ALGEBRE[1]

Corrigé de l'examen du 19 juin 2004

durée : 2 heures

Nota bene. *Le barême (approximatif) est I: 2 pts, II: 5 pts et III: 13 pts. L'exercice I est indépendant. Il pourra être utile d'utiliser les résultats de l'exercice II dans l'exercice III. Les notes de cours sont autorisées. L'usage de tout autre document est interdit.* Une réponse exacte sans justification ou avec une justification fausse ne rapportera aucun point. *Il sera fortement tenu compte de la clarté de la rédaction.*

I. Dans l'anneau de polynômes $(\frac{\mathbb{Z}}{11\mathbb{Z}}[X], +, \cdot)$ on considère le polynôme P défini par

$$P = \overline{1}\, X^{11} + \overline{10}\, X + \overline{1}.$$

Montrer que P n'a aucune racine. (On pourra utiliser le le petit théorème de Fermat dans $\frac{\mathbb{Z}}{11\mathbb{Z}}$ qui dit que $a^{10} = \overline{1}$ pour tout $a \in \frac{\mathbb{Z}}{11\mathbb{Z}}/\{\overline{0}\}$.)

Solution. On a $P(\overline{0}) = \overline{1}$ donc $\overline{1}$ n'est pas racine. Ensuite si $a \in \{\overline{1},\overline{2},\dots,\overline{10}\}$, d'après le petit théorème de Fermat $a^{10} = \overline{1} \Rightarrow a^{10} - \overline{1} = \overline{0}$ mais $-\overline{1} = \overline{10}$ donc

$$a^{10} + \overline{10} = \overline{0} \Rightarrow a^{10} \cdot a + \overline{10} \cdot a = \overline{0} \cdot a \Rightarrow a^{11} + \overline{10} \cdot a = \overline{0} \Rightarrow a^{11} + \overline{10} \cdot a + \overline{1} = \overline{1}$$

donc $P(a) = \overline{1}$ et ne s'annule donc pas. Le polynôme P n'a donc aucune racine. En fait, la fonction polynomiale $\tilde{P}$ associée à P est la fonction constante égale à $\overline{1}$.

□

II. Soit $w \in \mathbb{R}^{*+} =]0,\infty[$. On définit

$$\begin{aligned}\Omega &\stackrel{\text{def}}{=} \{\pm w^n, n \in \mathbb{Z}\} \\ &= \{1, w, w^{-1}, w^2, w^{-2}, \dots\} \cup \{-1, -w, -w^{-1}, -w^2, -w^{-2}, \dots\}\end{aligned}$$

A – Montrer que Ω est un sous-groupe de $(\mathbb{R}^*,\cdot)$, le groupe des nombres réels non nuls muni de la multiplication habituelle.

Solution. Ω est évidemment non vide et, puisque $w \neq 0$, inclus dans $\mathbb{R}^*$.

- Prenons $x,y \in \Omega$ et montrons que $x \cdot y \in \Omega$. On a

$$\begin{array}{rrcll} & x & = & \epsilon_x w^n & \text{où } \epsilon_x = \text{signe de } x \\ & y & = & \epsilon_y w^m & \text{où } \epsilon_y = \text{signe de } y \\ \Rightarrow & x \cdot y & = & \epsilon_{x\cdot y} w^{n+m} & \text{où } \epsilon_{x\cdot y} = \text{signe de } x \cdot y \\ \Rightarrow & x \cdot y & \in & \Omega & \end{array}$$

- Prenons $x \in \Omega$ et montrons $x^{-1} = \frac{1}{x} \in \Omega$. On a
  $x = \epsilon_x w^n \Rightarrow x^{-1} = \frac{1}{\epsilon_x} w^{-n} = \epsilon_x w^{-n} \in \Omega$.

Donc Ω est bien un sous-groupe de $(\mathbb{R}^*,\cdot)$.

□

Ajouté en cours d'épreuve : à partir de maintenant on suppose en outre $w \neq 1$.

B – Déterminer deux éléments a et b tels que $\Omega = \langle a,b \rangle$.

1. Licence de mathématiques (2-ième année), *Université Paul Sabatier (Toulouse III)*. Année scolaire 2003-2004

Solution. Tout élément x de Ω s'écrit $x = (-1)^\epsilon w^n$ avec $\epsilon = 0$ ou 1 et $n \in \mathbb{Z}$. Il suit que $\Omega = \langle -1,w \rangle$. □

C – Trouver un isomorphisme $f : \{-1,1\} \times \mathbb{Z} \to \Omega$ où $\{-1,1\}$ est muni de la *multiplication* et $\mathbb{Z}$ de l'*addition*.

(On rappelle que si G_1 est muni de la loi $*_1$ et G_2 de la loi $*_2$ alors la loi $*$ du groupe $G_1 \times G_2$ est définie par

$$(g_1,g_2) * (g_1',g_2') = (g_1 *_1 g_1' \, , g_2 *_2 g_2').)$$

En déduire que

$$\Omega \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}$$

où $\frac{\mathbb{Z}}{2\mathbb{Z}}$ est muni de la *addition*.

Solution. Nous considèrerons l'application f définie par

$$f : \begin{array}{ccc} \{-1,1\} \times \mathbb{Z} & \longrightarrow & \Omega \\ (\epsilon,m) & \longmapsto & \epsilon w^n. \end{array}$$

La loi $*$ sur $\{-1,1\} \times \mathbb{Z}$ est définie par

$$(\epsilon,n) * (\epsilon',m) \stackrel{\text{def}}{=} (\epsilon\epsilon' \, , n+m).$$

Nous montrerons successivement que f est un morphisme, puis que f est surjective et enfin que f est injective.

- Les relations suivantes montrent que f est un morphisme :

$$\begin{array}{rcl} f((\epsilon,n) * (\epsilon',m)) & = & f((\epsilon\epsilon' \, , n+m)) \\ & = & \epsilon\epsilon' w^{n+m} \\ & = & \epsilon w^n \epsilon' w^m \\ & = & f((\epsilon,n)) \cdot f((\epsilon',m)). \end{array}$$

- Soit $x = w^n$ alors $f(1,n) = x$ et si $x = -w^n$ alors $f(-1,n) = x$ donc tout élément de Ω admet un antécédent par f qui est donc surjective.
- Supposons maintenant $f((\epsilon,n)) = f((\epsilon',m))$ alors $\epsilon w^n = \epsilon' w^m \Rightarrow |\epsilon w^n| = |\epsilon' w^m|$ c'est-à-dire (puisque $w > 0$) $w^n = w^m$, ce qui implique en prenant le logarithme que $n = m$ - ici on utilise $w \neq 1$ qui donne $\ln(w) \neq 0$. Reportant $n = m$ dans $\epsilon w^n = \epsilon' w^m$ on trouve $\epsilon = \epsilon'$ d'où $(\epsilon,n) = (\epsilon',m)$ et cela montre que f est injective. (On aurait aussi pu montrer que le noyau de f est réduit à l'élément neutre de $\{-1,1\} \times \mathbb{Z}$ qui est $(1,0)$).

Finalement le groupe $(\{-1,1\},\cdot)$ étant cyclique d'ordre 2 est, d'après le cours, isomorphe à $(\frac{\mathbb{Z}}{2\mathbb{Z}},+)$. Appelons φ l'isomorphisme entre $\frac{\mathbb{Z}}{2\mathbb{Z}}$ et $\{-1,1\}$. L'application g définie sur $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}$ par $g(a,n) = f(\varphi(a),n)$ définit un isomorphisme entre $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{Z}$ et Ω.

□

III. Soit $\mathbb{Z}[\sqrt{2}]$ l'ensemble de nombres réels défini par

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

A – Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{R}, + ,\cdot)$.

Solution. $\mathbb{Z}[\sqrt{2}]$ est un sous ensemble non vide de $\mathbb{R}$. Pour montrer que c'est un sous-anneau de $(\mathbb{R}, + ,\cdot)$, il suffit de vérifier que

- $\forall \alpha,\beta \in \mathbb{Z}[\sqrt{2}]$ on a $\alpha - \beta \in \mathbb{Z}[\sqrt{2}]$,

- $\forall \alpha,\beta \in \mathbb{Z}[\sqrt{2}]$ on a $\alpha \cdot \beta \in \mathbb{Z}[\sqrt{2}]$.

Or, posant $\alpha = a + b\sqrt{2}$ et $\beta = a' + b'\sqrt{2}$ on a

$$\alpha - \beta = (a + b\sqrt{2}) - (a' + b'\sqrt{2}) = \underbrace{(a - a')}_{\in\mathbb{Z}} + \underbrace{(b - b')}_{\in\mathbb{Z}}\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

et

$$\alpha \cdot \beta = (a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) = \underbrace{(aa' + 2bb')}_{\in\mathbb{Z}} + \underbrace{(ab' + ba')}_{\in\mathbb{Z}}\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

□

B – Montrer que le corps quadratique $\mathbb{Q}(\sqrt{2})$ est le plus petit sous-corps de $\mathbb{R}$ qui contienne $\mathbb{Z}[\sqrt{2}]$.

Solution. Nous savons (cours) que $\mathbb{Q}[\sqrt{2}] = \{r + q\sqrt{2} : r,q \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$. D'après la définition même, puisque $\mathbb{Z} \subset \mathbb{Q}$ on $\mathbb{Z}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}]$. Soit maintenant F un sous-corps de $\mathbb{R}$ contenant $\mathbb{Z}[\sqrt{2}]$. Nous montrons que nécessairement $\mathbb{Q}[\sqrt{2}] \subset F$ et ceci prouvera que $\mathbb{Q}[\sqrt{2}]$ est le plus-petit sous-corps de $\mathbb{R}$ contenant $\mathbb{Z}[\sqrt{2}]$. Puisque F contient $\mathbb{Z}[\sqrt{2}]$, il contient $\mathbb{Z}$, et puisque c'est un corps, il contient alors $\mathbb{Q}$. Maintenant si F contient $\mathbb{Q}$ et $\sqrt{2}$ alors il contient aussi $\mathbb{Q}[\sqrt{2}]$.

□

Le but de cet exercice est de déterminer l'ensemble $\mathbb{Z}[\sqrt{2}]^*$ formé des éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{2}]$. On rappelle que $\alpha \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si il existe $\beta \in \mathbb{Z}[\sqrt{2}]$ tel que $\alpha \cdot \beta = 1$.

C – On considère l'application $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ définie par

$$\begin{aligned} N(a + b\sqrt{2}) &\overset{\text{def}}{=} (a + b\sqrt{2})(a - b\sqrt{2}) \\ &= a^2 - 2b^2 \end{aligned}$$

(1) Montrer que quels que soient α et β dans $\mathbb{Z}[\sqrt{2}]$, on a $N(\alpha.\beta) = N(\alpha).N(\beta)$.
(2) Montrer que si $\alpha \in (\mathbb{Z}[\sqrt{2}])^*$ alors $N(\alpha) \in \{-1, +1\}$.
(3) Montrer réciproquement que si $\alpha = a + b\sqrt{2}$ vérifie $N(\alpha) = \pm 1$ alors α est inversible et donner son inverse en fonction de a et b.

Solution. (1) En gardant la notation précédente pour α et β on a

$$\begin{aligned} N(\alpha \cdot \beta) &= (aa' + 2bb')^2 - 2(ab' + ba')^2 \\ &= (aa')^2 + 4aa'bb' + 4(bb')^2 - 4ab'ba' - 2(ab')^2 - 2(ba')^2 \\ &= (aa')^2 + 4(bb')^2 - 2(ab')^2 - 2(ba')^2 \\ \text{et} \quad N(\alpha) \cdot N(\beta) &= (a^2 - 2b^2)(a'^2 - 2b'^2) \\ &= a^2a'^2 + 4b^2b'^2 - 2b^2a'^2 - 2a^2b'^2 \end{aligned}$$

et l'égalité demandée suit.
(2) $\alpha \in (\mathbb{Z}[\sqrt{2}])^* \Rightarrow \exists \gamma \in (\mathbb{Z}[\sqrt{2}])^*$ tel que $\alpha \cdot \gamma = 1$. On a donc $N(\alpha \cdot \gamma) = N(1)$ qui donne avec la question précédente

$$\underbrace{N(\alpha)}_{\in\mathbb{Z}} \cdot \underbrace{N(\gamma)}_{\in\mathbb{Z}} = N(1) = 1$$

Cela signifie que l'entier $N(\alpha)$ est inversible i.e. appartient à $\mathbb{Z}^*$ mais $\mathbb{Z}^* = \{-1,1\}$.
(3) Si $\alpha = a + b\sqrt{2}$ on pose $\gamma = \frac{a - b\sqrt{2}}{N(\alpha)} \in \mathbb{Z}[\sqrt{2}]$ car $N(\alpha) = \pm 1$ et $\alpha \cdot \beta = \frac{N(\alpha)}{N(\alpha)} = 1$ donc α est inversible et γ est son inverse.

□

D – On pose $w = 1 + \sqrt{2}$ et $\Omega = \{\pm w^n, n \in \mathbb{Z}\}$. Montrer que $\Omega \subset (\mathbb{Z}[\sqrt{2}])^*$.

Solution. Puisque $N(w) = -1$, $w \in (\mathbb{Z}[\sqrt{2}])^*$ comme on a aussi $(-1) \in (\mathbb{Z}[\sqrt{2}])^*$ et que $(\mathbb{Z}[\sqrt{2}])^*$ est un groupe, on conclut que $\langle -1, w\rangle \subset (\mathbb{Z}[\sqrt{2}])^*$ mais d'après l'exercice I, $\langle -1, w\rangle = \Omega$.

□

E – Dans cette partie on veut établir que $(\mathbb{Z}[\sqrt{2}])^* \subset \Omega$ (ce qui impliquera, d'après le résultat de la question précédente, que $(\mathbb{Z}[\sqrt{2}])^* = \Omega$). Nous supposerons le contraire, à savoir :

(H) *Il existe* $\epsilon \in (\mathbb{Z}[\sqrt{2}])^*$ *tel que* $\epsilon \notin \Omega$.

et montrerons que cette hypothèse conduit à une contradiction.

(1) Montrer que $|\epsilon| \in (\mathbb{Z}[\sqrt{2}])^*$ et $|\epsilon| \notin \Omega$ où $|\cdot|$ désigne la valeur absolue.
(2) On note $\epsilon' = |\epsilon|$ si $|\epsilon| > 1$ et $\epsilon' = \frac{1}{|\epsilon|}$ si $|\epsilon| < 1$. Montrer que $\epsilon' \in (\mathbb{Z}[\sqrt{2}])^*$ mais $\epsilon' \notin \Omega$, puis qu'il existe $s \in \mathbb{N}$ tel que $w^s < \epsilon' < w^{s+1}$.
(3) On pose $\epsilon'' = \epsilon' w^{-s}$. Montrer que $1 < \epsilon'' < w$ et $\epsilon'' \in (\mathbb{Z}[\sqrt{2}])^*$ (de sorte que, conformément à C – (2), $N(\epsilon'') = \pm 1$).
(4) Montrer que les conditions $1 < \epsilon'' < w$ et $N(\epsilon'') = \pm 1$ conduisent à une contradiction.

Solution. (1) Si ϵ est positif il n'y rien à démontrer. Nous supposerons que ϵ est négatif de sorte que $|\epsilon| = -\epsilon$. Puisque $(\mathbb{Z}[\sqrt{2}])^*$ est un groupe, on a

$$-\epsilon = \underbrace{(-1)}_{\in(\mathbb{Z}[\sqrt{2}])^*} \cdot \underbrace{\epsilon}_{\in(\mathbb{Z}[\sqrt{2}])^*} \in (\mathbb{Z}[\sqrt{2}])^*.$$

De même si $-\epsilon \in \Omega$ alors puisque Ω est un groupe et $(-1) \in \Omega$ on a $(-1)\cdot(-\epsilon) \in \Omega$ soit $\epsilon \in \Omega$ ce qui est contraire à l'hypothèse (H).
(2) On remarque que puisque $1 \in \Omega$ et $|\epsilon| \notin \Omega$ on a ou bien $|\epsilon| > 1$ - auquel cas les propriétés demandées découlent de la question précédente - ou bien $|\epsilon| < 1$. Etudions ce second cas. D'abord $\epsilon' \in (\mathbb{Z}[\sqrt{2}])^*$ car c'est le symétrique d'un élément de $(\mathbb{Z}[\sqrt{2}])^*$ qui est un groupe. On a aussi $\epsilon' \notin \Omega$ car si $\epsilon' \in \Omega$ alors son symétrique $|\epsilon|$ appartient aussi à Ω car Ω est un groupe or on a vu dans la question précédente que $|\epsilon| \notin \Omega$. Enfin, puisque $w > 1$, on a

$$[1,\infty[= \cup_{s\in\mathbb{N}}[w^s, w^{s+1}].$$

Comme $\epsilon' \in [1,\infty[$ on en déduit l'existence de $s \in \mathbb{N}$ tel que $\epsilon' \in [w^s, w^{s+1}]$ ou encore $w^s \leq \epsilon' \leq x^{s+1}$ et comme $\epsilon' \notin \Omega$ les inégalités doivent être strictes.
(3) L'inégalité $w^s < \epsilon' < x^{s+1}$ donne immédiatement $1 < \epsilon'' < w$. On montre comme précédemment en utilisant le fait que $(\mathbb{Z}[\sqrt{2}])^*$ est un groupe et que $w^{-s} \in (\mathbb{Z}[\sqrt{2}])^*$ que $\epsilon'' \in (\mathbb{Z}[\sqrt{2}])^*$.
(4) Ecrivons $\epsilon'' = x + y\sqrt{2}$. On a $|N(\epsilon'')| = 1 \Rightarrow \left|x + y\sqrt{2}\right| \cdot \left|x - y\sqrt{2}\right| = 1$. Comme $\left|x + y\sqrt{2}\right| = \epsilon'' > 1$ on en déduit $\left|x - y\sqrt{2}\right| < 1$ soit $-1 < x - y\sqrt{2} < 1$. En ajoutant à cette inégalité, l'inégalité $1 < x + y\sqrt{2} < w$ on obtient $0 < 2x < 2 + \sqrt{2}$. Comme x est un entier la seule possibilité est $x = 1$ qui implique à son tour $y = 0$ d'où $\epsilon'' = 1 \in \Omega$ et on a une contradiction.

□

FIN