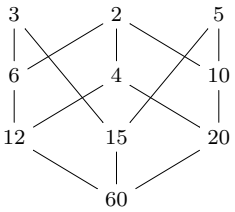
université de BORDEAUX	ANNÉE UNIVERSITAIRE 2020 / 2021 Session 2 de printemps **PARCOURS / ÉTAPE : 4TMA903U** **Code UE : 4TTN901S, 4TTN901S** **Épreuve :** Structures algébriques 2 **Date :** 7/6/2021 **Heure :** 14h30 **Durée :** 3h Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	Collège Sciences et technologies

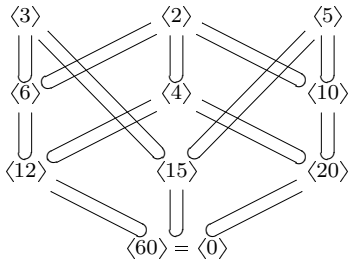
Exercice 1

Quels sont les idéaux, les idéaux premiers et les idéaux maximaux de $\mathbf{Z}/60\,\mathbf{Z}$?

Solution : Si $n \in \mathbf{N}_{>0}$, les idéaux de $\mathbf{Z}/n\mathbf{Z}$ sont les parties de la forme $d\mathbf{Z}/n\mathbf{Z}$ où d est un diviseur de n. Ici $n = 60 = 2^2 \times 3 \times 5$: dressons la liste des diviseurs de 60. Elle est résumée dans le diagramme suivant



qui se traduit par le treillis suivant



Parmi ceux-ci, les idéaux premiers correspondent aux diviseurs d qui sont premiers : ici, ce sont $\langle 2\rangle$, $\langle 3\rangle$ et $\langle 5\rangle$. Il sont tous maximaux.

Exercice 2

Soient K un corps et $P, Q \in K[Y]$ non constants et premiers entre eux. Montrer que le polynôme $XP(Y) - Q(Y)$ est irréductible dans $K[X,Y]$ et dans $K(X)[Y]$.

Solution : Posons $f(X,Y) = XP(Y) - Q(Y) \in K[X,Y]$.

• Supposons $f = gh$ avec $g, h \in K[X,Y]$. C'est une égalité dans $K(Y)[X]$: comme $\deg_X(f) = 1$, on a $\deg_X(g) = 0$ ou $\deg_X(h) = 0$. Quitte à échanger, supposons $\deg_X(g) = 0$ et $\deg_X(h) = 1$: cela montre que $g \in K[Y]$ divise P et Q. Comme ils sont premiers entre eux, on a nécessairement $g \in K^\times$. Cela montre que f est irréductible dans $K[X,Y]$.

• L'anneau $K[Y]$ est factoriel. Comme $\mathsf{pgcd}(P,Q) = 1$, le polynôme $f \in (K[Y])[X]$ est primitif : comme il est irréductible dans $K[X,Y]$, il l'est aussi dans $K(Y)[X]$.

Exercice 3

Posons $A = \mathbf{Z}[\sqrt{2}] = \{x + \sqrt{2}y\,;\, x, y \in \mathbf{Z}\}$. C'est un sous-anneau de $\mathbf{R}$.

(1) Quel est le corps des fractions de A ?

(2) Construire un isomorphisme $\mathbf{Z}[X]/\langle X^2 - 2\rangle \xrightarrow{\sim} A$.

(3) Montrer que l'application $\sigma\colon A \to A$ définie par $\sigma(x + \sqrt{2}y) = x - \sqrt{2}y$ (pour tous $x, y \in \mathbf{Z}$) est un morphisme d'anneaux. En déduire que l'application

$$N\colon A \to \mathbf{N}$$
$$x + \sqrt{2}y \mapsto \left|x^2 - 2y^2\right|$$

est multiplicative (*i.e.* telle que $N(z_1 z_2) = N(z_1)N(z_2)$ pour tous $z_1, z_2 \in A$).

(4) Montrer que muni du stathme N, l'anneau A est euclidien.

(5) Montrer que $z \in A^\times \Leftrightarrow N(z) = 1$. En déduire que $\alpha := 1 + \sqrt{2} \in A^\times$ et préciser la valeur de α^{-1}.

(6) Dans cette question, on montre que $A^\times = \{\pm\alpha^k\}_{k\in\mathbf{Z}}$. Soit $z = x + \sqrt{2}y \in A^\times$ (avec $x, y \in \mathbf{Z}$). Quitte à multiplier z par -1, on peut supposer que $x \geqslant 0$.

(a) Montrer qu'il existe $\varepsilon \in \{\pm 1\}$ tel que $z\alpha^\varepsilon = x_1 + \sqrt{2}y_1$ vérifie $x_1 \in \{\pm 1\}$ ou $|x_1| < x$ [indication : justifier que $x > 0$ et $|y| \leqslant x$, montrer que $\alpha^\varepsilon = \varepsilon + \sqrt{2}$ et calculer $z\alpha^\varepsilon$, puis traiter les cas $|y| = x$ et $|y| < x$ séparément].

(b) Conclure en itérant ce qui précède.

(c) En déduire un isomorphisme de groupes $(\mathbf{Z}/2\,\mathbf{Z}) \times \mathbf{Z} \xrightarrow{\sim} A^\times$.

(7) Montrer que 5 est premier dans A, mais que 7 ne l'est pas.

Solution : (1) On a $\mathbf{Z} \subset A$ donc $\mathbf{Q} \subset \mathsf{Frac}(A)$: comme $\sqrt{2} \in A$, on a donc $\mathbf{Q}(\sqrt{2}) \subset \mathsf{Frac}(A)$. Comme $A \subset \mathbf{Q}(\sqrt{2})$ et $\mathbf{Q}(\sqrt{2})$ est un corps, on a réciproquement $\mathsf{Frac}(A) \subset \mathbf{Q}(\sqrt{2})$ donc $\mathsf{Frac}(A) = \mathbf{Q}(\sqrt{2})$.

(2) Par la propriété universelle de l'anneau de polynômes $\mathbf{Z}[X]$, il existe un unique morphisme d'anneaux $f\colon \mathbf{Z}[X] \to \mathbf{R}$ tel que $f(X) = \sqrt{2}$ (ce n'est autre que le morphisme d'évaluation en $\sqrt{2}$). Par définition, on a $\mathsf{Im}(f) = A$. Si $P(X) \in \mathsf{Ker}(f)$, notons $P(X) = (X^2 - 2)Q(X) + R(X)$ avec $Q(X), R(X) \in \mathbf{Z}[X]$ et $\deg(R) < 2$ la division euclidienne de $P(X)$ par $X^2 - 2$ (licite puisque $X^2 - 2$ est unitaire). Écrivons $R(X) = x + yX$ avec $x.y \in \mathbf{Z}$: on a $R(X) \in \mathsf{Ker}(f)$ *i.e.* $x + \sqrt{2}y = 0$. Comme $(1, \sqrt{2})$ est une base de $\mathbf{Q}(\sqrt{2})$ sur $\mathbf{Q}$, cela implique $x = y = 0$, et donc $P(X) \in \langle X^2 - 2\rangle$. On a donc $\mathsf{Ker}(f) \subset \langle X^2 - 2\rangle$. L'inclusion réciproque est immédiate : on a $\mathsf{Ker}(f) = \langle X^2 - 2\rangle$. En passant au quotient, le morphisme f induit un isomorphisme $\tilde{f}\colon \mathbf{Z}[X]/\langle X^2 - 2\rangle \xrightarrow{\sim} A$.

(3) • Considérons l'unique morphisme d'anneaux $s\colon \mathbf{Z}[X] \to A$ tel que $s(X) = -\sqrt{2}$ (par la propriété universelle de l'anneau de polynômes $\mathbf{Z}[X]$ encore). Comme $s(X^2 - 2) = 0$, il se factorise en un morphisme d'anneaux $\tilde{s}\colon \mathbf{Z}[X]/\langle X^2 - 2\rangle \to A$. Combiné avec l'isomorphisme de la question précédente, il fournit un morphisme d'anneaux $\sigma\colon A \to A$ tel que $\sigma(\sqrt{2}) = -\sqrt{2}$, et donc $\sigma(x + \sqrt{2}y) = x - \sqrt{2}y$ pour tous $x, y \in \mathbf{Z}$.

• Comme σ est multiplicative, il en est de même de $A \to A; z \mapsto z\sigma(z)$, et donc de son composé N avec la valeur absolue $|.|\,:\, \mathbf{R} \to \mathbf{R}_{\geqslant 0}$. Notons que si $x, y \in \mathbf{Z}$, on a $N(x + \sqrt{2}y) = \left|x^2 - 2y^2\right| \in \mathbf{N}$.

(4) Soient $z \in A$ et $d \in A\backslash\{0\}$. On a $\lambda = \frac{z}{d} \in \mathsf{Frac}(A) = \mathbf{Q}(\sqrt{2})$: écrivons $\lambda = u + \sqrt{2}v$ avec $u, v \in \mathbf{Q}$. Il existe $x, y \in \mathbf{Z}$ tels que $|u - x| \leqslant \frac{1}{2}$ et $|v - y| \leqslant \frac{1}{2}$: posons $q = x + \sqrt{2}y \in A$. On a

$$N(\lambda - q) = \left|(u - x)^2 - 2(v - y)^2\right| \leqslant (u - x)^2 + 2(v - y)^2 \leqslant \tfrac{3}{4}$$

de sorte que si $r = z - qd$, on a $N(r) \leqslant \frac{3}{4}N(d)$

(5) Si $z \in A^\times$, on a $zz^{-1} = 1$ donc $N(z)N(z^{-1}) = N(1) = 1$: comme $N(z), N(z^{-1}) \in \mathbf{N}$, on a $N(z) = 1$. Réciproquement, si $z \in A$ est tel que $N(z) = 1$, on a $z\sigma(z) \in \{\pm 1\}$, donc $z \in A^\times$ (d'inverse $\sigma(z)$ ou $-\sigma(z)$). On a $N(1 + \sqrt{2}) = 1$ donc $1 + \sqrt{2} \in A^\times$. On a $\alpha^{-1} = -1 + \sqrt{2}$.

(6) (a) On a $\left|x^2-2y^2\right|=1$ donc $n\neq 0$ et d'où $x>0$ vu l'hypothèse. Cela implique aussi que $2y^2\leqslant 1+x^2$, d'où $|y|\leqslant x$. On a $z\alpha^{\varepsilon}=z(\varepsilon+\sqrt{2})=x_1+\sqrt{2}y_1$ avec $x_1=\varepsilon x+2y$ et $y_1=x+\varepsilon y$. Choisissons $\varepsilon\in\{\pm 1\}$ tel que $\varepsilon y<0$.
• Si $|y|=x$, on a $y_1=x+\varepsilon y=0$, donc $z(\varepsilon+\sqrt{2})\in\{\pm 1\}$.
• Si $|y|<x$, on a $-2x<-2|y|<0$, donc $-x<x-2|y|<x$, *i.e.* $|x_1|=|x-2|y||<x$.
(b) En répétant ce qui précède un nombre fini de fois, on construit inductivement des suites $(z_k=x_k+\sqrt{2}y_k)_{0\leqslant k\leqslant n}$ dans A et $(\varepsilon_k)_{1\leqslant k\leqslant n}$ dans $\{\pm 1\}$ telles que $z_0=z$, $z_k=z_{k-1}\alpha^{\varepsilon_k}$ et $|x_k|<|x_{k-1}|$ pour tout $k\in\{1,\dots,n\}$. Le processus s'arrête lorsque $z_n\in\{\pm 1\}$ (il s'arrête nécessairement au bout d'un nombre fini d'étapes parce que la suite $(|x_k|)_{1\leqslant k\leqslant n}$ est strictement décroissante et positive). Si $k=-(\varepsilon_1+\cdots+\varepsilon_n)\in\mathbf{Z}$, on a donc $z\alpha^{-k}\in\{\pm 1\}$ et donc $z=\pm\alpha^k$.
(c) D'après la question précédente, l'application

$$\begin{aligned}\psi\colon \{\pm 1\}\times\mathbf{Z}&\to A^\times\\ (\varepsilon,k)&\mapsto\varepsilon\alpha^k\end{aligned}$$

est surjective. C'est bien sûr un morphisme de groupes. Si $(\varepsilon,k)\in\mathsf{Ker}(\psi)$, on a $\varepsilon\alpha^k=1$: comme $\alpha>0$, cela implique $\varepsilon=1$, et donc $\alpha^k=1$, d'où $k=0$ vu que $|\alpha|\neq 1$. Cela montre que ψ est un isomorphisme. On conclut en observant que $\{\pm 1\}\simeq\mathbf{Z}/2\,\mathbf{Z}$.
(7) • Supposons 5 réductible dans A : il existe $z,z'\in A$ tels que $zz'=5$ et $z,z'\notin A^\times$: on a alors $N(z)N(z')=25$ et $N(z)\neq 1$ et $N(z')\neq 1$, *i.e.* $\mathsf{N}(z)=N(z')=1$. Écrivons $z=x+\sqrt{2}y$ avec $x,y\in\mathbf{Z}$: on a $x^2-2y^2=\pm 5$. Comme 2 n'est pas un carré modulo 5, on a nécessairement $x\equiv 0 \mod 5$ et $y\equiv 0 \mod 5$, ce qui implique $25\mid 5$: absurde. Cela montre que 5 est irréductible dans A.
• On a $(3+\sqrt{2})(3-\sqrt{2})=7$, mais $N(3\pm\sqrt{2})=7$, de sorte que $3\pm\sqrt{2}\notin A^\times$, ce qui montre que 7 est réductible dans A.

Remarque. On le voit immédiatement en écrivant $A/5A\simeq\mathbf{F}_5[X]/\langle X^2-2\rangle\simeq\mathbf{F}_{25}$ (parce que 2 n'est pas un carré modulo 5), et $A/7A\simeq\mathbf{F}_7[X]/\langle X^2-2\rangle\simeq\mathbf{F}_7[X]/\langle(X+3)(X-3)\rangle\simeq\mathbf{F}_7^2$.

Exercice 4

Posons $K=\mathbf{Q}(\sqrt{2},\sqrt[3]{7})\subset\mathbf{R}$.
(1) Que vaut $[K:\mathbf{Q}]$?
(2) Donner une base de K vu comme $\mathbf{Q}$-espace vectoriel.
(3) En déduire que le polynôme minimal de $\alpha:=\sqrt{2}+\sqrt[3]{7}$ sur $\mathbf{Q}$ n'est pas de degré 2 ou 3.
(4) En déduire que $K=\mathbf{Q}(\alpha)$ et calculer le polynôme minimal de α sur $\mathbf{Q}$.

Solution : (1) On a les inclusions $\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})\subset K$ et $\mathbf{Q}\subset\mathbf{Q}(\sqrt[3]{7})\subset K$. On a $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2$ et $[\mathbf{Q}(\sqrt[3]{7}):\mathbf{Q}]=3$, parce que le polynôme minimal de $\sqrt{2}$ (resp. $\sqrt[3]{7}$) sur $\mathbf{Q}$ est le polynôme d'Eisenstein X^2-3 (resp. X^3-7). Par transitivité des degrés, cela implique que $6\mid[K:\mathbf{Q}]$. Par ailleurs, on a $[K:\mathbf{Q}]=[K:\mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}):\mathbf{Q}]\leqslant 6$ parce que $[K:\mathbf{Q}(\sqrt{2})]\leqslant[\mathbf{Q}(\sqrt[3]{7}):\mathbf{Q}]$ (le polynôme minimal de $\sqrt[3]{7}$ sur $\mathbf{Q}(\sqrt{2})$ divise son polynôme minimal sur $\mathbf{Q}$ (qui est X^3-7 comme on l'a vu). Finalement, on a $[K:\mathbf{Q}]=6$.
(2) Une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\sqrt{2})$ est $(1,\sqrt{2})$. D'après la question précédente, on a $6=[K:\mathbf{Q}]=[K:\mathbf{Q}(\sqrt{2})]\underbrace{[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]}_{=2}$ et donc $[K:\mathbf{Q}(\sqrt{2})]=3$. Cela montre que le polynôme minimal de $\sqrt[3]{7}$ sur $\mathbf{Q}(\sqrt{2})$ est de degré 3 : comme il divise X^3-7, il est égal à X^3-7. Cela implique qu'une base du $\mathbf{Q}(\sqrt{2})$-espace vectoriel K est $(1,\sqrt[3]{7},\sqrt[3]{7}^2)$. Le théorème de la base téléscopique implique qu'une base de K comme $\mathbf{Q}$-espace vectoriel est donnée par $\mathfrak{B}=(1,\sqrt{2},\sqrt[3]{7},\sqrt{2}\sqrt[3]{7},\sqrt[3]{7},\sqrt{2}\sqrt[3]{7}^2)$.

(3) • On a $\alpha^2 = 2 + 2\sqrt{2}\sqrt[3]{7} + \sqrt[3]{7}^2$. Si α était de degré 2 sur $\mathbf{Q}$, il existerait $x, y \in \mathbf{Q}$ tels que $\alpha^2 + x\alpha + y = 0$, donc $2\sqrt{2}\sqrt[3]{7} + \sqrt[3]{7}^2 + x\sqrt{2} + x\sqrt[3]{7} + y + 2 = 0$, contredisant le fait que $\mathfrak{B}$ est libre sur $\mathbf{Q}$.
• De même, on a $\alpha^3 = 2\sqrt{2} + 6\sqrt[3]{7} + 3\sqrt{2}\sqrt[3]{7}^2 + 7$. Si α était de degré 3 sur $\mathbf{Q}$, il existerait $x, y, z \in \mathbf{Q}$ tels que $\alpha^3 + x\alpha^2 + y\alpha + z = 0$, donc

$$3\sqrt{2}\sqrt[3]{7}^2 + 2x\sqrt{2}\sqrt[3]{7} + x\sqrt[3]{7}^2 + (y+2)\sqrt{2} + (y+6)\sqrt[3]{7} + 2x + z + 7 = 0,$$

contredisant le fait que $\mathfrak{B}$ est libre sur $\mathbf{Q}$.
(4) On a $\mathbf{Q} \subset \mathbf{Q}(\alpha) \subset K$, donc $[\mathbf{Q}(\alpha) : \mathbf{Q}] \mid 6$. Comme $[\mathbf{Q}(\alpha) : \mathbf{Q}] \notin \{1, 2, 3\}$ d'après la question précédente, on a nécessairement $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6$, *i.e.* $K = \mathbf{Q}(\alpha)$ (on a bien sûr $\alpha \notin \mathbf{Q}$). Cela montre que le polynôme minimal de α sur $\mathbf{Q}$ est de degré 6.
Si $P(X) = X^3 - 7$, on a $P(\alpha - \sqrt{2}) = 0$, donc α est racine de $P(X - \sqrt{2})$, donc *a fortiori* de

$$\begin{aligned} P(X-\sqrt{2})P(X+\sqrt{2}) &= \big((X-\sqrt{2})^3 - 7\big)\big((X+\sqrt{2})^3 - 7\big) \\ &= (X^2-2)^3 - 7\big((X-\sqrt{2})^3 + (X+\sqrt{2})^3\big) + 49 \\ &= X^6 - 6X^4 + 12X^2 - 8 - 7(2X^3 + 6X) + 49 \\ &= X^6 - 6X^4 - 14X^3 + 12X^2 - 42X + 41 \end{aligned}$$

Comme il est de degré 6 et unitaire, $X^6 - 6X^4 - 14X^3 + 12X^2 - 42X + 41$ est le polynôme minimal de α sur $\mathbf{Q}$.

Exercice 5

(1) Montrer qu'il existe $\alpha \in \mathbf{F}_{27}$ tel que $\mathbf{F}_{27} = \mathbf{F}_3[\alpha]$ et $\alpha^3 = \alpha - 1$.
(2) Montrer que α engendre le groupe multiplicatif $\mathbf{F}_{27}^\times$.

Solution : (1) Posons $P(X) = X^3 - X + 1 \in \mathbf{F}_3[X]$. Il n'a pas de racine dans $\mathbf{F}_3$: comme il est de degré 3, cela implique qu'il est irréductible dans $\mathbf{F}_3[X]$. Il en résulte que $\mathbf{F}_3[X]/\langle P(X)\rangle$ est une corps à $3^3 = 27$ éléments : on a $\mathbf{F}_3[X]/\langle P(X)\rangle \xrightarrow{\sim} \mathbf{F}_{27}$ et l'image α de la classe de X a les propriétés requises.
(2) Le groupe $\mathbf{F}_{27}^\times$ est d'ordre $26 = 2 \times 13$: d'après le théorème de Lagrange, l'ordre de α dans $\mathbf{F}_{27}^\times$ divise 26. L'élément α n'est pas d'ordre 2, vu qu'il est de degré 3 sur $\mathbf{F}_3$. Comme on est en caractéristique 3, on a $\alpha^9 = (\alpha^3)^3 = (\alpha - 1)^3 = \alpha^3 - 1 = \alpha + 1$. En multipliant par α^3, cela implique que $\alpha^{12} = (\alpha + 1)(\alpha - 1) = \alpha^2 - 1$, et donc $\alpha^{13} = \alpha^3 - \alpha = -1$. On a donc $\alpha^{13} \neq 1$ et α n'est pas d'ordre 13 : il est donc nécessairement d'ordre 26, et c'est un générateur de $\mathbf{F}_{27}^\times$.