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 $\mathbb{Z}/2\mathbb{Z}$.

Solution. a) $G^+(X_n)$ est le noyau du déterminant $\det : G(X_n) \to \{\pm 1\}$, donc c'est un sous-groupe distingué en tant que noyau. Or les symétries axiales ont -1 pour image, donc ce morphisme est surjectif, et le noyau est d'indice 2.

b) $G^+(X_n)$ est le groupe des rotations de centre le sommet du polygone et d'angle $2k\pi/n$, $k \in \mathbb{Z}$. Il est engrendré par la rotation d'angle $2\pi/n$.

c) Le morphisme det admet une section en envoyant 1 sur l'identité et -1 sur une une symétrie axiale s. Si $r \in G^+(X_n)$, alors $srs^{-1} = r^{-1}$. Donc $G(X_n)$ est le produit semidirect de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ défini par le morphisme $\mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/n\mathbb{Z})$ qui envoie 1 sur $k \mapsto -k$.

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 $Z(G) \neq \{1\}$.

Solution. Considérons l'action de G sur lui-même par conjugaison. Le cardinal de G est la somme des cardinaux des orbites. Or le cardinal de chaque orbite divise p^n, donc vaut 1 ou est multiple de p. Le cardinal del'ensemble des éléments fixés par l'action est donc divisible par p. Or un élément est fixé par l'action si et seulement si il est dans le centre de G. Donc le cardinal de $Z(G)$ est divisible par p, donc ne peut être 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 $GL_n(k)$.

Solution. a) Si H est un sous-groupe de G, notons $H_i = H \cap G_i$. Le noyau du morphisme $H \to G/G_i$ est H_i donc H_i est distingué dans H, et H/H_i s'identifie à un sous-groupe de G/G_i. Alors $H_{i+1}/H_i \subset G_{i+1}/G_i$ et commute donc avec tout G/G_i, donc en particulier avec H/H_i.
Si $\pi : G \to H$ est un morphisme surjectif. Notons $H_i := \pi(G_i)$. Alors π induit un morphisme surjectif $\pi_i : G/G_i \to H/H_i$ et H_{i+1}/H_i est l'image de G_{i+1}/G_i par π_i. Donc si $x \in H_{i+1}/H_i$ et $y \in H/H_i$, il existe $x_0 \in G_{i+1}/G_i$ et $y_0 \in G/G_i$ tels que $\pi_i(x_0) = x$ et $\pi_i(y_0) = y$. Or x_0 et y_0 commutent, donc en appliquant π_i, x et y commutent, ce qui prouve que H_{i+1}/H_i est dans le centre de H/H_i.

b) D'après l'exercice précédent $G_1 := Z(G)$ est non trivial. Par récurrence sur le cardinal $H := G/Z(G)$ est nilpotent, d'où une suite $1 = H_0 \subset H_1 \subset \cdots \subset H_n$ comme dans l'énoncé. Notons pour ß ≥ 1 G_i la préimage de H_{i-1} par la projection $G \to H$ (la définition est cohérente pour G_1). Alors pour $i \geq 1$ $G_{i+1}/G_i = H_i/H_{i-1}$ est bien central dans $G/G_i = H/H_{i-1}$ et pour $i = 0$, c'est clair par définition de G_1.

c) Notons F_k le sous-espace vectoriel engendré par $e_1, \cdots, e_k$. Alors $U_n(K)$ est l'ensemble des applications linéaires f telles que $(f - Id)(F_k) \subset F_{k-1}$ pour tout k. Notons G_{n-i} l'ensemble des applications linéaires f telles que $(f - Id)(F_k) \subset F_{k-i-1}$. Vérifions que G_{n-i} est un sous-groupe, soient $f, g \in G_i$ alors $fg - Id = f(g - Id) + (f - Id)$, $f(g - Id)(F_k) \subset f(F_{k-i-1}) \subset F_{k-i-1}$ et $(f - Id)(F_k) \subset F_{k-i-1}$. Comme F_{k-i-1} est stable par addition, fg est bien dans G_i. De même $f^{-1} - Id = f^{-1}(Id - f)$ et donc $(f^{-1} - Id)(F_k) \subset f^{-1}(F_{k-i-1}) \subset F_{k-i-1}$.
De plus si $g \in G_{n-i}$ et $h \in U_n(K)$; Alors $ghg^{-1} - Id = g(h - Id)g^{-1}$ et $g(h - Id)g^{-1}(F_k) \subset g(h - Id)(F_k) \subset g(F_{k-i-1}) \subset F_{k-i-1}$ et donc $ghg^{-1} \in G_i$, ce qui prouve que G_i est distingué.

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 $\prod_{p|n} G_p \to G$.

Solution. a) Comme gG_qg^{-1} est un q-Sylow, par unicité du q-Sylow, on a $gG_qg^{-1} = G_q$, et de même $hG_ph^{-1} = G_p$. Donc $ghg^{-1} \in G_q$ et $(ghg^{-1})h^{-1} \in G_q$ en tant que produit d'éléments de G_q. De même $hg^{-1}h^{-1} \in G_p$ et $g(hg^{-1}h^{-1}) \in G_p$ en tant que produit d'éléments de G_p.
Or $\sharp G_p \cap G_q | pgcd(\sharp G_p, \sharp G_q) = 1$ donc $G_\cap G_q = \{1\}$.

b) Considérons l'application $\phi : G_{p_1} \times \cdots \times G_{p_k} \to G$ qui à $(g_1, \cdots, g_k)$ associe $g_1 \cdots g_k$. Comme les G_p commutent deux à deux, ϕ ne dépend pas de l'ordre des p_i et est bien un morphisme de groupe. Ce morphisme est injectif, en effet si $(g_1, \cdots, g_k)$ est dans le noyau de ϕ, $1 = (g_1 \cdots g_k)^{(p_1 \cdots p_{k-1})^r} = g_k^{(p_1 \cdots p_{k-1})^r}$ pour r assez grand (on utilise le fait que les g_i commutent deux à deux), or $(p_1 \cdots p_{k-1})^r$ est premier à l'ordre de g_k, donc $g_k = 1$ et de même pour les autres g_i. Or les deux groupes ont même cardinal, c'est donc un isomorphisme.

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 $\mathfrak{A}_5$.

Solution. a) D'après le théorème de Sylow, n_5 divise 12 et est congru à 1 modulo 5. les seules possibilités sont 1 ou 6. Mais si $n_5 = 1$, le 5-Sylow est distingué, ce qui contredit la simplicité de G.Il y a 4 éléments d'ordre 5 dans chaque 5-Sylow qui s'intersectent trivialement 2 à 2, d'où 24 éléments d'ordre 5.

b) Le théorème de Sylow nous donne $n_3 = 1, 4$ ou 10. $n_3 = 1$ est impossible car le 3-Sylow serait distingué. Si $n_3 = 4$, l'action de G par conjugaison sur l'ensemble des 3-Sylow fournit un morphisme non trivial $G \to \S_4$, or comme $\sharp G > \sharp \S_4$ le noyau doit être non trivial, d'où un sous-groupe distingué non trivial de G, ce qui contredit la simplicité de G. Il y a 2 éléments d'ordre 3 par 3-Sylow, d'où 20 éléments d'ordre 3.

c) Si G contient un élément x d'ordre 6, x normalise le 3-Sylow $\langle x^2 \rangle$. Or le cardinal du normalisateur de $\langle x^2 \rangle$ est $60/10 = 6$, donc $\langle x \rangle$ est le normalisateur de $\langle x^2 \rangle$. En particulier le centralisateur de x est réduit à $\langle x \rangle$, donc x à 10 conjugués. De plus x et x^{-1} ne sont pas conjugués (car le normalisateur et le centralisateur de x coincident). On obtient donc au moins 20 éléments d'ordre 6, ce qui fait 64 éléments avec ceux d'ordre 3 et 5.
De même, si G contient un élément x d'ordre 10, il a 6 conjugués et n'est pas conjugué avec x^3, x^7 et x^9, d'où au mons 24 éléments d'ordre 10 ce qui est trop.

d) Les 2-Sylow sont d'ordre 4 donc sont commutatifs. soit $x \neq 1 \in H_1 \cap H_2$, alors sont commutateur $C(x)$ contient H_1 et H_2, donc n'est contenu dans aucun 2-Sylow, donc un élément y d'ordre 3 ou 5 commute avec x. Alors xy est un élément d'ordre 6 ou 10, ce qui est impossible.

e) D'après la question 3, tout élément est d'ordre $1, 2, 3, 4$ ou 5. Il y a donc 15 éléments d'ordre 2 ou 4, chacun étant contenu dans un unique 2-Sylow et chaque 2-Sylow contient 3 tels éléments. Il y a donc $15/3 = 5$ 2-Sylow.

f) L'action de G sur les 2-Sylow fournit un morphisme non trivial $G \to \S_5$. Comme G est simple, ce morphisme est injectif. G s'identifie donc à un sous-groupe d'indice 2 de S_5, qui ne peut être que A_5.

2 Groupes abéliens

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

$$\underset{Ab}{\mathrm{Hom}}(X, Y) = \{\text{Morphismes de groupes abéliens } X \to Y\}$$

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 $\mathrm{Hom}_{Ab}(X, Y)$.

Solution. On vérifie d'abord que $f+g$ est bien dans $\mathrm{Hom}_{Ab}(X,Y)$. c'est-à-dire $(f+g)(x+y) = (f+g)(x) + (f+g)(y)$.Ensuite $((f+g)+h)(x) = f(x)+g(x)+h(x) = (f+(g+h))(x)$ donc la loi est associative ; $f(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$ donc la loi est commutative ; $x \mapsto 0$ est élément neutre et en posant $(-f)(x) = -(f(x))$ ($-f$ est bien un élément de $\mathrm{Hom}_{Ab}(X,Y)$), on a $(f+(-f))(x) = 0$, donc $-f$ est un inverse de f.

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

Solution. Soit $x \neq 0 \in A$. Alors $\langle x \rangle$ est un sous-groupe, nécessairement distingué, de A. Donc par simplicité $\langle x \rangle = A$, donc A est cyclique et engendré par tout élément non nul, ce qui n'est possible que si A est fini (dans $\mathbb{Z}$, 2 n'engendre pas $\mathbb{Z}$), et si $p|\sharp A =: n$, $\bar{p}$ n'engendre pas $\mathbb{Z}/n\mathbb{Z}$, donc on doit avoir $\bar{p} = 0$, donc $n = p$ (ou 1 mais le groupe trivial n'est pas simple).

Exercice 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.

Solution. Notons π la projection $A \to B$. Si $x \in nA$, il existe $a \in A$ tel que $x = na$ donc $\pi(x) = n\pi(a) = 0$. Donc $nA \in \mathrm{Ker}(\pi)$ et d'où une surjection $A/nA \to A/\mathrm{Ker}(\pi) \simeq B$.

Exercice 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 $B \oplus A/B$.

Solution. Soit m l'ordre de A/B et π la projection $A \to A/B$. On a $\pi(mx) = m\pi(x) = 0$, donc le morphisme $A \to A$ défini par $x \mapsto mx$ est à image dans B. On obtient donc un morphisme $\phi : A \to B \oplus A/B$ en envoyant x sur $(mx, \pi(x))$. Si $x \in \mathrm{Ker}\,\phi$, alors $\pi(x) = 0$ donc $x \in B$ et $mx = 0$, or m est premier à l'ordre de B, donc par le théorème de Lagrange, $x = 0$. Le morphisme ϕ est donc injectif, c'est donc un isomorphisme puisque les deux groupes ont même cardinal.

Exercice 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.

Solution. a) On a clairement $0 \in A$. Si $m, n \in I$ et $x \in A$, $(m+n)(x) = mx + nx = 0$ donc $m + n \in I$. De même $-mx = 0$ donc $-m \in I$. Donc I est un sous-groupe de $\mathbb{Z}$

b) Par le théorème de Lagrange, $(\sharp A)A = 0$, donc $\sharp A \in I$, donc l'exposant de A divise $\sharp A$.

c) Soit n le produit des exposants des composantes p-primaires. Alors pour tout p, $nA(p) = 0$. Or les composantes p-primaires engendrent A, donc $nA = 0$ et $n \in I$; donc l'exposant de A divise n. Réciproquement, soit e l'exposant de A. $eA = 0$, donc $eA(p) = 0$ donc l'exposant e_p de $A(p)$ divise e et donc $ppcm_p(e_p)|e$. Or d'après la question 1, e_p est une puissance de p, donc les e_p sont premiers deux à deux, donc $n = ppcm_p(e_p)|e$.

d) Supposons qu'il n'existe pas d'élément d'ordre $e_p = p^{n_p}$ (l'exposant de $A(p)$) dans $A(p)$). Alors l'ordre de tout élément de $A(p)$ diviserait $p^{n_p - 1}$ et donc $p^{n_p-1} \in I$, ce qui contredit la définition de e_p. Soit donc $x_p \in A(p)$ d'ordre e_p. Soit $x = \sum_p x_p$. Alors l'ordre de x_p est bien $\prod_p e_p$.

Exercice 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 $\widehat{\widehat{A}}$.

Solution. a) On utilise l'exercice 6, pour $X = G$ et $Y = \mathbb{C}^*$.

b) Soit $\chi \in \widehat{A}$ et $a \in A$, alors $\chi^d(a) = \chi(da) = 1$ donc $\chi^d = 1$ pour tout χ donc l'exposant de $\widehat{A}$ divise d.

c) Supposons $A = \mathbb{Z}/n\mathbb{Z}$. Si $k \in \mathbb{Z}$, on peut définir χ_k par $\chi_k(\bar{a}) = e^{2i\pi ka/n}$, d'où un morphisme $\mathbb{Z} \to \widehat{A}$, défini par $k \mapsto \chi_k$, dont le noyau est $n\mathbb{Z}$. On en déduit un morphisme injectif $\phi : \mathbb{Z}/n\mathbb{Z} \to \widehat{A}$. Réciproquement, si $\chi \in \widehat{A}$, alors $\chi(1)^n = \chi(\bar{n}) = \chi(0) = 1$ donc $\chi(1)$ doit être de la forme $e^{2i\pi k/n}$ pour un certain $k \in /Z$. Mais alors $\chi(\bar{a}) = \chi(1)^a = e^{2i\pi ka/n}$, donc $\chi = \chi_k$, ce qui montre que ϕ est bijectif.

d) considérons $\phi : \widehat{A} \to \widehat{B} \oplus \widehat{C}$ qui à χ associe (χ_B, χ_C) (où χ_B et χ_C) sont les restrictions de χ à B et C). Soit $\chi \in \mathrm{Ker}\,\phi$ et $a \in A$. Alors $a = b + c$ avec $b \in B$ et $c \in C$, donc $\chi(a) = \chi(b)\chi(c) = 1$ car $\chi_B = 1, \chi_C = 1$. Donc ϕ est injective. Réciproquement, soit $\chi_1 \in \widehat{B}$ et $\chi_2 \in \widehat{C}$, et soit $\pi_B : A \to B$ et $\pi_C : A \to C$ les projections canoniques. Définissons $\chi : A \to \mathbb{C}^*$ par $\chi(a) = \chi_1(\pi_B(a))\chi_2(\pi_C(a))$; $\chi_1 \circ \pi_B$ et $\chi_2 \circ \pi_B$ sont des morphismes de groupes en tant que composés de morphisme de groupe et donc $\chi \in \widehat{A}$ en tant que somme (au sens de l'exo 6) d'éléments de A. De plus si $b \in B$, $\pi_B(b) = b$ et $\pi_C(b) = 0$ donc $\chi(b) = \chi_1(b)$; l'analogue pour C montre que $\phi(\chi) = (\chi_1, \chi_2)$, donc ϕ est un isomorphisme.

e) soient $\chi_1, \chi_2 \in \widehat{B}$ et $a \in A$,

$$\widehat{\alpha}(\chi_1+\chi_2)(a) = ((\chi_1+\chi_2)\circ\alpha)(a) = (\chi_1+\chi_2)(\alpha(a)) = \chi_1(\alpha(a)) + \chi_2(\alpha(a))$$
$$= \chi_1\circ\alpha(a) + \chi_2\circ\alpha(a) = \widehat{\alpha}(\chi_1)(a) + \widehat{\alpha}(\chi_2)(a) = (\widehat{\alpha}(\chi_1)+\widehat{\alpha}(\chi_2))(a),$$

donc $\widehat{\alpha}$ est un morphisme de groupes.

f) Soit $\chi \in \operatorname{Ker}\widehat{\alpha}$ et $b \in B$. Comme α est surjectif, il existe $a \in A$ tel que $\alpha(a) = b$. Alors $\chi(b) = \chi\alpha(a) = \widehat{\alpha}(\chi)(a) = 0$ car $\widehat{\alpha}(\chi) = 0$. Donc $\chi = 0$, ce qui montre que $\widehat{\alpha}$ est injective.

g) Pour simplifier les notations, on identifie B avec $\alpha(B)$, de sorte que $\widehat{\alpha}$ est juste la restriction à B. Soit $\chi \in \widehat{B}$. Soit E l'ensemble des sous-groupes N de A contenant B tels qu'il existe $\chi_0 \in \widehat{N}$ dont la restriction à B est χ, et considérons un élément maximal pour l'inclusion N_0 de E (E est non vide car $B \in E$) et soit $\chi_0 \in \widehat{N_0}$ prolongeant χ. Supposons par l'absurde $E \neq A$. Soit $a \notin N_0$ et notons $N_1 = N + \langle x\rangle$. Soit $\psi : \mathbb{Z} \to N_1$ qui envoie n sur nx et soit d le générateur positif de $\psi^{-1}(N)$. Soit λ une racine $d$ième de $\chi_0(dx)$ et définissons $chi_1(a+nx) = \lambda^n\chi_0(a)$. Pour que χ_1 définisse un élément de $\widehat{N_1}$, il suffit de vérifier que, si $a+nx = 0$, $\lambda^n\chi_0(a) = 1$. Or, si $a+nx = 0$, $n \in \psi^{-1}(N)$, donc il existe $m \in \mathbb{Z}$ tel que $n = dm$; alors $\lambda^n\chi_0(a) = \lambda^{dm}\chi_0(a) = \chi_0(dx)^m\chi_0(a) = \chi_0(mdx+a) = 1$. Donc χ_0 se prolonge à N_1 et donc χ aussi, ce qui contredit la maximalité de N_0. Donc $N_0 = A$ et $\widehat{\alpha}$ est bien surjectif.

h) Comme dans la question c, considérons $\chi_0 \in \widehat{B}$ défini par $\chi_0(ka) = exp(2i\pi k/d)$. D'après la question précédente χ_0 se prolonge en $\chi \in \widehat{A}$, et $\chi(a) = exp(2i\pi/d)$ vérifie la propriété voulue.
$B \cap Ker(\chi) = \operatorname{Ker}(\chi_B) = \{0\}$ et si $x \in A$ l'ordre de $\chi(x)$ divise d, donc $chi(x)$ est de la forme $exp(2i\pi k/d)$ pour un certain $k \in \mathbb{Z}$. Donc $\chi(x) = \chi(ka)$ et $x = ka + (x-ka)$ avec $ka \in B$ et $x - ka \in \operatorname{Ker}(\chi)$.

i) On procède par récurrence forte sur le cardinal du groupe abélien fini A. Si $A = 0$, c'est évident. Sinon, l'exposant d de A est strictement plus grand que 1, et d'après la question précédente $A \simeq \mathbb{Z}/d\mathbb{Z} \oplus Ker\chi$ avec $\operatorname{Ker}\chi$ de cardinal strictement inférieur à celui de A. Par hypothèse de récurrence $\operatorname{Ker}\chi$ se décompose comme produit de groupes cycliques. Donc A aussi.

j) On vérifie facilement que $a^\vee \in \widehat{\widehat{A}}$ et que $\phi : a \mapsto a^\vee$ est un morphisme de groupe. Soit $a \neq 0 \in A$. Alors il existe $\chi_0 \in \widehat{\langle a\rangle}$ tel que $\chi_0(a) \neq 0$ d'après la question c et chi_0 se prolonge en $\chi \in \widehat{A}$. Donc $a^\vee(\chi) = \chi(a) \neq 0$, donc a n'est pas dans le noyau de ϕ. Donc ϕ est injective.
Si A est cyclique $\sharp\widehat{A} = \sharp A$. En utilisant d, on obtient que la formule reste vrai quand A est un produit de groupes cycliques. Or d'après i, tout groupe abélien fini est cyclique. Donc $\sharp\widehat{A} = \sharp A$ pour tout groupe abélien. Donc $\sharp\widehat{\widehat{A}} = \sharp\widehat{A} = \sharp A$, donc phi est un isomorphisme.

Exercice 12. 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

$$E := \operatorname{Ker}((\mathbb{Z}/p^{n+m}\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*)$$

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 $n \geq 1$.

Solution. a) $(x+p^n y)^p = \sum_{i=0}^p \binom{p}{i} x^{p-i}p^{ni}y^i$. Les deux premiers termes correspondent au termes de l'expression voulue. Pour $i \geq 3$, $ni \geq n+2$ (car $n \geq 1$) donc tous les termes en $i \geq 3$ sont divisibles par p^{n+2}.
Pour le terme $i = 2$ $2n \geq n+1$ quoi qu'il arrive et $2n \geq n+2$ si $n \geq 2$. Dans le cas où $n = 1$, alors $p \geq 3$ par hypothèse donc $p|\binom{p}{2}$ et donc $p^{n+2}|\binom{p}{i}x^{p-i}p^{ni}$ comme voulu.

b) On a $(x+2y)^2 = x^2+4xy+4y^2$ qui n'est pas congru modulo 8 à x^2+4xy si y est impair.

c) Le morphisme $(\mathbb{Z}/p^{n+m}\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$ est surjectif et $\sharp E = \phi(p^{n+m})/\phi(p^n) = p^m$ comme voulu. Comme $x = 1 \mod p^n$, $x \in E$. Soit y tel que $x = 1 + yp^n$ avec $y \neq 0 \mod p$. En appliquant la formule de la question a, on obtient $x^p = 1 + yp^{n+1} \mod p^{n+2}$ puis $x^{p^2} = 1 + yp^{n+2} \mod p^{n+3}$, et par récurrence $x^{p^{m-1}} = 1 + yp^{n+m-1} \neq 1 \mod p^{n+m}$ ce qui montre que l'ordre de x ne divise pas p^{m-1}. Donc l'ordre de x est p^m et donc x engendre E.

d) Appliquons la question précédente à $m = n-1$ et $n = 1$. Alors $E := \mathrm{Ker}((\mathbb{Z}/p^N\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*)$ est cyclique d'ordre $\mathbb{Z}/p^{n-1}\mathbb{Z}$. Comme $pgcd(\sharp E, \sharp(\mathbb{Z}/p\mathbb{Z})^*) = 1$, on peut appliquer l'exercice 9. Donc $(\mathbb{Z}/p^N\mathbb{Z})^* \simeq E \oplus (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/p^{n-1}\mathbb{Z} \oplus (\mathbb{Z}/(p-1)\mathbb{Z})$ qui est cyclique.

Exercice 13. 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.

Solution. On a $Y_1 = \mathbb{Z}/8\mathbb{Z}$, $Y_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $Y_3 = (\mathbb{Z}/2\mathbb{Z})^3$.
On a $X_1 = \mathbb{Z}/16\mathbb{Z}$, $X_2 = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $X_3 = (\mathbb{Z}/4\mathbb{Z})^2$, $X_4 = \mathbb{Z}/4\mathbb{Z} \times (/Z/2\mathbb{Z})^2$ et $X_5 = (\mathbb{Z}/2\mathbb{Z})^3$.
Y_1 est isomorphe à un sous-groupe de X_1 et X_2. Y_2 est un sous-groupe de X_2, X_3 et X_4. Y_3 est un sous-groupe de X_4 et X_5.

Exercice 14. 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 ?

Solution. $216 = 2^3 3^3$, donc $a = b = 3$. X est isomorphe à $X[2] \times X[3]$;$X[2]$ est isomorphe à $Y_1 = \mathbb{Z}/8\mathbb{Z}$, $Y_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $Y_3 = (\mathbb{Z}/2\mathbb{Z})^3$; $X[3]$ est isomorphe à $Z_1 = \mathbb{Z}/27\mathbb{Z}$, $Z_2 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou $Z_3 = (\mathbb{Z}/3\mathbb{Z})^3$.
On obtient donc 9 classes d'isomorphisme de groupes abéliens de cardinal 216
$432 = 2^4 3^3$ et donc $a = 4$. D'après l'exercice précédent, il y a maintenant 5 classe d'isomorphisme pour $X[2]$, d'où 15 classe d'isomorphisme pour X.

Exercice 15. 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.

Solution. Décomposons X sous la forme $X = A_1 \times \cdots \times A_r$ avec A_i cyclique d'ordre n_i, de générateur noté e_i. Soit d_i divisant n_i tel que $\prod_i d_i = d$ Alors le sous-groupe de X engendré par les $\frac{n_i}{d_i} e_i$ est de cardinal d. De même X a un sous-groupe H de cardinal n/d, et le quotient X/H est donc de cardinal d.
La bijection $H \mapsto X/H$ entre sous-groupes et quotients montre qu'il suffit d'étudier le cas des sous-groupes. Si $X \simeq \mathbb{Z}/n\mathbb{Z}$, X a bien un unique sous-groupe d'ordre d (le noyau de la multiplication par d). Réciproquement, si X n'est pas cyclique, dans la décomposition $X = A_1 \times \cdots \times A_r$, il existe $i \neq j$ tels que n_i, n_j ne soit pas premiers entre eux d'après le lemme chinois. Soit m leur pgcd et B_i, B_j les sous-groupes de cardinal m dans A_i et A_j respectivement. Comme $A_i, A_J \subset A$, on peut aussi voir B_I et B_j comme des sous-groupes de A. Alors B_i et B_j sont deux sous-groupes distincts de A de même cardinal.

Exercice 16. 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 $X/Y \simeq \mathbb{Z}/12\mathbb{Z}$.

Solution. $X = \mathbb{Z}/8\mathbb{Z}$ ou $X = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ($(\mathbb{Z}/2\mathbb{Z})^3$ quand à lui n'a pas de sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$).
Regardons $X[2]$ et $X[3]$. On a $X[3] = \mathbb{Z}/9\mathbb{Z}$ ou $(\mathbb{Z}/3\mathbb{Z})^2$ et $X[2] = \mathbb{Z}/8\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. D'où 4 possibilités pour X.

Exercice 17. Soit $(d_i)_{1 \leq i \leq m}$ et $(e_i)_{1 \leq i \leq n}$ deux familles d'entiers naturels tels que $1 < d_1 | d_2 | \ldots | d_m$ et $1 < e_1 | e_2 | \ldots | e_n$. 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.

Solution. Si $e_i | d_i$ pour tout i, alors le morphisme $Y \to X : (\bar{a}_i)_i \mapsto (\frac{d_i}{e_i}$ identifie Y a un sous-groupe de X.
Réciproquement, soit phi un morphisme injectif $Y \to X$. Soit $f_i \in Y$ le générateur de la composante $\mathbb{Z}/e_i\mathbb{Z}$. Et notons $H_k = \prod_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z} \subset X$. Alors $\phi(f_n)$ est d'ordre e_n donc e_n divise d_n. procédons par récurrence sur k pour montrer que e_{n-k} divise d_{n-k}.
Si e_{n-k+1} divise déjà d_{n-k}, on a bien ce qu'on veut. Sinon,

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.

Solution. a) Soit $x \in I \cdot J$, alors $x = \sum a_i b_i$ avec $a_i \in I$ et $b_i \in J$. Comme I et J sont des idéaux, on a $a_i b_i \in I$ et $a_i b_i \in J$ donc $x \in I \cap J$.

b) On a $I \cdot J \subset I \cdot (J + L)$ et $I \cdot L \subset I \cdot (J + L)$ donc $(I \cdot J) + (I \cdot L) \subset I \cdot (J + L)$. Réciproquement, soit $x \in I \cdot (J + L)$. On a $x = \sum a_i(b_i + c_i)$ avec $a_i \in I$, $b_i \in J$ et $c_i \in L$. Mais alors $x = (\sum a_i b_i) + (\sum a_i c_i)$, on voit que $\sum a_i b_i \in I \cdot J$ et $\sum a_i c_i \in I \cdot L$. Ainsi $x \in (I \cdot J) + (I \cdot L)$.

c) Soit $x = y + z$ avec $y \in I \cap J$ et $z \in I \cap L$, alors $y + z \in I$ et $y + z \in J + L$ donc $x \in I \cdot (J + L)$.

d) Il s'agit de montrer la réciproque de (ıı) en supposant A principal. Si x et y sont des éléments de A, on notera $x \wedge y$ le p.g.c.d de x et y et $x \vee y$ le p.p.c.m de x et y. Soient a, b et c dans A tels que $I = (a)$, $J = (b)$ et $L = (c)$, on a

$$I \cap (J + L) = (a \vee (b \wedge c)) = ((a \vee b) \wedge (a \vee c)) = ((a \vee b)) + ((a \vee c)) = I \cap J + I \cap L.$$

e) Par (ıı) on sait que $J + (I \cap L) \subset I \cap (J + L)$. Soit $x \in I \cap (J + L)$, on a $x \in I$ et $x = y + z$ avec $y \in J$ et $z \in L$. Comme $J \subset I$, on a $y \in I$, donc $z = x - y \in I$. Ainsi $y \in J$ et $z \in I \cap L$, donc $x \in J + (I \cap L)$.

f) On a $I \cap J = (XY)$ et $I \cap L = (X(X + Y))$. Ainsi

$$I \cap J + I \cap L = (XY) + (X(X + Y)) = (XY, X^2).$$

Par ailleurs, on a $J + L = (Y) + (X + Y) = (X, Y)$, donc

$$I \cap (J + L) = (X) \cap (X, Y) = (X).$$

Ainsi on a bien l'inclusion $I \cap J + I \cap L \subset I \cap (J + L)$ mais pas égalité.

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 $I^n + J^n = A$.

Solution. Comme $I+J=A$, il existe $x \in I$ et $y \in J$ tels que $x+y=1$. En élevant à la puissance $2n$, on a alors

$$1 = \sum_{k=0}^{2n} \binom{2n}{k} x^k y^{2n-k}.$$

Cependant, si $k \in [0,n]$, alors $k \leq n$ donc $x^k \in I^n$ et si $k > n$, alors $2n-k \leq n$ donc $y^{2n-k} \in J^n$. Ainsi $1 \in I^n + J^n$ donc $I^n + J^n = A$.

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 $J = (a)$.

Solution. (i) Soit $x \in I$ et soit $y \in J$, on a $xy \in I$ donc $I \subset (I:J)$. Réciproquement, soit $z \in (I:J)$. On sait que I et J sont comaximaux donc $I+J=A$ et en particulier, il existe $x \in I$ et $y \in J$ tels que $1 = x+y$. Mais alors comme $z \in (I:J)$, on a $zy \in I$. On a donc $z = zx + zy$ avec $zy \in I$ et $zx \in I$ car $x \in I$. Ainsi $z \in I$ et $(I:J) \subset I$, d'où l'égalité.
Soit L tel que $I \cdot L \subset J$. Soit $z \in L$, on réutilise les $x \in I$ et $y \in J$ tels que $x+y=1$. On a alors $z = xz + yz$ or $xz \in I \cdot L \subset J$ et $yz \in J$ car $y \in J$. Ainsi $z \in J$.
(ii) Comme précedement, on a $\mathfrak{p} \subset (\mathfrak{p}:\mathfrak{q})$. Soit $x \in (\mathfrak{p}:\mathfrak{q})$, et soit $y \in \mathfrak{q}$ tel que $y \notin \mathfrak{p}$ (ce qui est possible par hypothèse). On a alors $xy \in \mathfrak{p}$ et comme $\mathfrak{p}$ est premier, $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Comme $y \notin \mathfrak{p}$ c'est que $x \in \mathfrak{p}$ donc $(\mathfrak{p}:\mathfrak{q}) \subset \mathfrak{p}$, d'où l'égalité. De manière symétrique on a l'égalité $\mathfrak{q} = (\mathfrak{q}:\mathfrak{p})$.
Le premier exemple de l'exercice précédent convient : $\mathfrak{p} = (X)$ et $\mathfrak{q} = (Y)$. Alors $\mathfrak{p}$ et $\mathfrak{q}$ sont premiers, $\mathfrak{p} \cdot \mathfrak{q} = (XY) = \mathfrak{p} \cap \mathfrak{q}$ et $\mathfrak{p} + \mathfrak{q} = (X,Y) \subsetneq A$.
(iii) Si $(a) = I \cdot J$, alors on peut écrire $a = \sum x_i y_i$ avec $x_i \in I$ et $y_i \in J$. Ainsi $a \in I$ et $a \in J$. Supposons que $I \not\subset (a)$ et $J \not\subset (a)$, soit alors $x \in I$ avec $x \notin (a)$ et $y \in J$ avec $y \notin (a)$. On a alors $xy \in I \cdot J = (a)$ ce qui est absurde car (a) est premier. Ainsi $I = (a)$ ou $J = (a)$. Disons par exemple que $I = (a)$ (l'autre cas est symétrique).
Dans l'écriture $a = \sum x_i y_i$ on a alors $x_i \in I = (a)$ donc $x_i = a x_i'$. On a donc $a = \sum a x_i' y_i$ et comme A est intègre $1 = \sum x_i' y_i \in J$, donc $J = A$.

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.

Solution. Voici plusieurs contre exemples :
Soient k un corps et $A = k[X,Y]$. On pose $I = (X)$ et $J = (Y)$. Si $P \in I \cap J$, alors X et Y divisent P. Comme X et Y sont irréductibles, on a XY divise P et $I \cap J = (XY) = I \cdot J$. Cependant $I + J = (X,Y) \subsetneq A$.

Soient k un corps et $A = k[X, X^{\frac{1}{2}}, X^{\frac{1}{3}}, \cdots, X^{\frac{1}{n}}, \cdots]$ l'anneau des polynômes en des puissances fractionnaires de X. Tout élément de A s'écrit de manière unique comme somme finie

$$\sum_{r \in \mathbb{Q}_+} a_r X^r.$$

L'ensemble des ""polynômes"" tels que $a_0 = 0$ est un idéal I de A et on a $I^2 = I$. En effet, tout élément

$$P = \sum_{r \in \mathbb{Q}_+^*} a_r X^r \in I$$

peut s'écrire sous la forme

$$P = X^\alpha \sum_{r \in \mathbb{Q}_+^*} a_r X^{r-\alpha}$$

où α est un rationnel strictement positif et strictement plus petit que tous les $r \in \mathbb{Q}_+^*$ tels que $a_r \neq 0$ (il n'y en a qu'un nombre fini).
On a donc $I \cdot I = I = I \cap I$ et pourtant $I + I = I \subsetneq A$.

Soit $\mathcal{C}$ l'anneau des fonctions continues sur $\mathbb{R}$ et I l'idéal des fonctions qui s'annulent en 0. Si $f \in I$, on peut écrire

$$f(x) = \sqrt{|f(x)|} \cdot \sqrt{|f(x)|}\ \mathrm{signe}(f(x))$$

avec $\sqrt{|f(x)|} \in I$ et $\sqrt{|f(x)|}\ \mathrm{signe}(f(x)) \in I$. Ainsi $I \cdot I = I = I \cap I$ et pourtant $I + I = I \subsetneq A$.

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).

Solution. Soit $x \in A$ un élément non nul. Il faut montrer que x est inversible. Considérons la suite d'idéaux $(x) \supset (x^2) \supset \cdots \supset (x^n) \cdots$, il y en a une infinité et comme A n'a qu'un nombre fini d'idéaux, deux d'entre eux (au moins) sont égaux, disons $(x^n) = (x^m)$ avec $m > n \geq 1$. Il existe donc $a \in A$ tel que $x^n = ax^m$. On a donc $x^n(1 - ax^{m-n}) = 0$. Comme A est intègre et $x \neq 0$, on a $1 - ax^{m-n} = 0$. Mais alors on a $x \cdot ax^{m-n-1} = 1$ donc x est inversible (remarquons que $m - n - 1 \geq 0$).

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.

Solution. (i) Commençons par le cas $n = 2$, nous montrerons le cas général par récurrence. Soit I un idéal de A et notons I_1 et I_2 les images de I par les projections de $A_1 \times A_2 \to A_1$ (resp. $A_1 \times A_2 \to A_1$).
Montrons que I_1 est un idéal de A_1. Soient x_1 et y_1 dans I_1 et $a_1 \in A_1$, il existe x_2 et y_2 dans A_2 tels que $x = (x_1, x_2) \in I$ et $y = (y_1, y_2) \in I$. On a alors $x + y \in I$ donc $(x_1 + y_1, x_2 + y_2) \in I$ et donc $x_1 + y_1 \in I_1$. Par ailleurs, on a pour tout $a_2 \in A_2$, $(a_1, a_2) \cdot (x_1, x_2) \in I$ donc $(a_1x_1, a_2x_2) \in I$ et donc $a_1x_1 \in I_1$. Par conséquent, I_1 est un idéal et de même I_2 aussi.
Montrons maintenant que $I = I_1 \times I_2$. Soit $x = (x_1, x_2) \in I$, alors $x_1 \in I_1$ et $x_2 \in I_2$ donc $I \subset I_1 \times I_2$. Réciproquement, soit $(x_1, x_2) \in I_1 \times I_2$, il existe alors $x_1' \in A_1$ et $x_2' \in A_2$ tels que $(x_1, x_2') \in I$ et $(x_1', x_2) \in I$. Mais alors on a

$$(x_1, x_2) = (1, 0) \cdot (x_1, x_2') + (0, 1)(x_1', x_2) \in I.$$

Lorsque $n \geq 2$, on procède par récurrence sur n : les idéaux de $A_1 \times \cdots \times A_n$ sont de la forme $I_1 \times J$ où J est un idéal de $A_2 \times \cdots \times A_n$. Par récurrence, on a $J = I_2 \times \cdots \times I_n$.
(ii) Soit $I = I_1 \times \cdots \times I_n$ un idéal de A, il est premier si et seulement si $A/I = A_1/I_1 \times \cdots \times A_n/I_n$ est intègre. Ce produit est intègre si et seulement s'il n'a qu'un terme (disons A_i/I_i) et que ce terme est intègre (c'est-à-dire I_i premier). Les idéaux premiers de A sont donc de la forme $A_1 \times \cdots \times I_i \times \cdots A_n$ avec I_i idéal premier de A_i. De même $I = I_1 \times \cdots \times I_n$ est maximal si et seulement si $A/I = A_1/I_1 \times \cdots \times A_n/I_n$ est un corps. Il doit donc être premier et le quotient A_i/I_i doit être un corps donc I_i est maximal. Les idéaux maximaux sont de la forme $A_1 \times \cdots \times I_i \times \cdots A_n$ avec I_i idéal maximal de A_i.
(iii) Si A_i est un corps, ses seuls idéaux sont (0) et A_i. Un idéal de A étant de la forme $I = I_1 \times \cdots \times I_n$, pour chaque indice i, on a deux possibilités : $I_i = (0)$ ou $I_i = A_i$. On a donc 2^n idéaux dans A. Il y en a n premiers qui sont aussi maximaux.

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.

Solution. (i) Supposons que pour tout $x \in K$, il existe $f \in I$ telle que $f(x) \neq 0$. On a alors

$$\bigcap_{f \in I} f^{-1}(0) = \emptyset.$$

Les complémentaires notés U_f des fermés $f^{-1}(0)$ sont ouverts et vérifient :

$$\bigcup_{f \in I} U_f = K.$$

Comme K est compact, on peut extraire un sous-recouvrement fini de ce recouvrement, il existe donc des éléments $f_1, \cdots, f_n$ de I tels que

$$\bigcup_{i=1}^{n} U_{f_i} = K.$$

Posons alors

$$f(x) = \sum_{i=1}^{n} f_i^2(x).$$

Pour tout $x \in K$, il existe i tel que $x \in U_{f_i}$ et donc $f_i(x) \neq 0$, ainsi pour tout $x \in K$, on a $f(x) > 0$. Mais alors f est inversible donc $I = A$, c'est absurde.
(ii) Soit $x \in K$, et considérons $I_x = \{f \in A \ / \ f(x) = 0\}$. Montrons que I_x est maximal. On a le morphisme $\varphi_x : A \to \mathbb{R}$ défini par $\varphi(f) = f(x)$. Ce morphisme est surjectif et son noyau est exactement I_x. Ainsi $A/I_x = \mathbb{R}$ qui est un corps donc I_x est maximal.
Réciproquement, soit I un idéal maximal. On a vu qu'il existe $x \in K$ tel que pour tout $f \in I$, on a $f(x) = 0$. Ainsi $I \subset I_x$. Mais comme I est maximal, on a nécessairement $I = I_x$.
Les idéaux maximaux sont donc les I_x pour $x \in K$. Enfin, remarquons que si $x \neq y$, alors $I_x \neq I_y$. En effet, il existe toujours $f \in A$ telle que $f(x) = 0 \neq f(y)$ (c'est le lemme de Tietze-Urysohn).

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 $n > 0$.

Solution. (i) Soit φ un morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{R}$, on a

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1.$$

Ainsi $\varphi(i) \in \mathbb{R}$ et $\varphi(i)^2 = -1$. C'est impossible.
(ii) Soit φ un morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{Q}$, on a

$$\varphi(\sqrt{2})^2 = \varphi(\sqrt{2}^2) = \varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1 + 1 = 2.$$

Ainsi $\varphi(\sqrt{2}) \in \mathbb{Q}$ et $\varphi(\sqrt{2})^2 = 2$. C'est impossible car $\sqrt{2}$ et $-\sqrt{2}$ ne sont pas rationnels.
(iii) Soit φ un morphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Z}$, on a

$$2 \cdot \varphi(\frac{1}{2}) = (1+1)\varphi(\frac{1}{2}) = (\varphi(1) + \varphi(1))\varphi(\frac{1}{2}) = \varphi(1+1)\varphi(\frac{1}{2}) = \varphi(2)\varphi(\frac{1}{2}) = \varphi(2 \cdot \frac{1}{2}) = \varphi(1) = 1.$$

Ainsi $\varphi(\frac{1}{2}) \in \mathbb{Z}$ et $2\varphi(\frac{1}{2}) = 1$. C'est impossible.
(i) Soit φ un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$ et notons $\overline{x}$ la classe dans $\mathbb{Z}/n\mathbb{Z}$ de $x \in \mathbb{Z}$. On a

$$0 = \varphi(0) = \varphi(\overline{n}) = \varphi(\underbrace{\overline{1} + \cdots + \overline{1}}_{n \text{ fois}}) = \underbrace{\varphi(\overline{1}) + \cdots + \varphi(\overline{1})}_{n \text{ fois}} = n \cdot \varphi(\overline{1}) = n.$$

On trouve que $0 = n > 0$ dans $\mathbb{Z}$, c'est absurde.

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.

Solution. Soit φ un morphisme d'anneau de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Nous noterons $\hat{x}$ et $\overline{x}$ respectivement les classes de $x \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ et respectivement dans $\mathbb{Z}/m\mathbb{Z}$. Alors on a

$$0 = \varphi(0) = \varphi(\hat{n}) = \varphi(\underbrace{\hat{1} + \cdots + \hat{1}}_{n \text{ fois}}) = \underbrace{\varphi(\hat{1}) + \cdots + \varphi(\hat{1})}_{n \text{ fois}} = n \cdot \varphi(\hat{1}) = n \cdot \overline{1} = \overline{n}.$$

Ainsi pour que φ existe, il faut que $\overline{n} = \overline{0} \in \mathbb{Z}/m\mathbb{Z}$ c'est-à-dire m divise n.
Définir un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est équivalent à définir un morphisme φ de $\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ tel que $\varphi(n) = \overline{0}$. Cependant on a nécessairement $\varphi(1) = \overline{1}$ donc $\varphi(n) = \overline{0} \Leftrightarrow \overline{n} = \overline{0}$ ce qui est équivalent au fait que m divise n. Par ailleurs le morphisme est unique car $\varphi(x) = \overline{x}$ pour tout $x \in \mathbb{Z}$.

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 $rs \in R$.

Solution. Supposons qu'il existe $x \in A$ tel que $1 \cdot x = 0$, alors $x = 0$ donc $1 \in R$.
Soient maintenant r et s deux éléments non diviseurs de 0. Supposons qu'il existe $x \in A$ tel que $x \cdot rs = 0$. On a alors $xr \cdot s = 0$ donc comme s n'est pas diviseur de 0, on a $xr = 0$ et comme r n'est pas diviseur de 0, on a $x = 0$. Ainsi $rs \in R$.

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

Solution. Soit $a \in A$ un élément régulier (c'est-à-dire non diviseur de 0). On considère alors le morphisme d'anneau : $\mu_a : A \to A$ défini par $\mu_a(x) = ax$. Comme a est régulier cette application est injective. Mais comme A est fini, l'application est aussi surjective et donc il existe $b \in A$ tel que $\mu_a(b) = 1$ c'est-à-dire $ab = 1$ donc a est inversible.

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 ?

Solution. Remarque préliminaire :
Soit $\mathfrak{p}$ un idéal de B, alors comme $0 \in \mathfrak{p}$, alors $f^{-1}(\mathfrak{p}) \supset \ker f$. Ainsi le morphisme induit

$$\overline{f} : A/f^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$$

est injectif : si $\overline{x} \in \ker \overline{f}$, alors $f(x) \in \mathfrak{p}$ donc $x \in f^{-1}(\mathfrak{p})$ donc $\overline{x} = 0$. Ainsi $\overline{f}$ est toujours injectif.
(i) Si $\mathfrak{p}$ est premier, alors $B/\mathfrak{p}$ est intègre, mais comme $\overline{f} : A/f^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$ est injectif, $A/f^{-1}(\mathfrak{p})$ est aussi intègre donc $f^{-1}(\mathfrak{p})$ est premier.
(ii) Si f n'est pas surjectif, c'est faux. Par exemple considérons l'inclusion $\mathbb{Z} \to \mathbb{Q}$ et prenons $\mathfrak{p} = (0) \subset \mathbb{Q}$ qui est un idéal maximal de $\mathbb{Q}$. Alors $f^{-1}(\mathfrak{p}) = (0)$ qui est un idéal premier de $\mathbb{Z}$ (car $\mathbb{Z}/(0)$ est intègre) mais pas maximal (car $\mathbb{Z}/(0)$ n'est pas un corps).
Si par contre f est surjectif, alors $\overline{f}$ est surjectif. Or on a vu qu'il est injectif donc il est bijectif. Si $\mathfrak{p}$ est maximal, alors $B/\mathfrak{p}$ est un corps et donc $A/f^{-1}(\mathfrak{p})$ aussi (car $\overline{f}$ est bijective) et $f^{-1}(\mathfrak{p})$ est maximal.

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.

Solution. (i) Soit $\mathcal{C} = \{J \subset A, \text{ idéal } / \ I \subset J\}$ et $\mathcal{E} = \{L \subset A/I \ / \ J \text{ est un idéal}\}$. Considérons les applications suivantes $f : \mathcal{C} \to \mathcal{E}$, $f(J) = \pi(J)$ ($\pi(J)$ est bien un idéal de A/I car il est stable par addition et si $\pi(a) \in A/I$ et $\pi(j) \in \pi(J)$, alors $\pi(a)\pi(j) = \pi(aj) \in \pi(J)$) et $g : \mathcal{E} \to \mathcal{C}$, $g(L) = \pi^{-1}(L)$ ($\pi^{-1}(L)$ contient bien I car $0 \in L$ et $\pi^{-1}(0) = I$).
Nous montrons que f et g sont des bijections réciproques. On a $f(g(L)) = \pi(\pi^{-1}(L)) \subset L$. Soit maintenant $x \in L$, comme π est surjective, on peut écrire $x = \pi(a)$, mais alors $a \in \pi^{-1}(L)$ et donc $x \in \pi(\pi^{-1}(L))$. On a bien $f \circ g = \mathrm{Id}_{\mathcal{E}}$.
Par ailleurs, $g(f(J)) = \pi^{-1}(\pi(J)) = J + I = J$ car $I \subset J$. On a bien $g \circ f \mathrm{Id}_{\mathcal{C}}$.
(ii) Supposons maintenant que $J \in \mathcal{C}$ est premier, c'est-à-dire A/J est intègre. Son image dans $\mathcal{E}$ est $\pi(J) = J/I$ et on a $(A/I)/(J/I) \simeq A/J$ est intègre donc $\pi(J)$ est premier.
Réciproquement, si $L \in \mathcal{E}$ est premier, c'est-à-dire $(A/I)/L$ est intègre. Son image dans $\mathcal{C}$ est $J = \pi^{-1}(L)$ et on a $A/L = (A/I)/(J/I) \simeq A/J$ est intègre donc J est premier.
De même en remplaçant premier par maximal et anneau intègre par corps, on a le résultat pour 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 $\mathbb{C}$.

Solution. Rappelons les résultats suivants :
• si k est un corps, les idéaux premiers de $k[X]$ sont les (P) avec P irréductible. En effet, soit (P) un idéal premier (rappelons que $k[X]$ est euclidien donc principal ainsi tout idéal est de la forme (P)), si $P = P_1P_2$, alors $\overline{P_1}\overline{P_2} = 0$ dans $k[X]/(P)$. Ceci impose comme (P) est premier que $\overline{P_1} = 0$ ou $\overline{P_2} = 0$ et donc P_1 ou P_2 est multiple de P, l'autre polynôme est donc constant. Ainsi P est irréductible.
Réciproquement, si P est irréductible et que P_1 et P_2 sont deux éléments de $k[X]$ tels que $\overline{P}_1\overline{P}_2 = 0$ dans $k[X]/(P)$, alors P divise le produit P_1P_2 et comme P est irréductible, il divise l'un ou l'autre c'est-à-dire $\overline{P_1} = 0$ ou $\overline{P_2} = 0$ donc (P) est premier.
• Si A est un anneau et I un idéal et soit $\pi : A \to A/I$. Les idéaux premiers de A/I sont en bijection (définie par $J \mapsto \pi(J)$ et de bijection réciproque $\overline{J} \mapsto \pi^{-1}(\overline{J})$) avec les idéaux premiers de A contenant I (cf. exercice précédent).
Nous pouvons maintenant résoudre l'exercice.
(i) Les idéaux premiers de $\mathbb{C}[X]$ sont les (P) avec P irréductible. Or sur $\mathbb{C}$ qui est algébriquement clos, les polynômes irréductibles sont les $X-a$ avec $a \in \mathbb{C}$. Les idéaux premiers de $\mathbb{C}[X]$ sont donc les $(X-a)$ avec $a \in \mathbb{C}$.
(ii) Les idéaux premiers de $\mathbb{R}[X]/(X^2+X+1)$ sont en bijection avec les idéaux premiers de $\mathbb{R}[X]$ qui contiennent (X^2+X+1). Les idéaux premiers de $\mathbb{R}[X]$ sont les (P) avec P irréductible. Si de plus on a $(X^2+X+1) \subset (P)$ alors P divise X^2+X+1. Comme X^2+X+1 est irréductible, ceci impose que $P = a(X^2+X+1)$ avec $0 \neq a \in \mathbb{R}$. Ainsi il y a un unique idéal premier contenant (X^2+X+1) c'est (X^2+X+1) lui-même. L'anneau $\mathbb{R}[X]/(X^2+X+1)$ a donc un unique idéal premier : (0).
(iii) Les idéaux premiers de $\mathbb{R}[X]/(X^3-6X^2+11X-6)$ sont en bijection avec les idéaux premiers de $\mathbb{R}[X]$ qui contiennent $(X^3-6X^2+11X-6)$. Les idéaux premiers de $\mathbb{R}[X]$ sont les (P) avec P irréductible. Si de plus on a $(X^3-6X^2+11X-6) \subset (P)$ alors P divise le polynôme $X^3-6X^2+11X-6$. On écrit la décomposition de $X^3-6X^2+11X-6$ dans $\mathbb{R}[X]$:

$$X^3-6X^2+11X-6 = (X-1)(X^2-5X+6) = (X-1)(X-2)(X-3).$$

Les polynômes irréductibles qui divisent $X^3-6X^2+11X-6$ sont donc $X-1$, $X-2$ et $X-3$. Il y a donc trois idéaux premiers dans $\mathbb{R}[X]/(X^3-6X^2+11X-6)$ qui sont $(X-1)/(X^3-6X^2+11X-6)$, $(X-2)/(X^3-6X^2+11X-6)$ et $(X-3)/(X^3-6X^2+11X-6)$.
(iv) Les idéaux premiers de $\mathbb{R}[X]/(X^4-1)$ sont en bijection avec les idéaux premiers de $\mathbb{R}[X]$ qui contiennent (X^4). Les idéaux premiers de $\mathbb{R}[X]$ sont les (P) avec P irréductible. Si de plus on a $(X^4-1) \subset (P)$ alors P divise le polynôme X^4-1. On écrit la décomposition de X^4-1 dans $\mathbb{R}[X]$:

$$X^4-1 = (X-1)(X+1)(X^2+1).$$

Les polynômes irréductibles qui divisent X^4-1 sont donc $X-1$, $X+1$ et X^2+1. Il y a donc trois idéaux premiers dans $\mathbb{R}[X]/(X^4-1)$ qui sont $(X-1)/(X^4-1)$, $(X+1)/(X^4-1)$ et $(X^2+1)/(X^4-1)$.
(v) Cas (i) : soit $\varphi : \mathbb{C}[X] \to \mathbb{C}$ un morphisme de $\mathbb{R}$-algèbres, on a

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1,$$

donc $\varphi(i) = \pm i$. Soit $\alpha \in \mathbb{C}$ l'image de X et soit $P \in \mathbb{C}[X]$ avec $P = \sum a_nX^n + i\sum b_nX^n$ où a_n et b_n sont dans $\mathbb{R}$, on a :

$$\varphi(P) = \sum a_n\alpha^n + \varphi(i)\sum b_n\alpha^n.$$

Ainsi si $\varphi(i) = i$, alors $\varphi(P) = P(\alpha)$ et si $\varphi(i) = -i$, alors $\varphi(P) = \overline{P}(\alpha)$. Aucun de ces morphismes n'a son image contenue dans $\mathbb{R}$.
Cas (ii) : les morphismes φ de $\mathbb{R}$-algèbre de $\mathbb{R}[X]/(X^2+X+1)$ dans $\mathbb{C}$ sont les morphismes φ de $\mathbb{R}$-algèbre de $\mathbb{R}[X]$ dans $\mathbb{C}$ qui envoient X^2+X+1 sur 0. Le raisonnement précédent montre que $\varphi(P) = P(\alpha)$ pour un certain $\alpha = \varphi(X)$ (ici il n'y a pas le problème avec i). Par ailleurs, il faut que $0 = \varphi(X^2+X+1) = \alpha^2+\alpha+1$. On a donc $\alpha = j$ ou $\alpha = j^2$. Il y a donc deux morphismes dans $\mathbb{C}$ donnés par $\varphi(P) = P(j)$ et $\varphi(P) = P(j^2)$. Aucun de ces morphismes n'a son image contenue dans $\mathbb{R}$.

Cas (iii) : le même raisonnement montre que les morphismes de $\mathbb{R}$-algèbre dans $\mathbb{C}$ sont donnés par $\varphi(P) = P(1)$, $\varphi(P) = P(2)$ ou $\varphi(P) = P(3)$. Tous ces morphismes sont à valeurs dans $\mathbb{R}$.
Cas (iv) : cette fois-ci les morphismes de $\mathbb{R}$-algèbre dans $\mathbb{C}$ sont donnés par $\varphi(P) = P(1)$, $\varphi(P) = P(-1)$, $\varphi(P) = P(i)$ ou $\varphi(P) = P(-i)$. Les deux premiers sont à valeurs dans $\mathbb{R}$ et pas les deux derniers.

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.

Solution. Supposons que $\mathfrak{p}$ ne contienne aucun des idéaux I_i, alors pour chaque i, il existe $x_i \in I_i$ tel que $x_i \notin \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, le produit de ces x_i n'est pas dans $\mathfrak{p}$. Cependant on a

$$\prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} I_i \subset \mathfrak{p}$$

ce qui est une contradiction.

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 $\mathfrak{p}_i$.

Solution. Quitte à remplacer les $\mathfrak{p}_i$ par un sous-ensemble, on peut supposer qu'aucun des $\mathfrak{p}_i$ n'est contenu dans un $\mathfrak{p}_j$ (sinon on garde le plus grand, le plus petit ne sert à rien).
Remarquons que comme $\mathfrak{p}_j \not\subset \mathfrak{p}_1$ pour $j \geq 2$, on peut trouver $b_j \in \mathfrak{p}_j$ tel que $b_j \notin \mathfrak{p}_1$ et on a $a_1 = b_2 \cdots b_n \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ mais $a_1 \notin \mathfrak{p}_1$. De même on peut trouver des $a_j \notin \mathfrak{p}_j$ tels que a_j appartienne à tous les autres $\mathfrak{p}_i$.
Supposons que I n'est contenu dans aucun $\mathfrak{p}_i$, alors pour tout i, il existe $x_i \in I$ tel que $x_i \notin \mathfrak{p}_i$.
Considérons l'élément $x = \sum a_i x_i$. Comme $x_i \in I$ pour tout i, on a $x \in I$.
Par ailleurs, comme $a_1 \notin \mathfrak{p}_1$, $x_1 \notin \mathfrak{p}_1$ et que $\mathfrak{p}_1$ est premier on a $a_1 x_1 \notin \mathfrak{p}_1$. Mais on a $a_2 x_2 + \cdots a_n x_n \in \mathfrak{p}_1$ car tous les $a_i \in \mathfrak{p}_1$ pour $i \geq 2$, ainsi $x \notin \mathfrak{p}_1$. De même, $x \notin \mathfrak{p}_i$ pour tout i, donc

$$x \notin \cup_{i=1}^{n} \mathfrak{p}_i$$

ce qui est absurde.

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

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

Solution. Soient $a \in A$ et $x \in$ nil(A), alors il existe $n \in \mathbb{N}$ tel que $x^n = 0$, mais alors $(ax)^n = a^n x^n = 0$ donc $ax \in$ nil(A).
Soient x et y des éléments de nil(A), alors il existe $n \in \mathbb{N}$ tel que $x^n = 0$ et $m \in \mathbb{N}$ tel que $y^m = 0$. On calcule alors

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Si $k \in [0, n]$, alors $n + m - k \geq m$ donc $y^{n+m-k} = 0$ et si $k \in [n, n+m]$, alors $x^k = 0$. Ainsi $(x+y)^{n+m} = 0$ et $x + y \in$ nil(A).
(ii) Soit $\mathfrak{p}$ un idéal premier et $x \in$ nil(A), il existe alors $n \in \mathbb{N}$ tel que $x^n = 0 \in \mathfrak{p}$. Mais comme $\mathfrak{p}$ est premier, ceci impose que $x \in \mathfrak{p}$.
(iii) Montrons que l'ensemble des idéaux de A disjoints de S vérifie les hypothèses du lemme de Zorn c'est-à-dire est inductif pour l'inclusion : pour toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux disjoints de S, alors la réunion I de ces idéaux est encore un idéal disjoint de S.

Il est clair que I est encore un idéal, en effet, si x et y sont dans I, alors il existe n et m tels que $x \in I_n$ et $y \in I_m$ et on a $x + y \in I_{\max(n,m)} \subset I$. De même si $a \in A$, alors $ax \in I_n \subset I$.
Il reste à voir que I ne rencontre pas S. Mais si I rencontrait S, alors il existerait $k \in \mathbb{N}$ tel que $s^k \in I$ ce qui signifie qu'alors il existerait un $n \in \mathbb{N}$ tel que $s^k \in I_n$, c'est-à-dire que I_n rencontrerait S, c'est absurde.
Ainsi par le lemme de Zorn, il existe un idéal maximal parmi les idéaux de A disjoints de S. Soit $\mathfrak{p}$ un tel idéal, montrons qu'il est premier. Soient donc x et y dans A tels que $xy \in \mathfrak{p}$. Il faut montrer que $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Si on a $x \notin \mathfrak{p}$ et $y \notin \mathfrak{p}$, alors les idéaux $\mathfrak{p} + (x)$ et $\mathfrak{p} + (y)$ rencontrent S. Il existent donc n et m des entiers tels que

$$s^n = p_1 + a_1 x \quad \text{et} \quad s^m = p_2 + a_2 y$$

avec $p_i \in \mathfrak{p}$ et $a_i \in A$. Alors on calcule le produit, on a

$$s^{n+m} = p_1 p_2 + p_1 a_2 y + p_2 a_1 x + a_1 a_2 xy \in \mathfrak{p}.$$

Ce qui est absurde car $\mathfrak{p}$ ne rencontre pas S. L'idéal $\mathfrak{p}$ est donc premier.
Montrons la dernière égalité. On a vu au (ıı) que pour tout idéal premier, on a $\mathrm{nil(A)} \subset \mathfrak{p}$ donc

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

Réciproquement, soit $s \notin \mathrm{nil(A)}$, d'après ce qu'on vient de montrer, il existe un idéal premier $\mathfrak{p}$ tel que $\mathfrak{p}$ ne rencontre pas S, en particulier $s \notin \mathfrak{p}$ ce qui montre que $s \notin \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$.

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

Solution. Soit $\mathfrak{p}$ un idéal premier et soit $\mathfrak{m}$ un idéal le contenant. Comme l'anneau est principal, on peut écrire $\mathfrak{p} = (p)$ et $\mathfrak{m} = (m)$. Le fait que $\mathfrak{p} \subset \mathfrak{m}$ se traduit par : $p = am$ avec $a \in A$. Mais alors comme $\mathfrak{p}$ est premier, on a $a \in \mathfrak{p}$ ou $m \in \mathfrak{p}$. Si $m \in \mathfrak{p}$, alors $\mathfrak{p} = \mathfrak{m}$ et on a fini. Sinon, alors $a \in \mathfrak{p}$ donc il existe $u \in A$ tel que $a = up$ donc $p = upm$ et comme A est intègre (car principal) on a $1 = um$ donc m est inversible et $\mathfrak{m} = A$. L'idéal $\mathfrak{p}$ est donc maximal.

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

Solution. On montre que $\mathbb{C}[X,Y]/(Y - X^2)$ est isomorphe à $\mathbb{C}[X]$. En effet, introduisons le morhisme d'anneaux : $\varphi : \mathbb{C}[X,Y] \to \mathbb{C}[X]$ défini par $\varphi(P) = P(X, X^2)$. Il est clair que φ est surjectif. On a $\varphi(Y - X^2) = X^2 - X^2 = 0$ donc $Y - X^2 \in \ker\varphi$. Par ailleurs, si $P \in \ker\varphi$ on peut effectuer la division euclidienne de P par $Y - X^2$ car le coefficient dominant de $Y - X^2$ dans $\mathbb{C}[X][Y]$ est égal à 1 donc inversible. On a ainsi $P(X,Y) = (Y - X^2)Q(X,Y) + R(X,Y)$ où $R(X,Y)$ est un polynôme de $\mathbb{C}[X][Y]$ de degré en Y strictement inférieur à celui de $Y - X^2$, c'est-à-dire de degré nul. Donc $R(X,Y)$ est un polynôme en X uniquement. On a donc

$$0 = \varphi(P) = \varphi(Y - X^2)\varphi(Q) + \varphi(R) = \varphi(R).$$

Mais $\varphi(R) = R(X, X^2) = R(X)$ donc $R = 0$ et $P \in (Y - X^2)$. On a donc $\ker\varphi = (Y - X^2)$ ce qui nous donne un isomorphisme

$$\overline{\varphi} : \mathbb{C}[X,Y]/(Y - X^2) \to \mathbb{C}[X].$$

Comme $\mathbb{C}[X]$ est principal, $\mathbb{C}[X,Y]/(Y - X^2)$ l'est aussi.

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.

Solution. (ı) Si $y = Cl(Y)$, on a $xy = 1$ donc x est inversible d'inverse y (en particulier $y = x^{-1}$. Soit $a \in A$, on peut écrire

$$a = \sum_{i,j} \alpha_{i,j} x^i y^j = \sum_{i,j} \alpha_{i,j} x^i x^{-j} = \sum_{i,j} \alpha_{i,j} x^{i-j} = \sum_k \beta_k x^k,$$

où $\beta_k = \sum_j \alpha_{j+k,j}$. Soit m le plus petit entier tel que $\beta_m \neq 0$ (il existe car il n'y a qu'un nombre fini de $\alpha_{i,j}$ non nuls) et soit $P(X) = \sum_{k \geq 0} \beta_{k+m} X^k$. On a bien $a = x^m P(x)$ et $P(0) = \beta_m \neq 0$. Il reste à voir que

cette écriture est unique. Si on a deux telles écriture $x^m P(x) = a = x^n Q(x)$ avec disons $m \leq n$, alors on a $x^m(P(x) - x^{n-m}Q(x)) = 0$ et comme x est inversible on a $P(x) - x^{n-m}Q(x) = 0$. Ceci signifie que $XY - 1$ divise $P(X) - X^{n-m}Q(X)$ et comme ce dernier polynôme est de degré 0 en Y ceci impose que $P(X) - X^{n-m}Q(X) = 0$. On a donc $P(X) = X^{n-m}Q(X)$ et $P(0) \neq 0$. Ceci impose que $n = m$ et on a alors $P = Q$.
(ii) Si $a = 0$, on choisit $q = r = 0$. Sinon, écrivons $a = x^m A(x)$ et $b = x^n B(x)$ où A et B sont des polynômes tels que $A(0) \neq 0$ et $B(0) \neq 0$. Effectuons la division euclidienne de A par B : il existe Q et R deux polynômes tels que $R = 0$ ou $\deg R < \deg B$ tels que $A = BQ + R$. Mais alors on a

$$a = x^m A(x) = x^m B(x)Q(x) + x^m R(x) = x^n B(x)x^{n-m}Q(x) + x^m R(x).$$

On pose alors $q = x^{n-m}Q(x)$ et $r = x^m R(x)$ et on a $a = bq + r$. Si $R = 0$, on a $r = 0$ ce qui convient. Si $R(0) \neq 0$, alors $e(r) = \deg R < \deg B = e(b)$. Si enfin $R(0) = 0$, alors il existe $k > 0$ tel que $R(X) = X^k U(X)$ avec $U(0) \neq 0$. On a alors $r = x^{m+k}U(x)$ et

$$e(r) = \deg U = \deg R - k < \deg R < \deg B = e(b).$$

(iii) Soit I un idéal, si $I = (0)$, alors I est principal, sinon soit $b \in I$ tel que $e(b)$ soit minimal. Soit maintenant $a \in I$, on a $a = bq + r$ avec $r = 0$ ou $e(r) < e(b)$. Comme a et b sont dans I, on a $r \in I$. Comme $e(b)$ est minimal, on a nécessairement $r = 0$ donc $a = bq \in (b)$ donc $I = (b)$.

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.

Solution. (i) Soient x et y les images de X et Y dans A. On a $x^2 = xy = y^2$, ainsi tou élément de A s'écrit sous la forme $a + bx + cy$ avec a, b et c dans k. Cet élément est inversible si et seulement s'il existe a', b' et c' dans k tels que

$$(a + bx + cy)(a' + b'x + c'y) = 1$$

c'est-à-dire

$$aa' + (ab' + a'b)x + (ac' + a'c)y = 1.$$

Ceci impose que l'on ait $aa' = 1$, $ab' + a'b = 0$ et $ac' + a'c = 0$. Ce système a une solution si et seulement si $a \neq 0$, la solution est alors $a' = \frac{1}{a}$, $b' = -\frac{b}{a^2}$ et $c' = -\frac{c}{a^2}$. Ainsi $a + bx + cy$ est inversible si et seulement si $a \neq 0$.
(ii) Soit I un idéal principal de A. Si $I = A$, alors I est engendré par un élément inversible quelconque. Supposons $I \neq A$, alors I est engendré par un élément non inversible donc de la forme $bx + cy$. Il reste à déterminer à quelle condition deux éléments $bx + cy$ et $b'x + c'y$ définissent le même idéal c'est-à-dire à quelle condition ils diffèrent par multiplication par un inversible.
On cherche donc $\alpha + \beta x + \gamma y$ tel que $\alpha \neq 0$ et $(\alpha + \beta x + \gamma y)(bx + cy) = b'x + c'y$. Ceci nous donne $\alpha b = b'$ et $\alpha c = c'$, c'est-à-dire les couple (b, c) et (b', c') sont proportionnels. Ainsi, on voit que si $b \neq 0$, on peut supposer $b = 1$ et on a $c \in k$ quelconque. Si par contre $b = 0$ et $c \neq 0$, on peut supposer $c = 1$ et on a le couple $(0, 1)$, enfin il y a le couple $(0, 0)$. Les idéaux principaux de A sont donc A, $(x + cy)$, (y) et (0).
(iii) Soit I un idéal non principal de A. Alors I est engendré par deux éléments qui sont de la forme $ax + by$ et $cx + dy$ (ils ne peuvent être inversibles sinon $I = A$ est principal) et non proportionnels. Ainsi les vecteurs (a, b) et (c, d) engendrent tout k^2 c'est-à-dire que $ax + by$ et $cx + dy$ engendrent tous les termes de la forme $\alpha x + \beta y$. L'idéal I contient donc l'idéal (x, y). Or $A/(x, y) \simeq k$ donc (x, y) est maximal. Comme $I \neq A$, on a $I = (x, y)$ qui est le seul idéal non principal 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 $I = A$.

Solution. On écrit $\mathfrak{p} = (a)$ avec $a \neq 0$ et $I = (b)$. Comme $I \supset \mathfrak{p}$, alors b divise a, c'est-à-dire $a = ub$. Comme $\mathfrak{p}$ est premier ceci impose que $b \in (a)$ ou $u \in (a)$. Dans le premier cas on a $I = \mathfrak{p}$. Dans le second cas $u = ax$ donc $a = axb$ et comme $a \neq 0$ et A intègre on a $1 = xb$ donc b est inversible et $I = A$. Cet exercice est une autre forme du premier exercice du paragraphe.

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

Solution. Tout élément de $\mathbb{Z}[\sqrt{2}]$ s'écrit de manière unique sous la forme $a + b\sqrt{2}$ avec a et b dans $\mathbb{Z}$ (l'unicité résulte du fait que $\sqrt{2} \notin \mathbb{Q}$).
De même tout élément de $\mathbb{Z}[\sqrt{3}]$ s'écrit de manière unique sous la forme $a + b\sqrt{3}$ avec a et b dans $\mathbb{Z}$ (l'unicité résulte du fait que $\sqrt{3} \notin \mathbb{Q}$).

Soit maintenant $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ un morphisme d'anneaux, alors $\varphi'\sqrt{2}) = a + b\sqrt{3}$ avec a et b dans $\mathbb{Z}$. Mais alors on a

$$\varphi(2) = \varphi(\sqrt{2}^{\,2}) = \varphi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Par ailleurs, on a $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$. Ainsi on doit avoir l'égalité

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2.$$

Ceci impose $a^2 + 3b^2 = 2$ et $2ab = 0$. On a donc $a = 0$ ou $b = 0$. Si $a = 0$, alors $3b^2 = 2$ ce qui est impossible (on a pas $b = 0$ et si $b \geq 1$, alors $3b^2 > 2$). Si $b = 0$, alors $a^2 = 2$ qui n'a pas de solution dans $\mathbb{Z}$ car $\sqrt{2} \notin \mathbb{Q}$.

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) $f_*\big(\sqrt{I}\big) \subset \sqrt{f_*(I)}$ et $f^{-1}\big(\sqrt{J}\big) = \sqrt{f^{-1}(J)}$.

Solution. (i) Soit $x \in I$, alors $f(x) \in f(I) \subset f_*(I)$ et donc $x \in f^{-1}(f_*(I))$. Soit maintenant $y \in f_*(f^{-1}(J))$, alors on peut écrire $y = \sum b_i y_i$ avec $b_i \in B$ et $y_i \in f(f^{-1}(J)) \subset J$. Mais alors $y \in J$.
(ii) Si on applique (i) à $f^{-1}(J)$, on a $f^{-1}(J) \subset f^{-1}(f_*(f^{-1}(J)))$. Mais par (i), on a aussi $f_*(f^{-1}(J)) \subset J$ donc $f^{-1}(f_*(f^{-1}(J))) \subset f^{-1}(J)$.
De même, on applique (i) à $f_*(I)$, on a $f_*(f^{-1}(f_*(I))) \subset f_*(I)$. Mais par (i), on a aussi $I \subset f^{-1}(f_*(I))$ donc $f_*(I) \subset f_*(f^{-1}(f_*I))$.
(iii) Si $I \in \mathcal{C}$, alors $I = f^{-1}(J)$, ainsi par (ii) on a bien $I = f^{-1}(f_*I)$. Réciproquement si $I = f^{-1}(f_*I)$, alors I est la contraction de f_*I idéal de B.
Si $J \in \mathcal{E}$, alors $J = f_*I$ et par (ii) on a bien $J = f_*(f^{-1}(J))$. Réciproquement, si on a $J = f_*(f^{-1}(J))$, alors J est l'extension de $f^{-1}(J)$ idéal de A.
(iv) Considérons les applications $f_* : \mathcal{C} \to \mathcal{E}$ et $f^{-1} : \mathcal{E} \to \mathcal{C}$ définies par $I \mapsto f_*I$ et $J \mapsto f^{-1}(J)$. On a alors par (iii) : si $I \in \mathcal{C}$, alors $f^{-1}(f_*I) = I$ et si $J \in \mathcal{E}$, alors $f_*(f^{-1}(J)) = J$. Ainsi f^{-1} est la bijection réciproque de f_*.
(v) Soit $y \in f_*(I_1 + I_2)$, alors $y = \sum_i b_i y_i$ avec $b_i \in B$ et $y_i \in f(I_1 + I_2)$. Ainsi, on a $y_i = f(x_{i,1} + x_{i,2})$ avec $x_{i,1} \in I_1$ et $x_{i,2} \in I_2$. Mais alors on a $y = \sum b_i f(x_{i,1}) + \sum b_i f(x_{i,2})$ et donc $y \in f_*(I_1) + f_*(I_2)$.
Réciproquement, si $y \in f_*(I_1) + f_*(I_2)$, alors $y = \sum b_i f(x_{i,1}) + \sum b_i f(x_{i,2})$ avec $x_{i,1} \in I_1$ et $x_{i,2} \in I_2$. Mais alors on a $y = \sum b_i f(x_{i,1} + x_{i,2}) \in f_*(I_1 + I_2)$.
Soit $x \in f^{-1}(J_1) + f^{-1}(J_2)$, alors $x = x_1 + x_2$ avec $f(x_1) \in J_1$ et $f(x_2) \in J_2$. On a donc $f(x) = f(x_1) + f(x_2) \in J_1 + J_2$ et donc $x \in f^{-1}(J_1 + J_2)$.
(vi) Soit $y \in f_*(I_1 \cap I_2)$, alors $y = \sum b_i y_i$ avec $b_i \in B$ et $y_i \in f(I_1 \cap I_2)$. On a donc $y_i \in f(I_1)$ et donc $y \in f_*(I_1)$ et de même $y_i \in f(I_2)$ et donc $y \in f_*(I_2)$.
Soit $x \in f^{-1}(J_1 \cap J_2)$, alors $f(x) \in J_1 \cap J_2$. On a donc $f(x) \in J_1$ c'est-à-dire $x \in f^{-1}(J_1)$ et de même $f(x) \in J_2$ c'est-à-dire $x \in f^{-1}(J_2)$.
Réciproquement soit $x \in f^{-1}(J_1) \cap f^{-1}(J_2)$, alors on a $f(x) \in J_1$ et $f(x) \in J_2$. On a donc $f(x) \in J_1 \cap J_2$, ainsi $x \in f^{-1}(J_1 \cap J_2)$.
(vii) Soit $y \in f_*(I_1 \cdot I_2)$, alors $y = \sum b_i y_i$ avec $b_i \in B$ et $y_i \in f(I_1 \cdot I_2)$ donc $y_i = f(\sum a_{i,j} c_{i,j})$ avec $a_{i,j} \in I_1$ et $c_{i,j} \in I_2$. On a donc $y = \sum_i \sum_j b_i f(a_{i,j}) f(c_{i,j})$. Mais $b_i f(a_{i,j}) \in f_*I_1$ et $f(c_{i,j}) \in f_*I_2$ donc $\sum_j b_i f(a_{i,j}) f(c_{i,j}) \in f_*I_1 \cdot f_*I_2$ et donc $y = \sum_i \sum_j b_i f(a_{i,j}) f(c_{i,j}) \in f_*I_1 \cdot f_*I_2$.
Soit $x \in f^{-1}(J_1) \cdot f^{-1}(J_2)$, alors $x = \sum a_i b_i$ avec $a_i \in f^{-1}(J_1)$ et $c_i \in f^{-1}(J_2)$. On a donc $f(x) = \sum f(a_i) f(c_i) \in J_1 \cdot J_2$.

(viii) Soit $y \in f_*(I_1 : I_2)$, alors $y = \sum_i b_i f(x_i)$ avec $b_i \in B$ et $x_i \in (I_1 : I_2)$ et soit $z \in f_* I_2$, on a $z = \sum_j c_j f(z_j)$ avec $c_j \in B$ et $z_j \in I_2$, on calcule alors $yz = \sum_i \sum_j b_i c_j f(x_i z_j)$ mais comme $x_i \in (I_1 : I_2)$ et $z_j \in I_2$, on a $x_i z_j \in I_1$ et donc $yz \in f_* I_1$. On a donc $y \in (f_* I_1 : f_* I_2)$.
Soit $x \in f^{-1}(J_1 : J_2)$, alors $f(x) \in (J_1 : J_2)$. Soit maintenant $z \in f^{-1}(J_2)$ c'est-à-dire $f(z) \in J_2$, on calcule $f(yz) = f(y)f(z) \in J_1$ donc $yz \in f^{-1}(J_1)$ et ainsi $y \in (f^{-1}(J_1) : f^{-1}(J_2))$.
(ix) Soit $y \in f_*(\sqrt{I})$, alors $y = \sum b_i f(x_i)$ avec $x_i \in \sqrt{I}$ c'est-à-dire qu'il existe $n_i \in \mathbb{N}$ tel que $x_i^{n_i} \in I$.

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 $k(X)$.

Solution. (i) Remarquons que $\varphi(U^2 + V^3) = (X^3)^2 + (X^2)^3 = X^6 - X^6 = 0$ donc on a $U^2 + V^3 \in \ker \varphi$. Soit $P \in \ker \varphi$, on effectue la division euclidienne de P par $U^2 + V^3$ ce qui est possible car le coefficient dominant en U de $U^2 + V^3$ est 1 donc inversible. On a donc $P(U, V) = (U^2 + V^3)Q(U, V) + R(U, V)$ avec R de degré 1 en U donc $R(U, V) = A(V)U + B(V)$ où A et B sont des polynômes en une variable. On a $0 = \varphi(P) = \varphi(R)$ donc $A(-X^2) + X^3 B(-X^2) = 0$ ce qui impose $2 \deg A = 2 \deg B + 3$. Ce n'est possible que si $\deg A = \deg B = -\infty$ et donc $A = B = 0$. On a donc $R = 0$ et $P \in (U^2 + V^3)$. On a $\ker \varphi = (U^2 + V^3)$.
(ii) Soit $k \geq 2$, montrons que $X^k \in \mathrm{Im}\varphi$. Si $k = 2p$ est par, on a

$$\varphi((-1)^p V^p) = (-1)^p (-X^2)^p = X^{2p}.$$

Si $k = 2p + 3$ est impair avec $p \geq 0$, on a

$$\varphi((-1)^p U V^p) = (-1)^p X^3 (-X^2)^p = X^{2p+3}.$$

Ainsi par combinaison linéaire, tout polynôme $P(X) = a_0 + \sum_{k=2}^{n} a_k X^k$ est dans $\mathrm{Im}\varphi$. Par ailleurs si $Q(U, V) \in k[U, V]$, on écrit $Q(U, V) = \sum_{i \geq 0, j \geq 0} \alpha_{i,j} U^i V^j$, on a alors

$$\varphi(Q) = \sum_{i \geq 0, j \geq 0} \alpha_{i,j} (-1)^j X^{3i+2j}.$$

On ne peut avoir $3i + 2j = 1$ avec $i \geq 0$ et $j \geq 0$ donc

$$\mathrm{Im}\varphi = \left\{ P(X) = a_0 + \sum_{k=2}^{n} a_k X^k \ / \ a_i \in k \right\}.$$

C'est un sous-anneau de $k[X]$ et est donc intègre.
(iii) Soit K le corps des fractions de A. Il est contenu dans $k(X)$ le corps des fractions de $k[X]$. Comme $k(X)$ est le plus petit corps contenant $k[X]$, il suffit de montrer que $k[X] \subset K$ et donc que $X \in K$. Cependant

$$X = \frac{X^3}{X^2} = -\frac{\varphi(U)}{\varphi(V)} \in K.$$

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 $\mathbb{R}^2$.

Solution. Considérons le morphisme de $\mathbb{R}$-algèbre $f : \mathbb{R}[X] \to \mathbb{C}$ défini par $f(1) = 1$ et $f(X) = j$ ($\mathbb{R}[X]$ est une $\mathbb{R}$-algèbre libre engendrée par 1 et X). Comme $\mathbb{C}$ est engendré comme $\mathbb{R}$ espace vectoriel (et donc comme $\mathbb{R}$-algèbre) par 1 et j, le morphisme f est surjectif. Il reste à déterminer son noyau. On a $\ker f = \{P \in \mathbb{R}[X] \ / \ P(j) = 0\}$. Remarquons que $1 + j + j^2 = 0$ donc $(1 + X + X^2) \subset \ker f$. Soit $P \in \ker f$, on effectue la division euclidienne de P par $1 + X + X^2$. On a $P = (1 + X + X^2)Q + R$ où R est un polynôme de degré 1. On écrit $R(X) = aX + b$ avec a et b des réels. Comme $P(j) = 0$, on a $R(j) = 0$. On a donc $aj + b = \frac{a}{2} + b + \frac{a}{2} i = 0$. Ceci impose que $a = b = 0$ donc $R = 0$. Ainsi si $\ker f \subset (1 + X + X^2)$ et donc $\ker f = (1 + X + X^2)$ d'où l'isomorphisme recherché.
Considérons le morphisme de $\mathbb{R}$-algèbre $f : \mathbb{R}[X] \to \mathbb{R}^2$ défini par $f(1) = (1, 1)$ et $f(X) = (-1, 0)$ ($\mathbb{R}[X]$ est une $\mathbb{R}$-algèbre libre engendrée par 1 et X). Comme $\mathbb{R}$ est engendré comme $\mathbb{R}$ espace vectoriel (et donc comme $\mathbb{R}$-algèbre) par $(1, 1)$ et $(-1, 0)$, le morphisme f est surjectif. Il reste à déterminer son noyau. On a $\ker f = \{P = \sum_i a_i X^i \in \mathbb{R}[X] \ / \ \sum_i a_i (-1, 0)^i = 0\}$ (par convention $(a, b)^0 = (1, 1)$. On commence par remarquer que $X(X + 1) \in \ker f$. En effet, on a $f(X(X + 1)) = (-1, 0)((-1, 0) + (1, 1)) = (-1, 0)(0, 1) = (0, 0)$.

Soit maintenant $P \in \ker f$, on effectue la division euclidienne de P par $X(X+1)$. On a $P = X(X+1)Q + R$ où R est un polynôme de degré 1. On écrit $R(X) = aX + b$ avec a et b des réels. Comme $P((-1,0)) = 0$, on a $R((-1,0)) = 0$. On a donc $a(-1,0) + b(1,1) = (b-a,b) = (0,0)$. Ceci impose que $a = b = 0$ donc $R = 0$. Ainsi si $\ker f \subset (X(X+1))$ et donc $\ker f = (X(X+1))$ d'où l'isomorphisme recherché.

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.

Solution. Il s'agit de montrer que pour tout $x \in A$ et $y \in A$, on a

$$F(x+y) = F(x) + F(y) \quad \text{et} \quad F(xy) = F(x)F(y).$$

La seconde est évidente car $(xy)^p = x^p y^p$. Pour la première, on doit montrer que

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p.$$

Comme la caractéristique est $p > 0$, il suffit de montrer que $\binom{p}{k}$ est divisible par p si $0 < k < p$. On écrit

$$p! = k!(p-k)!\binom{p}{k},$$

de sorte que p divise le terme de droite. Cependant comme $k < p$ et $p - k < p$ et que p est premier, p ne divise pas $k!(p-k)!$. Il divise donc $\binom{p}{k}$.

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 $\mathfrak{p} \in \mathrm{Spec}(A) = \{\mathfrak{p} \ / \ \mathfrak{p} \text{ est un idéal premier}\}$.
Montrer que $A/\mathfrak{p}$ est de dimension finie sur k.

c) Montrer que $\mathfrak{p}$ est un idéal maximal.
Soient $\mathfrak{p}_i \in \mathrm{Spec}(A), i = 1, \cdots, n$ des idéaux distincts.

d) Montrer que la flèche

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

est surjective. En déduire l'inégalité $n \leq \dim_k(A)$.
On suppose dorénavant A réduite (c'est-à-dire nil(A) = 0).

e) Montrer que la flèche

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

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.

Solution. (1) Soit $a \in A$ un élément non nul. Il faut montrer que a est inversible. Considérons alors l'application A-linéaire (et donc k-linéaire) :

$$\mu_a : A \to A$$

$$x \mapsto ax.$$

Son noyau est formé des $x \in A$ tels que $ax = 0$ mais comme A est intègre et $a \neq 0$, on a $x = 0$. Ainsi μ_a est injective et comme A est un k-espace vectoriel de dimension finie, elle est aussi surjective. Il existe donc $b \in A$ tel que $\mu_a(b) = 1_A$ c'est-à-dire $ab = 1_A$ et donc a est inversible d'inverse b.

(ii) Soit $\mathfrak{p} \in \mathrm{Spec}(A) = \{\mathfrak{p} \ / \ \mathfrak{p} \text{ est un idéal premier}\}$.
(ii).a. On a une application A-linéaire (et donc k-linéaire) surjective $A \to A/\mathfrak{p}$. Ainsi comme A est de dimension finie sur k, c'est aussi le cas de $A/\mathfrak{p}$.
(ii).b. La k-algèbre $A/\mathfrak{p}$ est de dimension finie et intègre (car $\mathfrak{p}$ est un idéal premier). On peut donc appliquer le **1.** pour dire que $A/\mathfrak{p}$ est un corps. Ainsi $\mathfrak{p}$ est maximal.
Soient $\mathfrak{p}_i \in \mathrm{Spec}(A), i = 1, \cdots, n$ des idéaux distincts.
(ii).c. On a vu au (ii).b que les $\mathfrak{p}_i$ sont maximaux, ainsi si $\mathfrak{p}_i \neq \mathfrak{p}_j$, alors $\mathfrak{p}_i + \mathfrak{p}_j$ est un idéal contenant strictement $\mathfrak{p}_i$ et par maximalité, on a $\mathfrak{p}_i + \mathfrak{p}_j = A$. On peut donc appliquer le lemme chinois aux $\mathfrak{p}_i$. Et on a

$$A/(\mathfrak{p}_1 \cdots \mathfrak{p}_n) \simeq \bigoplus_{i=1}^{n} A/\mathfrak{p}_i.$$

Ainsi l'application

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

s'identifie à

$$A \to A/(\mathfrak{p}_1 \cdots \mathfrak{p}_n)$$

qui est évidement surjective.
Comme les $\mathfrak{p}_i$ sont premiers, on a $A/\mathfrak{p}_i \neq 0$ donc $\dim_k(A/\mathfrak{p}_i) \geq 1$. On voit alors que

$$\dim_k(A) \geq \dim_k \left(\bigoplus_{i=1}^{n} A/\mathfrak{p}_i \right) \geq n.$$

(ii).d D'après ce qui précède, on a nécessairement $\mathrm{card}(\mathrm{Spec}(A)) \leq \dim_k(A)$, c'est-à-dire qu'on a un nombre fini d'idéaux premiers. On peut donc reprendre le raisonnement précedent avec tous les idéaux premiers et on a

$$A/(\prod_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}) \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}.$$

Cependant, on a évidement que

$$\prod_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \subset \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathrm{Nil}(A)$$

et ce dernier idéal est nul car A est réduite. Ainsi, on a l'isomorphisme

$$A \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}.$$

(iii) Considérons l'algèbre $A = \mathbb{R}[X]/((X^2 + a)X(X + 1))$ avec $a \in \mathbb{R}$.
(iii).a On a ici un anneau factoriel $\mathbb{R}[X]$, ainsi le quotient $A = \mathbb{R}[X]/((X^2 + a)X(X + 1))$ est réduit si et seulement si l'élément $(X^2 + a)X(X + 1)$ n'a pas de facteur carré. Il y a alors quatre cas à distinguer :
1. Si $a > 0$, alors $X^2 + a$ est irréductible sur $\mathbb{R}$, il n'y a pas de facteur carré et A est réduite.
2. Si $a = 0$, alors il y a un facteur carré (et même cube) : X^3 et A n'est pas réduite.
3. Si $a = -1$, alors $X^2 + a = (X - 1)(X + 1)$ et $(X + 1)^2$ est un facteur carré, A n'est pas réduite.
4. Si $a < 0$ et $a \neq -1$, alors $X^2 + a = (X + \sqrt{-a})(X - \sqrt{-a})$ et il n'y a pas de facteur carré, A est réduite.
(iii).b Notons $\overline{P}$ la classe d'un polynôme $P \in \mathbb{R}[X]$ dans A. L'isomorphisme précedent est alors donné dans le cas 4. par

$$A \simeq \mathbb{R}[X]/(X - a) \oplus \mathbb{R}[X]/(X + a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X + 1) \simeq \mathbb{R}^4$$
$$\overline{P} \mapsto (P(a), P(-a), P(0), P(1)).$$

Dans le cas 1. il est donné par

$$A \simeq \mathbb{R}[X]/(X^2 + a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X + 1) \simeq \mathbb{C} \oplus \mathbb{R}^2$$
$$\overline{P} \mapsto (\alpha X + \beta, P(0), P(1)) \mapsto (P(\sqrt{-a}), P(0), P(1))$$

avec

$$\sqrt{-a} = i\sqrt{a}, \quad \alpha = \frac{P(\sqrt{-a}) - P(-\sqrt{-a})}{2\sqrt{-a}} \quad \text{et} \quad \beta = \frac{P(\sqrt{-a}) + P(-\sqrt{-a})}{2}.$$

Dans le cas 4, le morphisme se factorise par $\mathbb{R}[X]/(X^2 + a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X + 1)$ et la seconde formule est encore valable ce qui donne une formule valable dans tous les cas.

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 $M[X]$.

Solution. Considérons le morphisme de A-module

$$f : M^{\mathbb{N}} \to M[X]$$

$$(m_i)_{i\in\mathbb{N}} \mapsto \sum_{i=0}^{+\infty} m_i X^i.$$

La somme de droite est finie car le terme$(m_i)_{i\in\mathbb{N}}$ est dans une somme directe donc seul un nombre fini de termes est non nul. On montre que f est un isomorphisme. En effet, si $f((m_i)_{i\in\mathbb{N}}) = 0$, alors pour tout $i \in \mathbb{N}$, on a $m_i = 0$, donc f est injective. Par ailleurs si $P = \sum_{i=0}^{N} n_i X^i$ avec $n_i \in M$, alors posons $m_i = n_i$ pour $1 \leq i \leq N$ et $m_i = 0$ pour $i > N$, on a $f((m_i)_{i\in\mathbb{N}}) = P$ et f est surjective.

Exercice 52. Soit A et B deux anneaux et $f : A \longrightarrow B$ un homomorphisme d'anneaux.
(ı) 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.
(ıı) 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).
(ıı) 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 ?

Solution. (ı) On a les égalités

$$1 \cdot b = f(1)b = b$$

$$(a + a') \cdot b = f(a + a')b = (f(a) + f(a'))b = f(a)b + f(a')b = a \cdot b + a' \cdot b$$
$$(aa') \cdot b = f(aa')b = (f(a)f(a'))b = f(a)(a' \cdot b) = a \cdot (a' \cdot b)$$

qui prouvent que cette loi muni B d'une structure de A-module.
(ıı) Le noyau de f est un idéal de A. Comme A est un corps, les seuls idéaux de A sont (0) ou A. Mais comme $f(1_A) = 1_B \neq 0$, on a $1_A \notin \ker f$ et donc $\ker f = (0)$.
(ıı) Soit N un B-module, la loi $a \cdot n = f(a)n$ munit N d'une structure de A-module(on garde la même addition). Soit maintenant $x \in (0_A : N) = \mathrm{Ann}_A(N)$. On a

$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ \forall n \in N,\ x \cdot n = 0$$

$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ \forall n \in N,\ f(x)n = 0$$

$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ f(x) \in \mathrm{Ann}_B(N)$$

$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ x \in f^{-1}(\mathrm{Ann}_B(N)).$$

L'annulateur de N vu comme A-moduleest l'image réciproque par f de l'annulateur de N vu comme B-module : $\mathrm{Ann}_A(N) = f^{-1}(\mathrm{Ann}_B(N))$.

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 ${}^t({}^tf)\circ\theta = \theta\circ f$.

d) Montrer que si M est réflexif, on a $I(f) = I({}^tf)$.

Solution. (i) Considérons le morphisme de A-modules $\psi : A[X] \to \mathrm{End}_A M$ défini par $\psi(P) = P(f)$. On a $I(f) = \ker\psi$ donc c'est un idéal.
(ii) Soit $P \in I(f)$ On a alors $P(f) = 0$. On calcule alors $P({}^tf)(\varphi)$ pour $\varphi \in M^\vee$. On a $P({}^tf)(\varphi) = \varphi\circ P(f) = 0$ car $P \in I(f)$. On a donc $P({}^tf) = 0$ donc $P \in I({}^tf)$. On a bien $I(f) \subset I({}^tf)$.
(iii) On a

$$\big({}^t({}^tf)\circ\theta\big)(m) = {}^t({}^tf)(\theta(m)) = \theta(m)\circ {}^tf$$

et pour $\varphi \in M^\vee$, on a

$$\Big(\big({}^t({}^tf)\circ\theta\big)(m)\Big)(\varphi) = (\theta(m)\circ {}^tf)(\varphi) = (\theta(m))(\varphi\circ f) = \varphi(f(m)).$$

Par ailleurs, on a

$$(\theta\circ f)(m) = \theta(f(m))$$

et pour $\varphi \in M^\vee$, on a

$$\big((\theta\circ f)(m)\big)(\varphi) = \big(\theta(f(m))\big)(\varphi) = \varphi(f(m)),$$

ce qui prouve l'égalité ${}^t({}^tf)\circ\theta = \theta\circ f$.
(iv) Si M est réflexif on a donc ${}^t({}^tf) = \theta\circ f\circ\theta^{-1}$. Soit $P \in I({}^tf)$. On a alors $P \in I({}^t({}^tf))$, ainsi $P(\theta\circ f\circ\theta^{-1}) = P({}^t({}^tf)) = 0$ c'est-à-dire $\theta\circ P(f)\circ\theta^{-1} = 0$. Comme θ est inversible, ceci impose que $P(f) = 0$ donc $P \in I(f)$.

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 ?

Solution. (i) Soit m un générateur de M et considérons le morphisme de A-module$f : A \to M,\ a \mapsto am$. Il est surjectif (car m engendre M) et son noyau est un idéal I de A. Le morphisme $\overline{f} : A/I \to M$ est donc un isomorphisme.
(ii) Soit $m \in M$ un élément non nul et soit N le sous-module de M engendré par m. Comme $0 \neq m \in N$, le sous-module N est non nul, c'est donc M tout entier. L'élément m engendre donc M.
D'après la question précédente, on sait qu'il existe un idéal $\mathfrak{m}$ tel que $M \simeq A/\mathfrak{m}$. Il reste à vérifier que cet idéal est maximal. Soit donc I un idéal contenant strictement $\mathfrak{m}$, alors on a la suite exacte

$$0 \to I/\mathfrak{m} \to M \simeq A/\mathfrak{m} \to A/I \to 0.$$

Le module $I/\mathfrak{m}$ est donc un sous-module strict de M, il doit être nul c'est-à-dire $I = \mathfrak{m}$ donc $\mathfrak{m}$ est maximal.
(iii) D'après la question précédente, les modules simples de $\mathbb{Z}$ sont de la forme $\mathbb{Z}/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal. Il reste à déterminer les idéaux maximaux de $\mathbb{Z}$. Comme $\mathbb{Z}$ est principal, on a $\mathfrak{m} = (n)$ avec $n \in \mathbb{Z}$. L'idéal, (n) est maximal si et seulement si $\mathbb{Z}/(n)$ est un corps, c'est le cas si et seulement si n est premier. Les $\mathbb{Z}$ modules simples sont les $\mathbb{Z}/(p)$ avec p un nombre premier.

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 $f(T(M)) \subset T(N)$.

Solution. (i) Il faut montrer que $T(M)$ est non vide et stable par addition et multiplication par un scalaire.
Il est clair que $0 \in T(M)$ car $(0 : 0) = \mathrm{Ann}(0) = M$.
Soit maintenant m et m' dans $TM)$, a et a' dans A et x et x' dans $M - \{0\}$ tels que $xm = 0$ et $x'm' = 0$. Alors on a $(xx')(ax + a'm') = ax'(xm) + ax(x'm') = 0$ et $xx' \neq 0$ car A est intègre. Ainsi $T(M)$ est stable par addition et multiplication par un scalaire.
$T(M)$ est donc un sous-module de M.
(ii) Soient $Cl(m) \in M/T(M)$ et $a \in A - \{0\}$ tels que $a\cdot Cl(m) = 0$. Ceci signifie que $am \in T(M)$. Il existe donc $x \in A - \{0\}$ tel que $x(am) = 0$ et donc $(xa)m = 0$. Comme $a \in A - \{0\}$ et $x \in A - \{0\}$ on a $xa \in A - \{0\}$ (A

intègre) et donc $m \in T(M)$. On a donc $Cl(m) = 0$ ce qui signifie que le seul élément de torsion de $M/T(M)$ est 0, le module $M/T(M)$ est donc sans torsion.
(iii) Soit $m \in T(M)$ et $x \in A - \{0\}$ tels que $xm = 0$. On considère alors $f(m)$ et on a $af(m) = f(am) = f(0) = 0$. L'élément $f(m)$ est donc de torsion d'où l'inclusion $f(T(M)) \subset T(N)$.

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 $M = Am \oplus \ker f$.

Solution. Soit N un facteur direct de Am de sorte que $M = Am \oplus N$. Comme $\mathrm{Ann}(m) = (0)$, l'homomorphisme $A \to Am,\ a \mapsto am$ est un isomorphisme. On peut alors définir une forme linéaire f sur M par $f(am, n) = a$. On a bien $f(m) = 1$.
Réciproquement, s'il existe un tel f, le noyau de f est un sous-module N de M. De plus, si $am \in Am \cap N$, alors $f(am) = a = 0$ donc $Am \cap N = 0$. Enfin, si $m' \in M$, on écrit $m' = f(m')m + (m' - f(m')m)$. On a $f(m')m \in Am$ et $f(m' - f(m')m) = 0$ donc $m' - f(m')m \in N$ ce qui prouve que $Am \oplus N = M$.

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) $M_\alpha = (0 : I_\alpha) = J_\alpha \cdot M = \bigcap_{\beta\neq\alpha} N_\beta$.

Solution. (i) Fixons α, si $\beta \neq \alpha$, les idéaux I_α et I_β sont comaximaux. On peut donc écrire $1 = x_\beta + y_\beta$ avec $x_b \in I_\alpha$ et $y_\beta \in I_\beta$. On a alors

$$1 = \prod_{\beta\neq\alpha} (x_\beta + y_\beta).$$

On voit alors que 1 est somme d'éléments de I_α (touts les termes multiples d'un x_β) et de $\prod_{\beta\neq\alpha} y_\beta \in \prod_{\beta\neq\alpha} I_\beta \subset J_\alpha$.
(ii) Un élément $a \in A$ est dans $(0 : N_\alpha)$ si pour tout $n \in N_\alpha$ on a $an = 0$ c'est-à-dire pour tout $\beta \neq \alpha$ et pour tout $m \in M_\beta$, on a $am = 0$. Ainsi $(0 : N_\alpha)$ est l'intersection des $\mathrm{Ann}(M_\beta)$ pour $\beta \neq \alpha$ et donc $J_\alpha = (0 : N_\alpha)$.
(iii) Un élément $\sum m_\beta \in M$ avec $m_\beta \in M_\beta$ est dans $(0 : J_\alpha)$ si et seulement si $J_\alpha \cdot (\sum m_\beta) = 0$ c'est-à-dire pour tout β, on a $J_\alpha \cdot m_\beta = 0$. Si $\alpha \neq \beta$, l'inclusion $J_\alpha \subset I_\beta$ montre que tout $m_\beta \in M_\beta$ convient. Pour $\beta = \alpha$, l'égalité $I_\alpha + J_\alpha = A$ implique $I_\alpha m_\alpha + 0 = Am_\alpha$ et comme I_α annule M_α ceci impose $Am_\alpha = 0$ donc $m_\alpha = 0$. Ainsi $(0 : J_\alpha) = \oplus_{\beta\neq\alpha} M_\beta = N_\alpha$.
Pour $\beta \neq \alpha$, on a $A = I_\alpha + I_\beta$ donc $M_\beta = (I_\alpha + I_\beta)M_\beta = I_\alpha M_\beta$ et pour $\beta = \alpha$, on a $I_\alpha M_\alpha = 0$. Ainsi

$$I_\alpha M = \bigoplus_\beta I_\alpha M_\beta = \bigoplus_{\beta\neq\alpha} M_\beta = N_\alpha.$$

(iv) Un élément $\sum m_\beta \in M$ avec $m_\beta \in M_\beta$ est dans $(0 : I_\alpha)$ si et seulement si $I_\alpha \cdot (\sum m_\beta) = 0$ c'est-à-dire pour tout β, on a $I_\alpha \cdot m_\beta = 0$. Si $\alpha = \beta$, on a $I_\alpha = \mathrm{Ann}(M_\alpha)$ donc tout $m_\alpha \in M_\alpha$ convient. Pour $\beta \neq \alpha$, l'égalité $I_\alpha + I_\beta = A$ implique $0 + I_\beta m_\beta = Am_\beta$ et comme I_β annule M_β ceci impose $Am_\beta = 0$ donc $m_\beta = 0$. Ainsi $(0 : I_\alpha) = M_\alpha$.
On a $J_\alpha M = \oplus_\beta J_\alpha M_\beta = J_\alpha M_\alpha$ car $J_\alpha \subset I_\beta$ pour $\beta \neq \alpha$. On a par ailleurs $J_\alpha + I_\alpha = A$ donc $M_\alpha = J_\alpha M_\alpha + I_\alpha M_\alpha = J_\alpha M_\alpha$. On a donc $J_\alpha M = M_\alpha = \bigcap_{\beta\neq\alpha} N_\beta$.