ALGÈBRE GÉNÉRALE

par David Blottière, le 1er octobre 2023 à 12h54

UN CORRIGÉ

DS N°1

SOMMAIRE

§ 1. QUESTIONS DE COURS

Q1. — Énoncer le théorème de classification des groupes monogènes.

Q2. — Soit $n \in \mathbf{N}^*$. Énoncer le théorème sur les inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$, puis le démontrer.

Q3. — Énoncer le théorème des restes chinois.

Q4. — Soit $\mathbf{K}$ un corps. Énoncer le théorème décrivant les idéaux de $\mathbf{K}[X]$, puis le démontrer.

Q5. — Énoncer la formule de Leibniz dans $\mathbf{R}[X]$, puis la démontrer.

§ 2. ISOMÉTRIES D'UN ESPACE EUCLIDIEN

Soit $(E, \langle \cdot , \cdot \rangle)$ un espace euclidien. On note $|| \cdot ||$ la norme induite sur E par le produit scalaire $\langle \cdot , \cdot \rangle$. Un endomorphisme de E est une isométrie de E si :

$$\forall x \in E, \quad \left|\left| f(x) \right|\right| = ||x||.$$

L'ensemble des isométries de E est noté $\mathscr{O}(E)$.

Q6. — Démontrer que $\mathscr{O}(E)$ est un sous-groupe du groupe $(GL(E), \circ)$ des automorphismes de E.

• $\mathscr{O}(E) \subset GL(E)$. Soit f une isométrie de E. Soit $x \in \operatorname{Ker}(f)$. Alors $f(x) = 0_E$ et donc :

$$||x|| = \left|\left| f(x) \right|\right| = ||0_E|| = 0.$$

Par séparation de la norme $x = 0_E$. L'endomorphisme f de E est injectif. Comme E est de dimension finie, nous en déduisons que f est un automorphisme de E.

• $\mathrm{id}_E \in \mathscr{O}(E)$. L'application id_E est linéaire. De plus, pour tout $x \in E$:

$$||id_E(x)|| = ||x||.$$

Donc id_E est une isométrie de E.

• $\mathscr{O}(E)$ est stable par composition. Soit $(f, g) \in \mathscr{O}(E)^2$. L'application $f \circ g$ est un endomorphisme de E et pour tout $x \in E$:

$$\begin{array}{rcll} \|f \circ g(x)\| & = & \|f(g(x))\| & \\ & = & \|g(x)\| & [f \text{ est une isométrie de } E] \\ & = & \|x\| & [g \text{ est une isométrie de } E]. \end{array}$$

Donc $f \circ g$ est une isométrie de E.

• $\mathcal{O}(E)$ est stable par passage à l'inverse. Soit $f \in \mathcal{O}(E)$. Nous savons que f est bijective et que l'inverse d'une application linéaire bijective est linéaire. Donc f^{-1} est un endomorphisme de E. Soit $x \in E$. Comme $f \circ f^{-1} = \mathrm{id}_E$:

$$\begin{array}{rcll} \|x\| & = & \|f(f^{-1}(x))\| & \\ & = & \|f^{-1}(x)\| & [f \text{ est une isométrie de } E]. \end{array}$$

Donc f^{-1} est une isométrie de E.

• Conclusion. Comme $\mathcal{O}(E)$ est une partie de $GL(E)$ qui contient id_E et qui est stable par composition et par passage à l'inverse, $\mathcal{O}(E)$ est un sous-groupe de $(GL(E), \circ)$. ■

§ 3. SIMILITUDES COMPLEXES

Pour tout $(\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}$, on définit l'application $f_{\alpha,\beta}$ par :

$$f_{\alpha,\beta} \left| \begin{array}{ccc} \mathbf{C} & \longrightarrow & \mathbf{C} \\ z & \longmapsto & \alpha \cdot z + \beta. \end{array} \right.$$

On pose :

$$\mathcal{S} := \{f_{\alpha,\beta} \,:\, (\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}\}.$$

Q7. — Démontrer que la composition des applications induit une loi de composition interne sur $\mathcal{S}$.

Soient $(\alpha_1, \beta_1) \in \mathbf{C}^* \times \mathbf{C}$ et $(\alpha_2, \beta_2) \in \mathbf{C}^* \times \mathbf{C}$. Nous calculons l'image de $z \in \mathbf{C}$ par la composée $f_{\alpha_1,\beta_1} \circ f_{\alpha_2,\beta_2}$.

$$\begin{array}{rcl} f_{\alpha_1,\beta_1} \circ f_{\alpha_2,\beta_2}(z) & = & f_{\alpha_1,\beta_1}(f_{\alpha_2,\beta_2}(z)) \\ & = & f_{\alpha_1,\beta_1}(\alpha_2 z + \beta_2) \\ & = & \alpha_1\alpha_2 z + \alpha_1\beta_2 + \beta_1 \end{array}$$

Comme α_1 et α_2 sont non nuls, $\alpha_1\alpha_2 \neq 0$ ($\mathbf{C}$ est un corps donc intègre). Nous observons :

$$f_{\alpha_1,\beta_1} \circ f_{\alpha_2,\beta_2} = f_{\alpha_1\alpha_2\,,\,\alpha_1\beta_2+\beta_1} \in \mathcal{S}.$$

■

Q8. — Démontrer que $(\mathcal{S}, \circ)$ est un groupe. Est-il commutatif?

• La loi $\circ$ sur $\mathcal{S}$ est associative. Il s'agit d'une propriété formelle qui a été établie dans le cours.

• La loi $\circ$ sur $\mathcal{S}$ possède un élément neutre. Nous observons :

$$\mathrm{id}_{\mathbf{C}} = f_{\alpha,\beta} \text{ avec } \alpha = 1 \in \mathbf{C}^* \text{ et } \beta = 0.$$

Donc $\mathrm{id}_{\mathbf{C}} \in \mathcal{S}$. Pour toute application $f : \mathbf{C} \longrightarrow \mathbf{C}$:

$$f \circ \mathrm{id}_{\mathbf{C}} = f = \mathrm{id}_{\mathbf{C}} \circ f.$$

Ces identités valant en particulier pour les éléments de $\mathcal{S}$, l'application $\mathrm{id}_{\mathbf{C}} \in \mathcal{S}$ est le neutre de $(\mathcal{S}, \circ)$.

• Tout élément de $\mathcal{S}$ possède un inverse pour la loi $\circ$. Soit $(\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}$. Remarquons que $\dfrac{1}{\alpha} \in \mathbf{C}^*$ et que

$-\dfrac{\beta}{\alpha} \in \mathbf{C}$. D'après ce qui précède :

$$f_{\alpha,\beta} \circ f_{\frac{1}{\alpha}, -\frac{\beta}{\alpha}} = f_{1,0} = \mathrm{id}_{\mathbf{C}} \qquad \text{et} \qquad f_{\frac{1}{\alpha}, -\frac{\beta}{\alpha}} \circ f_{\alpha,\beta} = f_{1,0} = \mathrm{id}_{\mathbf{C}}.$$

Nous en déduisons que $f_{\alpha,\beta}$ est inversible pour la loi $\circ$ (autrement dit, bijective) et que :

$$\left(f_{\alpha,\beta}\right)^{-1} = f_{\frac{1}{\alpha}, -\frac{\beta}{\alpha}} \in \mathscr{S}.$$

• La loi $\circ$ sur $\mathscr{S}$ n'est pas commutative. D'après la question précédente :

$$f_{1,1} \circ f_{2,1} = f_{2,2} \quad \text{et} \quad f_{2,1} \circ f_{1,1} = f_{2,3}\,.$$

Comme $f_{2,2}(0) = 2$ et $f_{2,3}(0) = 3$, $f_{2,2} \neq f_{2,2}$.

• Conclusion. Donc $(\mathscr{S}, \circ)$ est une ensemble muni d'une loi interne associative, non commutative, possédant un élément neutre et tel que tout élément de $\mathscr{S}$ est inversible pour $\circ$. Aussi $(\mathscr{S}, \circ)$ est-il un groupe anabélien. ■

Q9. — À quelle condition sur $(\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}$, l'application $f_{\alpha,\beta}$ est-elle d'ordre fini dans $(\mathscr{S}, \circ)$?

• Calcul des puissances d'un élément de $\mathscr{S}$. Soit $(\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}$. Nous calculons :

$$\left(f_{\alpha,\beta}\right)^2 = f_{\alpha\,,\,\beta(\alpha+1)} \quad \text{et} \quad \left(f_{\alpha,\beta}\right)^3 = f_{\alpha^2\,,\,\beta(\alpha^2+\alpha+1)}.$$

Nous énonçons la conjecture :

$$\forall\, n \in \mathbf{N}^*, \quad \left(f_{\alpha,\beta}\right)^n = f_{\alpha^n\,,\,\beta \sum_{k=0}^{n-1} \alpha^k}$$

• Recherche d'une condition nécessaire pour qu'un élément de $\mathscr{S}$ soit d'ordre fini. Soit $(\alpha, \beta) \in \mathbf{C}^* \times \mathbf{C}$ tel que $f_{\alpha,\beta}$ est d'ordre fini. Soit $d \in \mathbf{N}^*$ son ordre. Alors :

$$\mathrm{id}_{\mathbf{C}} = \left(f_{\alpha,\beta}\right)^d = f_{\alpha^d\,,\,\beta \sum_{k=0}^{d-1} \alpha^k}$$

en particulier :

$$0 = \mathrm{id}_{\mathbf{C}}(0) = f_{\alpha^d\,,\,\beta \sum_{k=0}^{d-1} \alpha^k}(0) = \beta \sum_{k=0}^{d-1} \alpha^k.$$

Nous en déduisons :

$$1 = \mathrm{id}_{\mathbf{C}}(1) = f_{\alpha^d\,,\,0}(1) = \alpha^d.$$

Le nombre complexe α est donc une racine d-ième de l'unité. Comme :

$$X^d - 1 = (X-1)\left(\sum_{k=0}^{d-1} X^k\right)$$

il vient :

$$(\alpha - 1)\left(\sum_{k=0}^{d-1} \alpha^k\right) = 0.$$

Ainsi :

— si $\alpha = 1$, alors $\displaystyle\sum_{k=0}^{d-1} \alpha^k = d \neq 0$ et donc $\beta = 0$ (cf. (3)).

— si $\alpha \neq 1$, alors $\displaystyle\sum_{k=0}^{d-1} \alpha^k = 0$ et donc $\beta \displaystyle\sum_{k=0}^{d-1} \alpha^k = 0$ quelque soit la valeur de β.

Aussi si $f_{\alpha,\beta}$ est d'ordre fini alors :

— soit $\alpha = 1$ et $\beta = 0$;

— soit α est une racine de l'unité distincte de 1 (aucune condition sur β).

• Détermination des éléments d'ordre fini du groupe $(\mathscr{S}, \circ)$. Nous vérifions si les candidats trouvés à la fin de la précédente étude sont d'ordre fini dans $\mathscr{S}$.

— L'élément $f_{1,0}$ de $\mathscr{S}$ coïncide avec son neutre $\mathrm{id}_{\mathbf{C}}$. Il est donc d'ordre fini égal à 1.

— Soit $\alpha \in \mathbb{U}_d \setminus \{1\}$, où $d \in \mathbf{N}_{\geq 2}$ et soit $\beta \in \mathbf{C}$ quelconque. Nous savons :

$$\left(f_{\alpha,\beta}\right)^d = f_{\alpha^d\,,\,\beta \sum_{k=0}^{d-1} \alpha^k}.$$

Comme $\alpha^d = 1$ et :

$$\sum_{k=0}^{d-1} \alpha^k = 0$$

d'après (4) et $\alpha \neq 1$:

$$\left(f_{\alpha,\beta}\right)^d = f_{1,0} = \mathrm{id}_{\mathbf{C}}$$

L'élément $f_{\alpha,\beta}$ de $\mathscr{S}$ est donc d'ordre fini (et son ordre divise d).

• Conclusion. L'ensemble des éléments d'ordre fini du groupe $(\mathscr{S}, \circ)$ est donc :

$$\mathscr{S}_{\mathrm{tor}} = \{\mathrm{id}_{\mathbf{C}}\} \cup \left\{ f_{\alpha,\beta}\ :\ \alpha \in \left(\bigcup_{n \in \mathbf{N}_{\geq 2}} \mathbb{U}_n \right) \setminus \{1\}\ ,\ \beta \in \mathbf{C} \right\}$$

■

§ 4. Groupes dont les carrés égalent le neutre

Soit $(G, *)$ un groupe dont le neutre est noté e. On suppose que :

$$\forall\, x \in G, \quad x * x = e.$$

Q10. — Démontrer que le groupe $(G, *)$ est abélien.

Soit $(x, y) \in G^2$. Par hypothèse :

$$\left(x * y\right) * \left(x * y\right) = e\,.$$

En multipliant chaque terme de cette identité par $y^{-1} * x^{-1}$ à droite, il vient :

$$x * y = y^{-1} * x^{-1}.$$

Or comme $x * x = e$ et $y * y = e$, $x = x^{-1}$ et $y = y^{-1}$. Nous en déduisons :

$$x * y = y * x\,.$$

■

Désormais, on suppose que G est fini.

Q11. — Soient H un sous-groupe de G et $x \in G \setminus H$. On note K le sous-groupe engendré par $H \cup \{x\}$. Démontrer :

$$\mathrm{Card}\,(K) = 2 \cdot \mathrm{Card}\,(H)\,.$$

• Description du sous-groupe K. Considérons la partie L de G définie par :

$$L := \left\{ h * x^k \ : \ h \in H \text{ et } k \in \{0,1\} \right\}.$$

La partie L contient e. Comme H et $\{e, x\}$ sont stables par produit et comme G est abélien, L est stable par produit. En outre, pour tout $h \in H$:

$$(h * e)^{-1} = h^{-1} = h^{-1} * e \qquad \text{et} \qquad (h * x)^{-1} = x^{-1} * h^{-1} = x * h^{-1} = h^{-1} * x \qquad \left[x^2 = e \text{ et } G \text{ est abélien}\right]$$

L est également stable par passage au symétrique. Nous en déduisons que L est un sous-groupe de G.
Il est clair que L contient H, x et que tout sous-groupe de G contenant H et x contient L. Ainsi $L = K$.

• Cardinal de K. D'après la description de K précédente, l'application :

$$\varphi \left| \begin{array}{ccc} H \times \{e, x\} & \longrightarrow & K \\ (h, u) & \longmapsto & h * u \end{array} \right.$$

est surjective. Comme G est abélien, elle est également un morphisme de groupes. Puisque $x \notin H$, $\operatorname{Ker}(\varphi) = \{(e, e)\}$ et donc φ est injective. Nous en déduisons :

$$\operatorname{Card}(K) = \operatorname{Card}(H) \times \operatorname{Card}(< x >) = 2 \cdot \operatorname{Card}(H).$$

• Généralisation. En reprenant l'étude précédente, on démontre que si H_1 et H_2 sont deux sous-groupes d'un groupe abélien‘ G, alors le plus petit sous-groupe de G contenant H_1 et H_2 est :

$$\langle H_1 \cup H_2 \rangle = \{h_1 * h_2 \ : \ (h_1, h_2) \in H_1 \times H_2\}$$

et que les groupes $\langle H_1 \cup H_2 \rangle$ et $H_1 \times H_2$ sont isomorphes. ■

Q12. — En déduire que $\operatorname{Card}(G)$ est une puissance de 2.

Nous raisonnons par l'absurde. Supposons que le cardinal de G n'est pas une puissance de 2 et démontrons par récurrence que, pour tout $n \in \mathbf{N}$:

$$\mathscr{P}(n) \ : \text{ il existe un sous-groupe } H_n \text{ de } G \text{ de cardinal } 2^n.$$

Nous aboutirons alors à une contradiction car le cardinal de G est supposé fini et 2^n tend vers $+\infty$ quand n tend vers $+\infty$.

• Initialisation à $n = 0$. Posons $H_0 = \{e\}$. C'est un sous-groupe de G de cardinal $2^0 = 1$.

• Hérédité. Soit $n \in \mathbf{N}$ tel que $\mathscr{P}(n)$ soit vraie. Le sous-groupe H_n est de cardinal 2^n. Comme le cardinal de G n'est pas une puissance de 2, la partie H_n de G n'est pas égale à G. Il existe donc un élément noté x tel que $x \in G \setminus H_n$. Posons :

$$H_{n+1} := \langle H_n \cup \{x\} \rangle .$$

D'après la question précédente, H_{n+1} est un sous-groupe de cardinal $2 \operatorname{Card}(H_n) = 2^{n+1}$.

• Hérédité. De l'initialisation à $n = 0$, de l'hérédité et de l'axiome de récurrence, nous déduisons que pour tout $n \in \mathbf{N}$, il existe un sous-groupe H_n de G de cardinal 2^n.

• Autre solution. Comme G est abélien, l'application :

$$f \left| \begin{array}{ccc} (\mathbf{Z}, +) \times (G, *) & \longrightarrow & (G, *) \\ (k, g) & \longmapsto & g^k \end{array} \right.$$

est un morphisme de groupes. Comme, pour tout $x \in G$, $x^2 = e$, l'application :

$$\overline{f} \left| \begin{array}{ccc} \mathbb{F}_2 \times G & \longrightarrow & G \\ \left(\overline{k}, g\right) & \longmapsto & g^k \end{array} \right.$$

est bien définie. On vérifie alors que $\left(G,*,\overline{f}\right)$ est un $\mathbb{F}_2$-espace vectoriel. Ce dernier est de dimension finie, puisqu'engendré par G fini. Si l'on note d la dimension de G et $\mathscr{B}=(e_1,\dots,e_d)$ une base de G, alors l'application :

$$\left|\begin{array}{ccc} \mathbb{F}_2^d & \longrightarrow & G \\ \left(\overline{k_1},\dots,\overline{k_d}\right) & \longmapsto & e_1^{\overline{k_1}}*\dots*e_d^{\overline{k_d}} \end{array}\right.$$

est bijective. Ainsi $\mathrm{Card}\,(G)=\mathrm{Card}\left(\mathbb{F}_2^d\right)=2^d$. ∎

§ 5. GROUPES AYANT UN NOMBRE FINI DE SOUS-GROUPES

Soit $(G,*)$ un groupe possédant un nombre fini de sous-groupes.

Q13. — Démontrer que tout élément de G est d'ordre fini.

Nous raisonnons par l'absurde. Supposons qu'il existe un élément x de G d'ordre infini. Alors l'application f définie par :

$$f\left|\begin{array}{ccc} (\mathbf{Z},+) & \longrightarrow & (G,*) \\ n & \longmapsto & x^n \end{array}\right.$$

est un morphisme de groupes, qui est injectif.
Les sous-groupes $a\mathbf{Z}$, où $a\in\mathbf{N}$, de $(\mathbf{Z},+)$ sont deux-à-deux distincts. Comme f est un morphisme de groupes, $f(a\mathbf{Z})$ est un sous-groupe de $(G,*)$, pour tout $a\in\mathbf{N}$. Comme l'application f est injective, les sous-groupes $f(a\mathbf{Z})$, où $a\in\mathbf{N}$, de $(G,*)$ sont deux-à-deux distincts. Ceci contredit l'hypothèse faite sur le groupe $(G,*)$. ∎

Soient $g_1,g_2,\dots,g_r$ des éléments de G tels que $\langle g_1\rangle,\langle g_2\rangle,\dots,\langle g_r\rangle$ est une liste exhaustive, sans répétition, de tous les sous-groupes cycliques de G.

Q14. — Démontrer que :

$$\forall\, g\in G,\quad \exists\, i\in[\![1,r]\!],\quad \exists\, k\in\mathbf{N},\quad g=g_i^k.$$

Considérons le sous-groupe $\langle g\rangle$ engendré par g. Il est par définition monogène et, comme G est fini, il est également fini. Donc $\langle g\rangle$ est un sous-groupe cyclique de $(G,*)$. Aussi existe-t-il $i\in[\![1,r]\!]$ tel que :

$$\langle g\rangle=\langle g_i\rangle=\left\{g_i^k\ :\ k\in\mathbf{Z}\right\}.$$

Comme $g\in\langle g\rangle=\{g_i^k\ :\ k\in\mathbf{Z}\}$, il existe $k\in\mathbf{Z}$ tel que $g=g_i^k$.

• Remarque. Le groupe $\langle g_i\rangle$ est fini, possède $\mathrm{ord}\,(g_i)$ éléments et :

$$\langle g_i\rangle=\left\{g_i^k\ :\ k\in[\![0,\mathrm{ord}\,(g_i)-1]\!]\right\}$$

L'entier k obtenu précédemment peut donc être choisi dans $[\![0,\mathrm{ord}\,(g_i)-1]\!]$. ∎

Q15. — En déduire que G est fini et que :

$$\mathrm{Card}\,(G)\leqslant\sum_{i=1}^{r}\mathrm{ord}\,(g_i).$$

Nous rappelons que pour tout $i \in [\![1, r]\!]$, le groupe $\langle g_i \rangle$ est fini et possède $\text{ord}(g_i)$ éléments. Observons :

$$(\star) \qquad G = \bigcup_{i=1}^{r} \langle g_i \rangle \,.$$

L'inclusion $\supset$ est claire et l'inclusion $\subset$ résulte de la question précédente. Notons que la réunion $\bigcup_{i=1}^{r} \langle g_i \rangle$ n'est pas disjointe (le neutre de G appartient à tout sous-groupe). L'ensemble G est fini, puisque égal à une réunion finie d'ensembles finis. Alors de $(\star)$, nous déduisons :

$$\text{Card}(G) \leqslant \sum_{i=1}^{r} \text{Card}\left(\langle g_i \rangle\right) = \sum_{i=1}^{r} \text{ord}\left(g_i\right) \,.$$

■

§ 6. UN CORPS DE RUPTURE DU POLYNÔME $X^3 - X - 1$

Q16. — Démontrer que le polynôme $X^3 - X - 1$ possède une unique racine réelle α.

• Introduction de la fonction polynomiale associée. La fonction :

$$f \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^3 - x - 1 \end{array} \right.$$

est dérivable sur $\mathbf{R}$ et :

$$\forall\, x \in \mathbf{R}, \quad f'(x) = 3x^2 - 1 = 3\left(x - \frac{1}{\sqrt{3}}\right)\left(x + \frac{1}{\sqrt{3}}\right).$$

• Étude sur $\left]-\infty, -\frac{1}{\sqrt{3}}\right]$. La fonction f est continue sur $\left]-\infty, -\frac{1}{\sqrt{3}}\right]$ et dérivable à dérivée strictement positive sur $\left]-\infty, -\frac{1}{\sqrt{3}}\right[$. Elle induit donc une bijection de $\left]-\infty, -\frac{1}{\sqrt{3}}\right]$ sur :

$$\left] \lim_{x \to -\infty} f(x) \,,\, f\left(-\frac{1}{\sqrt{3}}\right)\right] = \left]-\infty, \frac{2}{3\sqrt{3}} - 1\right].$$

Le polynôme $X^3 - X - 1$ ne possède donc aucune racine dans $\left]-\infty, -\frac{1}{\sqrt{3}}\right]$.

• Étude sur $\left]-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right[$. La fonction f est dérivable à dérivée strictement négative sur $\left]-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right[$. Elle induit donc une bijection de $\left]-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right[$ sur :

$$\left] \lim_{x \to -\frac{1}{\sqrt{3}}} f(x) \,,\, \lim_{x \to \frac{1}{\sqrt{3}}} f(x) \right[= \left]-\frac{2}{3\sqrt{3}} - 1 \,,\, \frac{2}{3\sqrt{3}} - 1\right[.$$

Le polynôme $X^3 - X - 1$ ne possède donc aucune racine dans $\left]-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right[$.

• Étude sur $\left[\frac{1}{\sqrt{3}}, +\infty\right[$. La fonction f est continue sur $\left[\frac{1}{\sqrt{3}}, +\infty\right[$ et dérivable à dérivée strictement positive sur $\left]\frac{1}{\sqrt{3}}, +\infty\right[$. Elle induit donc une bijection de $\left[\frac{1}{\sqrt{3}}, +\infty\right[$ sur :

$$\left[f\left(\frac{1}{\sqrt{3}}\right) \,,\, \lim_{x \to +\infty} f(x) \right[= \left[-\frac{2}{3\sqrt{3}} \,,\, +\infty\right[.$$

Le polynôme $X^3 - X - 1$ possède donc une unique racine sur $\left]-\infty, -\frac{1}{\sqrt{3}}\right]$.

• Conclusion. Comme :

$$\mathbf{R} = \left]-\infty, -\frac{1}{\sqrt{3}}\right] \bigsqcup \left]-\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right[\bigsqcup \left[-\frac{2}{3\sqrt{3}}, +\infty\right[$$

nous déduisons de ce qui précède que le polynôme $X^3 - X - 1$ possède une unique racine sur $\mathbf{R}$, qui est strictement plus grande que $\frac{1}{\sqrt{3}}$. ■

Q17. — Donner une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}[\alpha] := \mathrm{Vect}_{\mathbf{Q}}\left(\left(\alpha^k\right)_{k\in\mathbf{N}}\right)$.

• La famille $(1, \alpha)$ engendre $\mathbf{Q}[\alpha]$. Soit $x \in \mathbf{Q}[\alpha]$. Alors il existe $d \in \mathbf{N}$ et $(q_0, \ldots, q_d) \in \mathbf{Q}^{d+1}$ tel que :

$$x = \sum_{i=0}^{d} q_i \cdot \alpha^i.$$

Considérons la division euclidienne du polynôme $P := \sum_{i=0}^{d} q_i \cdot X^i$ par le polynôme $X^3 - X - 1$:

$$(\star) \qquad P = \left(X^3 - X - 1\right) Q + (a_0 + a_1 X)$$

où $Q \in \mathbf{Q}[X]$ et $(a_0, a_1) \in \mathbf{Q}^2$. En évaluant $(\star)$ en $X \leftarrow \alpha$, il vient :

$$x = P(\alpha) = \left(\alpha^3 - \alpha - 1\right) Q(\alpha) + a_0 + a_1\alpha = a_0 + a_1\alpha \in \mathrm{Vect}_{\mathbf{Q}}(1, \alpha).$$

Nous en déduisons que $\mathbf{Q}[\alpha] \subset \mathrm{Vect}_{\mathbf{Q}}(1, \alpha)$. L'inclusion réciproque est évidente, d'où :

$$\mathbf{Q}[\alpha] = \mathrm{Vect}_{\mathbf{Q}}(1, \alpha).$$

• La famille $(1, \alpha)$ est libre sur $\mathbf{Q}$. Raisonnons par l'absurde et supposons la famille $(1, \alpha)$ est liée sur $\mathbf{Q}$. Alors $\alpha \in \mathbf{Q}$. En écrivant $\alpha = \frac{p}{q}$, où $p \in \mathbf{Z}$ et $q \in \mathbf{N}^*$ sont premiers entre eux, il vient :

$$\left(\frac{p}{q}\right)^3 - \frac{p}{q} - 1 = 0$$

puis :

$$p^3 - pq^2 - q^3 = 0.$$

Avec le lemme de Gauß, il vient $p \mid q$ et $q \mid p$. Par suite $\alpha = 1$ ou $\alpha = -1$, ce qui n'est pas.

• Conclusion. La famille $(1, \alpha)$ est une base de $\mathbf{Q}[\alpha]$ sur $\mathbf{Q}$. ■

Q18. — Démontrer que $\mathbf{Q}[\alpha]$ est un sous-corps de $\mathbf{R}$.

• Premières propriétés de $\mathbf{Q}[\alpha]$. Il est clair que $\mathbf{Q}[\alpha]$ contient $0, 1$ et est stable par somme et produit (il s'agit de la sous-$\mathbf{Q}$-algèbre de $\mathbf{R}$ engendrée par α).

• Tout élément non nul de $\mathbf{Q}[\alpha]$ est inversible. Soit $x \in \mathbf{Q}[\alpha] \setminus \{0\}$. Comme $\mathbf{Q}[\alpha]$ est intègre (puisque incluse dans $\mathbf{R}$ intègre), l'application :

$$\mu_x \left| \begin{array}{ccc} \mathbf{Q}[\alpha] & \longrightarrow & \mathbf{Q}[\alpha] \\ y & \longmapsto & xy \end{array} \right.$$

est injective. Comme $\mathbf{Q}[\alpha]$ est un $\mathbf{Q}$-espace de dimension finie (égale à 2), l'application μ_x est surjective. L'élément 1 possède donc un antécédent par μ_x, i.e. l'élément x est inversible. ■

§ 7. Conditions suffisantes pour qu'un anneau intègre soit un corps

Soit $(A, +, \times)$ *un anneau commutatif intègre.*

Q19. — Démontrer que, si A est fini, alors $(A, +, \times)$ est un corps.

Il nous faut établir que tout élément non nul de A est inversible. Soit $a \in A \setminus \{0_A\}$. Comme A est intègre, l'application :

$$\mu_a \left| \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array} \right.$$

est injective. Comme A est fini, l'application μ_A est surjective. L'élément 1_A possède donc un antécédent par μ_a, i.e. l'élément a est inversible. ■

Q20. — Démontrer que, si A ne possède qu'un nombre fini d'idéaux, alors $(A, +, \times)$ est un corps.

Il nous faut établir que tout élément non nul de A est inversible. Soit $a \in A \setminus \{0_A\}$. Pour tout $n \in N^*$:

$$(a^n) := \left\{a^n x \ : \ x \in A\right\}$$

est un idéal de A (idéal engendré par a^n). Comme A ne possède qu'un nombre fini d'idéaux, il existe deux entiers n et m tels que :

$$1 \leqslant n < m \qquad \text{et} \qquad (a^n) = (a^m).$$

Puisque $a^n \in (a^n) = (a^m)$, il existe $x \in A$ tel que :

$$a^n = a^m b = a^n a^{m-n} b.$$

Comme A est intègre et $a \neq 0_A$, $a^n \neq 0_A$ et :

$$1_A = a^{m-n} b.$$

■