. Un anneau est dit local s'il contient un unique idéal maximal.

a) Montrer qu'un anneau A est local si et seulement si $A\backslash A^*$ est un idéal.
b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est il local ?
c) Soient A un anneau local, I,J deux idéaux de A et $a\in A$ un élément non diviseur de 0 tels que $IJ=(a)$. Montrer qu'il existe $x\in I$ et $y\in J$ tels que $a=xy$. En déduire que $I=(x)$ et $J=(y)$.

4 Modules

Exercice 51. Soit M un A-module, montrer que la somme directe $M^{\mathbb{N}}$ est isomorphe au module des polynômes $M[X]$.

Exercice 52. Soit A et B deux anneaux et $f : A \longrightarrow B$ un homomorphisme d'anneaux.
(I) Montrer que la loi $a.b = f(a).b$ (où $a \in A$ et $b \in B$) munit B d'une structure de A-module. B muni de sa structure d'anneau et de cette structure de A-module est appelé une A-algèbre.
(II) Montrer que si A est un corps k alors f est injectif (c'est-à-dire : une k-algèbre contient un corps isomorphe à k).
(III) Montrer que tout B-module N est muni naturellement d'une structure de A-module. Quel est l'annulateur $\mathrm{Ann}(N) = (0_A : N)$ de ce module ?

Exercice 53. Soit M un A-module, on définit $M^\vee = \hom_A(M, A)$. On dit que M est réflexif si le morphisme naturel $\theta : M \to M^{\vee\vee}$ défini par $m \mapsto \theta(m) = (\varphi \mapsto \varphi(m))$ avec $\varphi \in M^\vee = \hom_A(M, A)$ est un isomorphisme. Soit $f \in \mathrm{End}_A M$, on définit sa transposée ${}^t f \in \mathrm{End}_A M^\vee$ par ${}^t f(\varphi) = \varphi \circ f$ pour tout $\varphi \in M^\vee = \hom_A(M, A)$.

a) Montrer que l'ensemble des polynômes P de $A[X]$ tels que $P(f) = 0$ est un idéal que l'on notera $I(f)$.
b) Montrer que $I(f) \subset I({}^t f)$.
c) Montrer que ${}^t({}^t f) \circ \theta = \theta \circ f$.
d) Montrer que si M est réflexif, on a $I(f) = I({}^t f)$.

Exercice 54. Soit M un A-module
(I) On suppose que M est monogène, montrer qu'il existe un idéal I de A tel que $M \simeq A/I$.
(II) On suppose que $M \neq (0)$ est simple (c'est-à-dire que ses seuls sous-modules sont (0) et M). Montrer que M est monogène, engendré par tout élément non nul de M. Montrer que M est isomorphe à $A/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal de A.
(III) Quels sont les $\mathbb{Z}$-modules simples ?

Exercice 55. Soit A un anneau intègre et M un A-module. On dit que $x \in M$ est de torsion si il existe $a \in A - \{0\}$ tel que $ax = 0$. On note $T(M)$ l'ensemble des éléments de torsion de M. Si $T(M) = 0$ on dit que M est sans torsion.

a) Montrer que l'ensemble des éléments de torsion de M est un sous-module de M.
b) Montrer que $M/T(M)$ est sans torsion.
c) Montrer que si $f : M \to N$ est un morphisme de A-modules alors $f(T(M)) \subset T(N)$.

Exercice 56. Soit M un A-moduleet $m \in M$ un élément dont l'annulateur $\mathrm{Ann}(m)$ est réduit à (0). Montrer que Am est facteur direct de M si et seulement si il existe $f \in M^\vee = \hom_A(M, A)$ tel que $f(m) = 1$. Montrer qu'alors on a $M = Am \oplus \ker f$.

Exercice 57. Soient $M_1, \ldots, M_r$ des A-modules et $I_1 = \mathrm{Ann}(M_1), \cdots, I_r = \mathrm{Ann}(M_r)$ leurs annulateurs. On suppose que les I_α sont deux à deux comaximaux (c'est-à-dire que l'on a $I_\alpha + I_\beta = A$ pour $\alpha \neq \beta$).
On pose : $M = \bigoplus_{\alpha=1}^r M_\alpha$, $I = \bigcap_{\alpha=1}^r I_\alpha$, $N_\alpha = \bigoplus_{\beta\neq\alpha} M_\beta$ et $J_\alpha = \bigcap_{\beta\neq\alpha} I_\beta$. Si J est un idéal de A on notera $(0 : J)$ le sous-A-module de M égal à $\{m \in M, J.m = 0\}$. Montrer les formules suivantes :
(I) Montrer que pour tout α, I_α et J_α sont comaximaux.
(II) $J_\alpha = (0 : N_\alpha)$,
(III) $N_\alpha = (0 : J_\alpha) = I_\alpha \cdot M$.
(IV) $M_\alpha = (0 : I_\alpha) = J_\alpha \cdot M = \bigcap_{\beta\neq\alpha} N_\beta$.