HAX501X – Groupes et anneaux 1

Contrôle continu 2 – Correction

Clément Dupont

Questions de cours (5 pts).

1) *Démontrer qu'un anneau intègre A est soit de caractéristique zéro soit de caractéristique un nombre premier p.*

   Voir le cours.

2) *Soit K un corps, soit $a \in K$. Montrer que pour tout polynôme $f \in K[X]$ on a l'équivalence :*

$$f(a) = 0 \quad \iff \quad X - a \text{ divise } f.$$

   Voir le cours.

3) *Soient A, B des anneaux commutatifs, $f : A \to B$ un morphisme d'anneaux, et J un idéal de B. Montrer que l'image réciproque $f^{-1}(J)$ est un idéal de A.*

   Voir le cours.

4) *Dans $\mathbb{R}^2$, soit r la rotation d'angle $\frac{\pi}{2}$ et soit s la réflexion par rapport à l'axe des abscisses $\mathbb{R}(1,0)$. Décrire précisément la composée $r \circ s$. (On ne demande pas de démonstration.)*

   Notons Δ l'axe des abscisses. D'après le cours, $r \circ s = r_{\frac{\pi}{2}} \circ s_\Delta$ est la réflexion par rapport à la droite $r_{\frac{\pi}{4}}(\Delta)$, qui est la droite engendrée par le vecteur $(1,1)$ ("première bissectrice").

5) *Donner (sous la forme compréhensible de votre choix) la liste des éléments d'ordre 2 dans le groupe diédral D_6.*

   Avec les notations du cours, les éléments d'ordre 2 dans D_6 sont :

   – les 6 réflexions $s_0, s_1, s_2, s_3, s_4, s_5$;

   – la rotation $r^3 = -\mathrm{id}_{\mathbb{R}^2}$.

Exercice 1 : sur les axiomes des groupes (5 pts). *Les deux questions de cet exercice sont indépendantes. Dans la première question on montre qu'on peut simplifier l'axiomatique des groupes en demandant seulement l'existence d'un "neutre à gauche" et d'"inverses à gauche". Dans la deuxième question on voit que ça ne fonctionne pas si l'on mélange gauche et droite.*

1) *Soit G un ensemble muni d'une loi de composition interne $*$ qui vérifie les axiomes :*

   (i) Associativité : pour tous $x, y, z \in G$, $(x * y) * z = x * (y * z)$.

   (ii) Neutre à gauche : il existe un élément $e \in G$ tel que pour tout $x \in G$, $e * x = x$.

   (iii) Inverses à gauche : pour tout $x \in G$, il existe $x^{-1} \in G$ tel que $x^{-1} * x = e$.

a) *Soit $y \in G$ tel que $y * y = y$. Montrer que $y = e$.*

Comme $y * y = y$, on a $y^{-1} * (y * y) = y^{-1} * y$. Or on a d'une part

$$y^{-1} * (y * y) \overset{(i)}{=} (y^{-1} * y) * y \overset{(iii)}{=} e * y \overset{(ii)}{=} y$$

et d'autre part

$$y^{-1} * y \overset{(iii)}{=} e.$$

On en déduit que $y = e$.

b) *En utilisant la question précédente, montrer que pour tout $x \in G$ on a $x * x^{-1} = e$.*

On pose $y = x * x^{-1}$ et on calcule :

$$y * y = (x * x^{-1}) * (x * x^{-1}) \overset{(i)}{=} x * (x^{-1} * x) * x^{-1} \overset{(iii)}{=} x * e * x^{-1} \overset{(ii)}{=} x * x^{-1} = y.$$

On déduit de la question précédente que $y = e$, c'est-à-dire $x * x^{-1} = e$. Les inverses à gauche sont donc aussi inverses à droite !

c) *En déduire que pour tout $x \in G$ on a $x * e = x$.*

Soit $x \in G$. En utilisant la question précédente on calcule :

$$x * e \overset{(iii)}{=} x * (x^{-1} * x) \overset{(i)}{=} (x * x^{-1}) * x \overset{1)b)}{=} e * x \overset{(ii)}{=} x.$$

Donc le neutre à gauche est aussi un neutre à droite !

2) *Soit G un ensemble non vide dont on note e un des éléments. On définit une loi de composition interne $*$ sur G par la formule : $x * y = y$.*

a) *Montrer que cette loi vérifie les axiomes (i) et (ii) ci-dessus ainsi que l'axiome :*
(iv) Inverses à droite : pour tout $x \in G$, il existe $x^{-1} \in G$ tel que $x * x^{-1} = e$.

On montre les trois axiomes (i), (ii), (iv).

(i) Pour $x, y, z \in G$ on a $(x * y) * z = y * z = z$ et $x * (y * z) = x * z = z$, donc $(x * y) * z = x * (y * z)$.

(ii) Clairement, pour tout $x \in G$ on a $e * x = x$.

(iv) Soit $x \in G$, en posant $x^{-1} = e$ on a bien $x * x^{-1} = e$.

b) *Montrer que si G a au moins deux éléments alors $(G, *)$ n'est pas un groupe.*

Si $(G, *)$ est un groupe, alors pour tout $x \in G$ l'égalité $x * x = x$ implique que x est l'élément neutre du groupe. C'est impossible si G a au moins deux éléments, puisque dans un groupe il n'y a qu'un seul élément neutre.

Exercice 2 : inversibles de $\mathbb{Z}[\sqrt{2}]$ (10 pts).

On définit :

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\ ,\ a, b \in \mathbb{Z}\}\ .$$

On rappelle (vu en TD) que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.

1) *Montrer que l'application $\varphi : \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{2}]$ défini par $\varphi(a,b) = a + b\sqrt{2}$ est un isomorphisme de groupes.*

On calcule, pour $(a,b),(a',b') \in \mathbb{Z}^2$:

$$\begin{aligned}\varphi((a,b)+(a',b')) &= \varphi(a+a', b+b') \\ &= (a+a') + (b+b')\sqrt{2} \\ &= (a+b\sqrt{2}) + (a'+b'\sqrt{2}) \\ &= \varphi(a,b) + \varphi(a',b').\end{aligned}$$

Donc φ est un morphisme de groupes.

Clairement, φ est surjectif par définition de $\mathbb{Z}[\sqrt{2}]$.

Il reste à montrer que φ est injectif. Pour cela on montre que $\ker(\varphi) = \{(0,0)\}$. Soit $(a,b) \in \mathbb{Z}^2$ tel que $\varphi(a,b) = 0$, c'est-à-dire $a + b\sqrt{2} = 0$. Si $b \neq 0$ alors on obtient $\sqrt{2} = -\frac{a}{b}$ et donc $\sqrt{2} \in \mathbb{Q}$, ce qui est absurde. Donc $b = 0$ et donc $a = -b\sqrt{2} = 0$, d'où $(a,b) = (0,0)$.

On a donc montré que φ est un isomorphisme de groupes.

2) *Montrer que les anneaux $\mathbb{Z}^2$ et $\mathbb{Z}[\sqrt{2}]$ ne sont pas isomorphes.*

[Remarque : il ne suffit pas de montrer que φ n'est pas un morphisme d'anneaux. On veut montrer qu'il n'existe *aucun* isomorphisme d'anneaux entre $\mathbb{Z}^2$ et $\mathbb{Z}[\sqrt{2}]$.]

L'anneau $\mathbb{Z}^2$ n'est pas intègre (car $(1,0) \times (0,1) = (0,0)$), alors que l'anneau $\mathbb{Z}[\sqrt{2}]$ est intègre (car c'est un sous-anneau de $\mathbb{R}$ et que $\mathbb{R}$ est intègre). On en déduit que ces anneaux ne sont pas isomorphes.

3) a) *Pour un élément $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on définit son conjugé $c(x) = a - b\sqrt{2}$. Montrer qu'on a la formule, pour $x, x' \in \mathbb{Z}[\sqrt{2}]$: $c(xx') = c(x)c(x')$.*

C'est une vérification simple : pour $x = a + b\sqrt{2}, x' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ on a

$$c(xx') = c\left((aa' + 2bb') + (ab' + a'b)\sqrt{2}\right) = (aa' + 2bb') - (ab' + a'b)\sqrt{2}$$

et

$$c(x)c(x') = (a - b\sqrt{2})(a' - b'\sqrt{2}) = (aa' + 2bb') - (ab' + a'b)\sqrt{2}\ .$$

b) *Pour un élément $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on définit sa norme $N(x) = a^2 - 2b^2$. Montrer qu'on a les formules :*

$$\forall x \in \mathbb{Z}[\sqrt{2}],\ N(x) = x\,c(x)$$
$$\forall x, x' \in \mathbb{Z}[\sqrt{2}],\ N(xx') = N(x)N(x')\ .$$

La première formule se vérifie facilement :

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2\ .$$

La deuxième formule est une conséquence de la question précédente et de la première formule :

$$N(xx') = xx'c(xx') = xx'c(x)c(x') = (xc(x))(x'c(x')) = N(x)N(x')\ .$$

(Bien sûr on peut aussi la vérifier à la main sans utiliser la conjugaison.)

4) *Montrer qu'un élément $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(x) \in \{-1, 1\}$.*

Si $x \in \mathbb{Z}[\sqrt{2}]$ est inversible alors on a $xx^{-1} = 1$ et donc par la question précédente : $N(x)N(x^{-1}) = N(1) = 1$. Comme $N(x)$ et $N(x^{-1})$ sont des entiers relatifs, on a donc $N(x) \in \{-1, 1\}$.

Réciproquement, si $N(x) \in \{-1, 1\}$ alors on a par la question précédente : $xc(x) = \pm 1$, d'où $x(\pm c(x)) = 1$, et donc x est inversible d'inverse $\pm c(x)$.

Le but de la suite de l'exercice est de montrer l'égalité :

$$\mathbb{Z}[\sqrt{2}]^\times = \left\{\varepsilon(1+\sqrt{2})^n \ , \ \varepsilon \in \{-1, 1\}, \, n \in \mathbb{Z}\right\}.$$

5) *Démontrer l'inclusion $\supset$.*

Comme $1 + \sqrt{2}$ est de norme $N(1 + \sqrt{2}) = -1$, il est inversible dans $\mathbb{Z}[\sqrt{2}]$, d'inverse $-1 + \sqrt{2}$. Comme $\mathbb{Z}[\sqrt{2}]^\times$ est un groupe, on voit que $(1 + \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times$ pour tout $n \in \mathbb{Z}$. De plus, -1 et 1 sont aussi inversibles dans $\mathbb{Z}[\sqrt{2}]$, et donc pour tous $\varepsilon \in \{-1, 1\}$ et $n \in \mathbb{Z}$ le produit $\varepsilon(1 + \sqrt{2})^n$ est dans $\mathbb{Z}[\sqrt{2}]^\times$. Cela montre l'inclusion $\supset$.

6) *Soit un élément $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ qui vérifie : $1 \leqslant a + b\sqrt{2} < 1 + \sqrt{2}$.*

a) *Montrer qu'on a l'inégalité : $-1 \leqslant a - b\sqrt{2} \leqslant 1$.*

Comme $a + b\sqrt{2}$ est inversible dans $\mathbb{Z}[\sqrt{2}]$, son inverse est $\pm(a - b\sqrt{2})$ d'après le raisonnement de la question 4). Or, comme $a + b\sqrt{2} \geqslant 1$, son inverse est dans $[0, 1]$, et donc $-1 \leqslant a - b\sqrt{2} \leqslant 1$.

b) *En déduire qu'on a nécessairement $a = 1$ puis $b = 0$.*

En sommant les inégalités $1 \leqslant a + b\sqrt{2} < 1 + \sqrt{2}$ et $-1 \leqslant a - b\sqrt{2} \leqslant 1$ on trouve : $0 \leqslant 2a < 2 + \sqrt{2}$ et donc $0 \leqslant a < 1 + \frac{\sqrt{2}}{2}$. On en déduit que $0 \leqslant a < 2$ et donc, comme a est un entier, que $a = 0$ ou $a = 1$.

- ▷ Le cas $a = 0$ est impossible car sinon $a + b\sqrt{2} = b\sqrt{2}$ serait de norme $-2b^2$, et donc $\neq \pm 1$, ce qui serait en contradiction avec le fait que $a + b\sqrt{2}$ est inversible dans $\mathbb{Z}[\sqrt{2}]$.
- ▷ On en conclut que $a = 1$. En remplaçant dans l'inégalité $1 \leqslant a + b\sqrt{2} < 1 + \sqrt{2}$ on obtient alors $0 \leqslant b\sqrt{2} < \sqrt{2}$ et donc $0 \leqslant b < 1$. Comme b est un entier on a donc $b = 0$.

7) *Déduire de la question précédente que tout inversible de $\mathbb{Z}[\sqrt{2}]$ qui est $\geqslant 1$ est de la forme $(1 + \sqrt{2})^n$ pour un $n \in \mathbb{N}$.*

Soit $x \in \mathbb{Z}[\sqrt{2}]$ un inversible qui vérifie $x \geqslant 1$. On considère la suite

$$(1 + \sqrt{2})^0 = 1, \, 1 + \sqrt{2}, \, (1 + \sqrt{2})^2, \, (1 + \sqrt{2})^3, \ldots$$

qui est strictement croissante et tend vers $+\infty$, car $1 + \sqrt{2} > 1$. Il existe donc (un unique) $n \in \mathbb{N}$ tel qu'on a l'inégalité :

$$(1 + \sqrt{2})^n \leqslant x < (1 + \sqrt{2})^{n+1} \ .$$

En divisant par $(1 + \sqrt{2})^n$ on obtient alors :

$$1 \leqslant x(1 + \sqrt{2})^{-n} < 1 + \sqrt{2} \ .$$

Or comme x et $1 + \sqrt{2}$ sont des inversibles de $\mathbb{Z}[\sqrt{2}]$, le produit $x(1 + \sqrt{2})^{-n}$ l'est aussi. Par la question précédente on a donc $x(1 + \sqrt{2})^{-n} = 1$, et donc $x = (1 + \sqrt{2})^n$.

8) *En déduire l'égalité annoncée.*

Soit $x \in \mathbb{Z}[\sqrt{2}]^\times$. On procède par disjonction de cas.

- ▷ Cas $x \geqslant 1$. Traité dans la question précédente.
- ▷ Cas $0 < x < 1$. Dans ce cas-là, $\frac{1}{x} > 1$ et est inversible dans $\mathbb{Z}[\sqrt{2}]$. Par le premier cas (c'est-à-dire la question précédente), $\frac{1}{x}$ est donc de la forme $(1+\sqrt{2})^n$ pour un $n \in \mathbb{N}$. On en déduit que $x = (1+\sqrt{2})^{-n}$.
- ▷ Cas $x < 0$. Alors $-x > 0$ et est inversible dans $\mathbb{Z}[\sqrt{2}]$ (d'inverse $-x^{-1}$), donc $-x = (1+\sqrt{2})^n$ pour un certain $n \in \mathbb{Z}$, par les deux premiers cas. Donc $x = -(1+\sqrt{2})^n$.

On a donc montré l'inclusion $\subset$, et donc l'égalité annoncée.