U2LG35 L3 Algèbre 2014-2015 **Université Paris-Diderot**

Feuille d'exercices numéro 5

On rappelle que $(\mathscr{A}, +, 0, \times, 1)$ est un « anneau unitaire » si $(\mathscr{A}, +, 0)$ est un groupe et si $\times$ est associatif, admet 1 pour élément neutre bilatéral et est distributif sur $+$ (des deux cotés). L'élément 0 n'est pas nécessairement distinct de 1. Un tel anneau sera noté simplement $\mathscr{A}$. On dit que $\mathscr{A}$ est « commutatif » si $\times$ est commutatif. Un « morphisme » d'anneaux unitaires préserve l'addition, la multiplication et l'unité. Un élément est « inversible » s'il divise 1. Un élément x de $\mathscr{A}$ est dit « premier » ou « irréductible » s'il n'est ni inversible et le produit de deux non inversibles. On dit que deux éléments x et y de $\mathscr{A}$ sont « équivalents » si l'un est le produit de l'autre par un élément inversible de $\mathscr{A}$ (il est immédiat que c'est une relation d'équivalence). Deux décompositions d'un élément x de $\mathscr{A}$ en produits de facteurs sont dites « équivalentes » si elles sont identiques à l'ordre près et à équivalence près des facteurs.

☞ **Exercice 1.** *Soit $\mathscr{A}$ un anneau unitaire.*

(a) Montrer que pour tout $x \in \mathscr{A}$, $0x = x0 = 0$.

(b) Montrer que pour tout $x \in \mathscr{A}$, $-x = (-1)x = x(-1)$.

(c) Montrer que l'addition de $\mathscr{A}$ est commutative.

(d) Montrer que $(-1)^2 = 1$.

☞ **Exercice 2.** *Soit $\mathscr{A}$ un anneau unitaire.*

(a) Montrer qu'il existe un unique morphisme d'anneaux unitaires $\mathbb{Z} \to \mathscr{A}$.

L'image de $n \in \mathbb{Z}$ par ce morphisme sera encore notée n, ceci quel que soit l'anneau $\mathscr{A}$. Pour éviter toute confusion, on pourra dire que cet $n \in \mathscr{A}$ est « la valeur de l'entier n dans $\mathscr{A}$ ».

(b) Soit $\varphi : \mathscr{A} \to \mathbb{Z}$ un morphisme d'anneaux unitaires. Montrer que pour tout entier non nul n, la valeur de n dans $\mathscr{A}$ n'est pas 0

☞ **Exercice 3.** *Soit $\mathscr{A}$ un anneau unitaire tel que $x^2 = x$ pour tout $x \in \mathscr{A}$. Un tel anneau est dit « booléen ».*

(a) Montrer que $x = -x$ pour tout $x \in \mathscr{A}$.

(b) Montrer que $\mathscr{A}$ est commutatif.

L'égalité $x = xy$ sera notée $x \leq y$.

(c) Montrer que $\leq$ est une relation d'ordre sur $\mathscr{A}$.

(d) Montrer que $\mathscr{A}$ a un plus petit et un plus grand élément.

On suppose désormais que $\mathscr{A}$ est fini.

(e) Montrer que toute partie de $\mathscr{A}$ a une borne supérieure, qu'on notera $\sup(A)$.

☞ **Exercice 4.** *Un élément x d'un anneau $\mathscr{A}$ est dit « nilpotent » s'il existe $n \in \mathbb{N}$ tel que $x^n = 0$.*

(a) Soit $\mathscr{A}$ un anneau unitaire. Montrer que si $x \in \mathscr{A}$ est nilpotent, alors $1 - x$ est inversible.

☞ **Exercice 5.** *Soit $n \in \mathbb{N}^*$. On note $\phi(n)$ le nombre d'entiers k tels que $1 \leq k \leq n$ qui sont premiers à n.*

(a) Montrer que le cardinal du groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est $\phi(n)$.

(b) Montrer que si n et m sont premiers entre eux, on a $\phi(nm) = \phi(n)\phi(m)$.

(c) Montrer que si p est premier et $k \in \mathbb{N}$, on a $\phi(p^k) = (p-1)p^{k-1}$.

(d) Montrer que pour tout $n \in \mathbb{N}^*$, on a $\phi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$, où le produit est étendu a l'ensemble $\{p_i\}$ des facteurs premiers de n.

(e) Montrer que $\phi : \mathbb{N}^* \to \mathbb{N}^*$ est une fonction croissante pour l'ordre de la divisibilité.

☞ **Exercice 6.** **(a)** Montrer que l'ensemble $\mathbb{Z}[\sqrt{-5}]$ des nombres complexes de la forme $a + ib\sqrt{5}$ tels que $a, b \in \mathbb{Z}$ est un sous-anneau de $\mathbb{C}$.

Pour tout $x \in \mathbb{Z}[\sqrt{-5}]$, on pose $N(x) = x\overline{x}$.

(b) Montrer que $N(x) \in \mathbb{N}$ et que $N(xy) = N(x)N(y)$, pour tous x et y de $\mathbb{Z}[\sqrt{-5}]$.

(c) Déterminer tous les éléments inversibles de $\mathbb{Z}[\sqrt{-5}]$ (utiliser N).

(d) Montrer que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont premiers dans $\mathbb{Z}[\sqrt{-5}]$.

(e) Montrer que 6 a deux décompositions non équivalentes en facteurs premiers dans $\mathbb{Z}[\sqrt{-5}]$.

☞ **Exercice 7.** *Soit $\mathscr{A}$ un anneau unitaire commutatif et a un élément non inversible de $\mathscr{A}$ qui est divisible par tous les non inversibles non nuls de $\mathscr{A}$.*

(a) Montrer que pour tout $x \in \mathscr{A}$, $1 + ax$ est inversible.

(b) Donner un exemple de cette situation dans lequel a n'est pas nul.

☞ **Exercice 8.** *Soit $\mathscr{A}$ un anneau unitaire commutatif. Un « idempotent » de $\mathscr{A}$ est un élément e de $\mathscr{A}$ tel que $e^2 = e$.*

(a) Soit e un idempotent de $\mathscr{A}$. Montrer que $e\mathscr{A} = \{ex \mid x \in \mathscr{A}\}$ est un anneau unitaire pour l'addition et la multiplication induites par $\mathscr{A}$, et que $x \mapsto ex$ est un morphisme d'anneaux unitaires $\mathscr{A} \to e\mathscr{A}$. Quelle est l'unité de $e\mathscr{A}$?

(b) On suppose que $1 = e + e'$ où e et e' sont deux idempotents. calculer ee' et montrer que $\mathscr{A}$ est isomorphe à l'anneau produit $e\mathscr{A} \times e'\mathscr{A}$.

☞ **Exercice 9.** *Soit G un groupe noté additivement mais a priori non abélien, et $\mathscr{A}$ un anneau unitaire. On note $\mathscr{A}[G]$ l'ensemble des polynômes en X à coefficients dans $\mathscr{A}$ et à exposants dans G.*

(a) Montrer que $\mathscr{A}[G]$ est un anneau unitaire pour les opérations usuelles sur les polynômes.

(b) Montrer que l'application $\varepsilon : \mathscr{A}[G] \to \mathscr{A}$ définie par $\varepsilon(a_{g_1}X^{g_1} + \cdots + a_{g_k}X^{g_k}) = a_{g_1} + \cdots + a_{g_k}$ est un morphisme d'anneaux unitaires.

On note $\mathscr{I}$ le noyau de ε, et $\mathscr{I}^2$ l'ensemble des sommes finies de produits de deux éléments de $\mathscr{I}$.

(c) Montrer que tout élément x de $\mathscr{I}$ s'écrit de manière unique comme une combinaison linéaire à coefficients dans $\mathscr{A}$ des polynômes $1 - X^g$ tels que $g \neq 0$.

(d) Montrer que l'application $\varphi : G \to \mathscr{I}/\mathscr{I}^2$ définie par $g \mapsto \overline{1 - X^g}$ est un morphisme de groupe (où le surlignement représente la classe d'équivalence modulo $\mathscr{I}^2$).

On suppose maintenant que $\mathscr{A} = \mathbb{Z}$.

(e) Montrer que φ est surjectif et que son noyau est le sous-groupe $[G, G]$ des commutateurs de G, c'est-à-dire le plus petit sous-groupe distingué de G contenant tous les éléments de la forme $g + h - g - h$.

Solutions des exercices de la feuille 5

☞ **Exercice 1.** **(a)** On a $0+0=0$ car 0 est neutre pour $+$, donc $(0+0)x=0x$, d'où $0x+0x=0x$ par distributivité et enfin $0x=0$ puisque dans un groupe tout élément est régulier.

(b) On a $0=0x=(1+(-1))x=x+(-1)x$ d'où $(-1)x=-x$.

(c) Il suffit de montrer que $x+y-x-y=0$. On a $x+y-x-y=x+y+(-1)x+(-1)y=(x+y)+(-1)(x+y)=(1+(-1))(x+y)=0$.

(d) On a $(-1)^2=(-1)(-1)=-(-1)=1$ (opposé de l'opposé de 1).

☞ **Exercice 2.** **(a)** On sait qu'étant donné un élément a dans un groupe G, il existe un unique morphisme de groupes $f:\mathbb{Z}\to G$ tel que $f(1)=a$ ($\mathbb{Z}$ est un groupe libre sur un générateur). Comme un morphisme d'anneaux doit envoyer 1 sur 1, il reste juste à vérifier que l'application ainsi obtenue préserve la multiplication. Elle préserve clairement la multiplication par 0 et par 1. Pour la multiplication par les entiers positifs, on peut raisonner par récurrence. On a alors $f((n+1)x)=f(nx+x)=nf(x)+f(x)=(n+1)f(x)$. Enfin, on a (pour $n\geq 0$) $f((n+(-n))x)=nf(x)+f((-n)x)$, donc $f((-n)x)=-nf(x)$.

(b) Pour tout entier $n\in\mathbb{Z}$, notons $\overline{n}$ la valeur de n dans $\mathscr{A}$. Notons $\psi:\mathbb{Z}\to\mathbb{Z}$ le morphisme d'anneaux unitaires $n\mapsto\varphi(\overline{n})$. Ce morphisme ne peut être que l'identité de $\mathbb{Z}$ d'après la question précédente. On a donc $\varphi(\overline{n})=n$ pour tout entier n. Si $n\neq 0$, on a alors nécessairement $\overline{n}\neq 0$, car $\varphi(0)=0$.

☞ **Exercice 3.** **(a)** On a $x+x=(x+x)^2=x^2+xx+xx+x^2=x+x+x+x$, donc $x+x=0$, puis $x=-x$.

(b) On a $x+y=(x+y)^2=x+xy+yx+y$, donc $xy+yx=0$, d'où $xy=-(yx)=yx$.

(c) On a $x=xx$ donc $x\leq x$. Si $x=xy$ et $y=yz$, on a $x=x(yz)=(xy)z=xz$ ce qui montre que $\leq$ est transitive. Enfin, si $x=xy$ et $y=yx$, on a $x=xy=yx=y$.

(d) On a $0=0x$ pour tout x, donc 0 est le plus petit élément de $\mathscr{A}$. De même, on a $x=x1$ pour tout x, donc 1 est le plus grand élément de $\mathscr{A}$.

(e) Il suffit de prendre pour $\sup(A)$ le produit de tous les majorants de A. En effet, cet élément est un majorant de A, car si $a\leq x$ et $a\leq y$, autrement-dit si $a=ax$ et $a=ay$, alors $a=a^2xy=axy$, c'est-à-dire $a\leq xy$. Par ailleurs, cet élément est clairement le plus petit majorant de A.

☞ **Exercice 4.** **(a)** On a en effet $(1-x)(1+x+x^2+\cdots+x^{n-1})=1-x^n=1$ dès que n est assez grand.

☞ **Exercice 5.** **(a)** Pour tout entier $k\in\mathbb{Z}$, notons $\overline{k}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$. Dire que $\overline{k}$ est inversible est dire qu'il existe un entier a tel que $\overline{k}\overline{a}=\overline{1}$, autrement-dit que $ka=1$ modulo n, ou encore qu'il existe a et b tels que $ka+bn=1$. Ceci revient à dire, d'après le théorème de Bézout que k est premier à n. Comme les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ ont un unique représentant dans l'intervalle $[1,n]$ de $\mathbb{Z}$, on a le résultat annoncé.

(b) Si n et m sont premiers entre eux, on a un isomorphisme de groupes (additifs) $f:\mathbb{Z}/nm\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. L'élément $(1,1)$ est un générateur de $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. En effet, il est d'ordre nm, car si $k(1,1)=0$, on a $(k,k)=(0,0)$, c'est-à-dire $n|k$ et $m|k$. Comme n et m sont premiers entre eux, $nm|k$ et $(1,1)$ est donc d'ordre nm. Un isomorphisme de groupes est donc donné par $x\mapsto(x,x)$. Il est immédiat qu'il préserve la multiplication et qu'il préserve l'unité. C'est donc un morphisme d'anneaux unitaires (d'ailleurs le seul). Par ailleurs, un couple (x,y) de $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ est inversible si et seulement si il existe un couple (a,b) tel que $(x,y)(a,b)=(1,1)$ autrement-dit si et seulement si x et y sont tous deux inversibles. On a donc $\phi(nm)=\phi(n)\phi(m)$.

(c) Les entiers de l'intervalle $[1,p^k]$ qui sont divisibles par p sont $p,2p,\ldots,p^{k-1}p$. Il sont au nombre de p^{k-1}. On a donc $\phi(p^k)=p^k-p^{k-1}=(p-1)p^{k-1}$.

(d) Soit $n=\prod_i p_i^{k_i}$ la décomposition de n en facteurs premiers. D'après la question **(b)**, on a $\phi(n)=\prod_i\phi(p_i^{k_i})=\prod_i(p_i-1)p_i^{k_i-1}=\prod_i\left(1-\frac{1}{p_i}\right)p_i^{k_i}=n\prod_i\left(1-\frac{1}{p_i}\right)$.

(e) Si $n|m$, tous les facteurs premiers p_i de n (avec exposants k_i) figurent parmi les facteurs premiers q_j de m

avec des exposants k'_j supérieurs ou égaux. On voit donc que $n = \prod_i (p_i - 1) p_i^{k_i - 1}$ divise $m = \prod_j (q_j - 1) q_j^{k'_j - 1}$.

☞ **Exercice 6.** **(a)** $\mathbb{Z}[\sqrt{-5}]$ contient 0 et 1 et est stable par addition, opposé et multiplication.

(b) On a $N(a+ib\sqrt{5}) = (a+ib\sqrt{5})(a-ib\sqrt{5}) = a^2+5b^2 \in \mathbb{N}$, et bien sûr $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$.

(c) Si x est inversible, il existe y tel que $xy = 1$. On a alors $N(x)N(y) = N(1) = 1$. Comme $N(x)$ et $N(y)$ sont des entiers naturels, ceci entraîne que $N(x) = 1$. Or $a^2 + 5b^2 = 1$ ne peut être réalisé que pour $a = \pm 1$ et $b = 0$. Ainsi, 1 et -1 sont les seuls éléments inversibles de $\mathbb{Z}[\sqrt{-5}]$.

(d) 2 n'est pas inversible et si on a $2 = xy$, on a $N(2) = 4 = N(x)N(y)$. Comme il n'existe aucun x tel que $N(x) = 2$, on doit avoir $N(x) = 1$ ou $N(y) = 1$ et donc l'un des deux est inversible. Le même raisonnement s'applique pour 3, puisque $N(3) = 9$ et qu'il n'existe aucun x tel que $N(x) = 3$. De même pour $1 \pm i\sqrt{5}$, puisque $N(1 \pm i\sqrt{5}) = 6$ et qu'il n'existe pas de x tel que $N(x) = 2$ ou $N(x) = 3$.

(e) On a les deux décompositions en facteurs premiers $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ qui sont clairement non équivalentes puisque les deux seuls inversibles sont 1 et -1.

☞ **Exercice 7.** **(a)** Posons $b = 1 + ax$. Alors b n'est pas nul, car sinon a serait inversible. Supposons b non inversible. Comme il n'est pas nul, il divise a, donc il divise ax, donc il divise $b - ax = 1$. Or, tout diviseur de 1 est inversible par définition.

(b) Il suffit de prendre $\mathscr{A} = \mathbb{Z}/4\mathbb{Z}$ et $a = 2$. a est non nul et non inversible et il est divisible par 2 qui est le seul non inversible non nul. Ainsi $1 + 2x$ est inversible pour tout x, et en effet, il s'agit des éléments 1 et 3.

☞ **Exercice 8.** **(a)** $e\mathscr{A}$ est stable par addition car $ex + ey = e(x + y)$ et par multiplication car $(ex)(ey) = e(exy)$. On a $0 = e0 \in e\mathscr{A}$. Par contre, 1 n'est généralement pas dans $e\mathscr{A}$, car $1 = ex$ entraîne que e est inversible, ce qui n'est pas nécessairement le cas. L'unité de $e\mathscr{A}$ est e (c'est-à-dire $e1$), car $e(ex) = e^2x = ex$. L'application donnée préserve l'addition et la multiplication puisque $(ex)(ey) = exy$. De plus, elle envoie l'unité 1 de $\mathscr{A}$ sur l'unité e de $e\mathscr{A}$.

(b) On a $ee' = e(1 - e) = e - e^2 = e - e = 0$. On définit $\varphi : \mathscr{A} \to e\mathscr{A} \times e'\mathscr{A}$ par $\varphi(x) = (ex, e'x)$. D'après la question précédente, φ est un morphisme d'anneaux unitaires. Il est injectif car $(ex, e'x) = (0, 0)$ entraîne $(e + e')x = 0$, donc $x = 0$. Il est surjectif car si on se donne un couple de la forme $(ex, e'y)$, on peut poser $z = ex + e'y$, et on a $ez = e(ex + e'y) = ex$ et de même $e'z = e'y$. Le couple $(ex, e'y)$ est donc l'image de z par φ.

☞ **Exercice 9.** **(a)** L'addition (usuelle) de ces polynômes est évidemment associative, admet le polynôme 0 pour élément neutre, et tout polynôme a un opposé qu'on obtient en remplaçant chaque coefficient par son opposé. La multiplication est donnée sur les monômes par $X^g X^h = X^{g+h}$. Elle n'est pas commutative si G n'est pas commutatif. Il n'y a pas de notion de degré puisque G n'est pas ordonné. La multiplication des monômes est associative car l'addition de G est associative et admet le polynôme X^0 (qu'on notera 1) comme élément neutre. Pour voir que la multiplication des polynômes est associative, il suffit de vérifier que les deux applications $(P, Q, R) \mapsto (PQ)R$ et $(P, Q, R) \mapsto P(QR)$ sont égales. Or ces deux application de $\mathscr{A}[G] \times \mathscr{A}[G] \times \mathscr{A}[G]$ vers $\mathscr{A}[G]$ sont $\mathscr{A}$-linéaires et donc déterminées par les images qu'elles donnent des monômes.

(b) Comme ε est clairement $\mathscr{A}$-linéaire, il suffit de faire les vérifications sur les monômes, ce qui est immédiat.

(c) Tout polynôme s'écrit $P = \sum_{g \in G} a_g X^g = a_0 X^0 + \sum_{g \neq 0} a_g X^g$. S'il est tel que $\varepsilon(P) = 0$, on a $a_0 = -\sum_{g \neq 0} a_g$, et donc $P = \sum_{g \neq 0} -a_g(1 - X^g)$. Si on a de plus $P = \sum_{g \neq 0} -b_g(1 - X^g)$, on voit que le polynôme $\sum_{g \neq 0} (a_g - b_g) X^g$ est nul, donc que $a_g = b_g$ pour tout $g \in G - \{0\}$.

(d) On a $1 - X^{g+h} = 1 - X^g X^h = (1 - X^g) + (1 - X^h) - (1 - X^g)(1 - X^h)$. Comme $(1 - X^g)(1 - X^h) \in \mathscr{I}^2$, on a $\overline{1 - X^{g+h}} = \overline{1 - X^g} + \overline{1 - X^h}$, et φ est donc un morphisme de groupes.

(e) D'après la question **(c)** tous les $\overline{1 - X^g}$ tels que $g \neq 0$ sont dans l'image de φ. Il en est donc de même de leur double, leur triple etc... de même que de leur opposé puisque l'image de φ est un sous-groupe $\mathscr{I}/\mathscr{I}^2$. Ainsi, toutes les combinaisons linéaires des $\overline{1 - X^g}$ à coefficients entiers sont dans l'image de φ, qui est donc surjectif.

Comme $\mathscr{I}/\mathscr{I}^2$ est un groupe commutatif, tout commutateur est dans le noyau de φ et comme ce noyau est distingué, $[G,G]$ est inclus dans le noyau de φ. Réciproquement, notons A le groupe abélien $G/[G,G]$, et $\pi : G \to G/[G,G]$ la projection canonique. On définit un morphisme de groupes $\psi : \mathscr{I} \to A$ en envoyant $1-X^g$ sur la classe de g. Ce morphisme est bien défini car $\mathscr{I}$ est un groupe abélien libre d'après la question **(c)**. Les éléments de $\mathscr{I}^2$ sont envoyés sur 0. En effet, $(1-X^g)(1-X^h)$, qui est egal à $(1-X^g)+(1-X^h)-(1-X^{g+h})$ est envoyé sur $g+h-(g+h)=0$. Comme on a $\psi(\varphi(g))=\overline{g}$ (y compris pour $g=0$, et où le surlignement représente la classe modulo $[G,G]$), on voit que tout élément g du noyau de φ est tel que $\overline{g}=0$, autrement-dit appartient à $[G,G]$.