

**AGRÉGATION INTERNE, 2013-2014**  
**3 JUILLET 2013**  
**IDÉAUX, ANNEAUX DE POLYNÔMES ET NOMBRES**  
**ALGÈBRIQUES**

P. EYSSIDIEUX

ÉNONCÉ

Si  $\mathbb{A}$  désigne un anneau commutatif unitaire, on note :

- 0 et 1 les éléments neutres pour l'addition et la multiplication de  $\mathbb{A}$ , avec  $0 \neq 1$ ;
- $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$  ;
- $\mathbb{A}^\times$  le groupe des éléments inversibles (on dit aussi des unités) de  $\mathbb{A}$ .

On rappelle que :

- $\mathbb{A}$  est intègre s'il est commutatif, unitaire et n'admet pas de diviseur de 0, c'est-à-dire que pour  $a, b$  dans  $\mathbb{A}$ , on a :

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0$$

- Un idéal de  $\mathbb{A}$  est un sous groupe  $I \subset \mathbb{A}$  du groupe  $(\mathbb{A}, +)$  tel que

$$\forall a \in \mathbb{A} \forall x \in I, a \cdot x \in I;$$

- Un idéal  $I \subsetneq \mathbb{A}$  est premier si et seulement si  $x \cdot y \in I$  implique  $x \in I$  ou  $y \in I$ .
- Un idéal  $I \subsetneq \mathbb{A}$  est maximal si et seulement si tout idéal  $J$  contenant  $I$  est  $I$  ou  $\mathbb{A}$ .
- Un idéal  $I \subset \mathbb{A}$  est principal si et seulement s'il est de la forme  $I = a \cdot \mathbb{A}$  où  $a \in \mathbb{A}$ . Un tel élément  $a$ , s'il existe, est appelé un générateur de  $I$ .
- un élément  $p$  de  $\mathbb{A}$  est irréductible si  $p \neq 0$ ,  $p$  n'est pas inversible et :

$$(p = uv) \Rightarrow (u \text{ ou } v \text{ est inversible})$$

(les seuls diviseurs de  $p$  sont les éléments inversibles ou les éléments de  $\mathbb{A}$  associés à  $p$ ) ;

- un élément  $p$  de  $\mathbb{A}$ , est premier si  $p \neq 0$ ,  $p$  n'est pas inversible et :

$$(p \text{ divise } uv) \Rightarrow (p \text{ divise } u \text{ ou } p \text{ divise } v)$$

**– I – Généralités sur les idéaux d'un anneau**

Dans cette partie  $\mathbb{A}$  désigne un anneau, non nécessairement intègre.

- (1) Montrer que l'idéal nul  $I = \{0\}$  est premier si et seulement si  $\mathbb{A}$  est intègre.
- (2) Montrer qu'un idéal  $I \subset \mathbb{A}$  est égal à  $\mathbb{A}$  si et seulement si  $1 \in I$  si et seulement si  $I \cap \mathbb{A}^\times \neq \emptyset$ .

- (3) Montrer que  $a.\mathbb{A} \subset b.\mathbb{A}$  si et seulement si  $b$  divise  $a$ .
- (4) Montrer qu'un idéal principal non nul  $I = a.\mathbb{A}$  est premier si et seulement si  $a$  est un élément premier de  $\mathbb{A}$ .
- (5) Montrer que le noyau d'un morphisme d'anneaux est un idéal.
- (6) Montrer que l'on définit sur l'ensemble  $\mathcal{P}(\mathbb{A})$  des parties de  $\mathbb{A}$  une loi de composition interne associative  $\oplus$  par la formule suivante,  $X, Y$  étant deux parties de  $\mathbb{A}$ :

$$X \oplus Y = \{z \in \mathbb{A}, \exists x \in X \exists y \in Y z = x + y\}$$

- (7) Pour  $I$  un sous groupe de  $(\mathbb{A}, +)$  on considère l'ensemble  $E$  formé des parties de  $\mathbb{A}$  de la forme  $\{a\} + I$  où  $a \in \mathbb{A}$ . Montrer que la loi  $\oplus$  laisse  $E$  stable et que  $(E, \oplus)$  est un groupe abélien dont on précisera l'élément neutre.
- (8) Montrer que l'application naturelle  $\pi : (\mathbb{A} \rightarrow (E, \oplus), a \mapsto \{a\} + I)$  est un morphisme surjectif de groupes de noyau  $I$ .
- (9) Montrer que  $E$  est l'ensemble quotient de  $\mathbb{A}$  par la relation d'équivalence  $x \sim_I y$  définie par  $x \sim_I y$  si et seulement si  $x - y \in I$ .
- (10) Supposons que  $I$  est un idéal. Montrer qu'il existe une unique loi associative  $\odot$  sur  $E$  tel que  $\pi$  soit un morphisme d'anneaux.
- (11) On note  $\mathbb{A}/I := (E, \oplus, \odot)$  l'anneau quotient de  $\mathbb{A}$  par  $I$  et  $\pi : \mathbb{A} \rightarrow \mathbb{A}/I$  le morphisme surjectif d'anneaux des questions I-8,10. Montrer qu'un morphisme d'anneaux  $\phi : \mathbb{A} \rightarrow \mathbb{B}$  vérifie  $\phi = \bar{\phi} \circ \pi$  où  $\bar{\phi} : \mathbb{A}/I \rightarrow \mathbb{B}$  est un morphisme d'anneaux si et seulement si  $\phi(I) = \{0\}$ .
- (12) Montrer que  $\mathbb{A}/I$  est intègre si et seulement si  $I$  est premier.

## – II – Idéaux et quotients de l'anneau $k[X]$

Soit  $k$  un corps et  $k[X]$  l'anneau de polynômes à coefficients dans  $k$ . Pour  $n \in \mathbb{N}$ , on note  $k[X]_{\leq n}$  l'ensemble des polynômes de degré inférieur ou égal à  $n$ .

- (1) Déterminer  $k[X]^\times$ .
- (2) Rappeler l'énoncé du théorème de division euclidienne dans  $k[X]$ .
- (3) Montrer que tout idéal  $I$  de  $k[X]$  est principal et admet un unique générateur de coefficient dominant 1, son *générateur normalisé*.
- (4) L'anneau  $k[X]/X^2k[X]$  est-il intègre?
- (5) Quels sont les idéaux premiers de  $k[X]$ ? Ses idéaux maximaux?
- (6) On munit  $k^k$  l'ensemble des fonctions de  $k$  vers  $k$  de sa structure d'anneau naturelle. Montrer que l'application  $\rho : k[X] \rightarrow k^k$  qui à  $P \in k[X]$  associe la fonction polynôme ( $x \mapsto P(x)$ ) est un morphisme d'anneau.
- (7) Montrer que  $\rho$  est injective si et seulement si  $k$  est infini. Si  $k$  est fini, quel est le générateur normalisé (au sens de II-3) de  $\ker(\rho)$ ?
- (8) Montrer que  $k^k$  n'est jamais intègre et en déduire que si  $k$  est infini  $\rho$  n'est pas surjective.
- (9) Montrer que si  $k$  est fini de cardinal  $q$ ,  $\rho$  est surjective. Indication: déterminer  $\rho(1 - X^{q-1})$ .
- (10) Si  $P, Q \in k[X]$  sont premiers entre eux, exhiber un isomorphisme d'anneaux de  $k[X]/P \cdot Qk[X]$  sur  $k[X]/Pk[X] \times k[X]/Qk[X]$ .

- (11) Soit  $P \in k[X]$  tel que  $\deg(P) = d \in \mathbb{N}$ . Montrer que l'application  $r_P : k[X] \rightarrow k[X]_{\leq d-1}$  qui à  $Q \in k[X]$  associe le reste de la division euclidienne de  $Q$  par  $P$  factorise par  $\pi : k[X] \rightarrow k[X]/Pk[X]$ , c'est à dire qu'il existe une application

$$\bar{r}_P : k[X]/Pk[X] \rightarrow k[X]_{d-1}$$

telle que  $\bar{r}_P \circ \pi = r_P$ .

- (12) Décrire l'unique structure de  $k$ -espace vectoriel sur  $k[X]/Pk[X]$  telle que  $\pi : k[X] \rightarrow k[X]/Pk[X]$  est une application  $k$ -linéaire.  
 (13) Montrer que  $\bar{r}_P$  est un isomorphisme de  $k$ -espaces vectoriels et déduire que  $k[X]/Pk[X]$  est un  $k$ -espace vectoriel de dimension  $d$ .

### – III – Éléments algébriques d'une extension de corps.

Soit  $K$  un corps et  $k$  un sous-corps de  $K$ . Un élément  $\alpha$  de  $K$  est dit algébrique sur  $k$  si et seulement si il existe  $P \in K[X]^*$  tel que  $P(\alpha) = 0$ . Dans le cas contraire on dit que  $\alpha$  est transcendant sur  $k$ .

- (1) Soit  $\alpha \in K$ . Montrer qu'il existe un unique morphisme d'anneaux  $\phi_\alpha$  de  $k[X]$  dans  $K$  tel que  $\phi_\alpha(X) = \alpha$  et  $\phi_\alpha|_k = \text{id}_k$ .  
 (2) Montrer que  $\alpha$  est transcendant si et seulement si  $\phi_\alpha$  est injectif.  
 (3) On suppose pour cette question seulement que  $K = k(X)$  le corps des fractions rationnelles de  $k$ . Montrer que  $X \in k(X)$  est transcendant sur  $k$ .  
 (4) Soit  $\alpha \in K$  un élément algébrique sur  $k$ . Montrer que l'ensemble

$$I_\alpha := \{P \in k[X], P(\alpha) = 0\}$$

est un idéal. Le générateur normalisé de  $I_\alpha$  se note  $\pi_\alpha$  et s'appelle le *polynôme minimal* de  $\alpha$ . Le *degré* de  $\alpha$  sur  $k$  est l'entier naturel  $\deg_k(\alpha) = \deg(\pi_\alpha)$ .

- (5) Montrer que  $k$  est l'ensemble des éléments de  $K$  de degré 1 sur  $k$ .  
 (6) Dans cette question seulement  $k = \mathbb{R}$ ,  $K = \mathbb{C}$ . Quel est le degré sur  $\mathbb{R}$  de  $z \in \mathbb{C} - \mathbb{R}$ ?  
 (7) Soit  $\alpha \in K$  un élément algébrique sur  $k$ . Montrer que  $\pi_\alpha$  est irréductible (Indication: on pourra utiliser I-12 II-5).  
 (8) Montrer l'équivalence des assertions suivantes:  
 (a)  $\alpha \in K$  est algébrique sur  $k$   
 (b) Le  $k$ -sous espace vectoriel de  $K$  engendré par  $1, \alpha, \alpha^2, \dots$  est de dimension finie.  
 (c)  $\alpha$  est contenu dans un sous corps  $L$  de  $K$  tel que  $L$  est un  $k$ -espace vectoriel de dimension finie.

Soit  $\alpha \in K$  un élément algébrique sur  $k$ . Décrire le plus petit sous-corps  $k(\alpha)$  de  $K$  contenant  $k$  et  $\alpha$  et donner sa dimension comme  $k$ -espace vectoriel.

- (9) Soit  $L$  un sous corps de  $K$  contenant  $k$  et tel que  $L$  soit comme  $k$ -espace vectoriel de dimension finie. Soit  $\alpha \in K$  tel que  $\alpha$  soit algébrique sur  $L$ . Montrer que  $\alpha$  est algébrique sur  $k$  et que  $\deg_k(\alpha) \leq \deg_L(\alpha) \dim_k(L)$ .  
 (10) Soient  $\alpha, \beta$  deux éléments de  $K$  algébriques sur  $k$ . Montrer que  $\alpha + \beta$  et  $\alpha\beta$  sont algébriques sur  $k$ .

- (11) Montrer que l'ensemble  $k_K^{alg} \subset K$  des éléments de  $K$  algébriques sur  $k$  est un sous-corps contenant  $k$  et que tout élément algébrique sur  $k_K^{alg}$  est algébrique sur  $k$ .

– IV – Nombres algébriques.

On spécialise les notations de la partie III, en supposant désormais que  $k = \mathbb{Q}$ ,  $K = \mathbb{C}$  et on note  $\bar{\mathbb{Q}} = \mathbb{Q}_{\mathbb{C}}^{alg}$ . Les éléments de  $\bar{\mathbb{Q}}$  sont appelés les nombres algébriques.

- (1) Montrer que  $\bar{\mathbb{Q}}$  est un corps algébriquement clos.
- (2) Montrer  $\bar{\mathbb{Q}}$  est dénombrable et déduire qu'il existe des nombres réels transcendants (sur  $\mathbb{Q}$ ).
- (3) Soit  $b \in \mathbb{Q}$  avec  $b > 0$  tel que  $b$  n'est pas un carré dans  $\mathbb{Q}$ . Montrer que  $\sqrt{b} \in \mathbb{R}$  est algébrique sur  $\mathbb{Q}$  de degré 2. Donner un exemple d'un tel nombre  $b$ .
- (4) Montrer que si  $\alpha \in \mathbb{R}$  est algébrique de degré 2 sur  $\mathbb{Q}$ , il existe un rationnel  $b \in \mathbb{Q}$  avec  $b > 0$  tel que  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b})$ .
- (5) On considère la suite de polynômes  $(P_n)_{n \in \mathbb{N}}$  définie par  $P_0 = 1$ ,  $P_1 = 2X$  et

$$P_{n+2} = 2XP_{n+1} - P_n.$$

On pose  $Q_n(X) = P_n(X/2)$ .

- (a) Déterminer le degré, le coefficient dominant, le terme constant et la parité de  $P_n$ .
- (b) Déterminer  $P_n$  pour  $n = 2, 3, 4$ .
- (c) Montrer que  $Q_n \in \mathbb{Z}[X]$ .
- (d) Montrer que les seules racines rationnelles possibles pour  $Q_n$  sont  $0, \pm 1$ .
- (e) Exprimer  $Q_{n+3} + XQ_n$  en fonction de  $Q_{n+1}$ . Déduire que les racines rationnelles non nulles de  $Q_{n+3}$  et de  $Q_n$  sont les mêmes. Préciser les  $P_n$  ayant une racine rationnelle.
- (6) Soit  $\theta \in \mathbb{R}$ . On considère la suite  $(u_n)_{n \in \mathbb{N}}$  définie par la donnée de  $u_0$  et  $u_1$  et la relation de récurrence :

$$u_{n+2} = 2 \cos(\theta)u_{n+1} - u_n.$$

- (a) Déterminer l'expression du terme général de la suite  $(u_n)$ .
- (b) Utiliser les résultats précédents pour exprimer  $P_n(\cos(\theta))$  en fonction de  $n, \theta$ . En déduire les racines  $x_{k,n}$  de  $P_n$  ( $1 \leq k \leq n$ ).
- (c) Montrer que  $\cos(\frac{2\pi}{5}), \cos(\frac{2\pi}{7})$  sont des nombres algébriques. Déterminer le polynôme minimal de  $\cos(\frac{2\pi}{5})$ .

– V – Constructibilité à la règle et au compas.

Soit  $\mathcal{P}$  le plan euclidien rapporté à un repère cartésien  $Oxy$  orthonormé direct. Soit  $S$  un ensemble de points de  $\mathcal{P}$ . Considérons toutes les droites joignant deux points de  $S$  et tous les cercles centrés en un point de  $S$  dont le rayon est la distance entre deux points de  $S$  et appelons les droites et cercles constructibles à partir de  $S$ . On note  $C_1(S)$  l'ensemble de points de  $\mathcal{P}$  formé de  $S$  et des points d'intersections de ces droites et cercles. On pose  $C_{n+1}(S) = C_1(C_n(S))$  et  $C_{\infty}(S) = \bigcup_{n \in \mathbb{N}} C_n(S)$ .

On dit que  $P \in \mathcal{P}$  est *constructible* (sous entendu “à la règle et au compas”) à partir de  $S$  ssi  $P \in C_\infty(S)$ . On dit que  $P \in \mathcal{P}$  est *constructible* s’il est *constructible* à partir de  $S = \{(0, 0); (1, 0)\}$ .

- (1) Montrer que  $(-1, 0)$ ,  $(0, 1)$  et  $(1, 1)$  sont constructibles.
- (2) Montrer que si  $(x, y)$  est constructible  $(y, x)$  l’est aussi.
- (3) Un réel est dit *constructible* si  $(x, 0)$  est constructible. Montrer qu’un point de  $\mathcal{P}$  est constructible si et seulement si son abscisse et son ordonnée sont des réels constructibles.
- (4) Supposons que  $S$  soit constitué de points à coordonnées dans le sous corps  $L$  de  $\mathbb{R}$ .
  - (a) Montrer que les droites et cercles constructibles à partir de  $S$  ont une équation de degré 2 à coefficients dans  $L$ .
  - (b) Montrer que les coordonnées d’un point de  $C_1(S)$  sont soit dans  $L$  soit de degré 2 sur  $L$ .
- (5) Une suite finie  $(K_i)_{i=0, \dots, p}$  de sous corps de  $\mathbb{R}$  est une *tour d’extension quadratiques* si  $K_0 = \mathbb{Q}$ ;  $K_i \subset K_{i+1}$  et  $\dim_{K_i} K_{i+1} = 2$ . Montrer que, pour tout réel constructible  $x$ , il existe une tour d’extensions quadratiques  $(K_i)_{i=0, \dots, p}$  telles que  $x \in K_p$ .
- (6) Montrer que la somme et la différence de deux réels constructibles est constructible.
- (7) Montrer que le produit de deux réels constructibles est constructible. Indication: on pourra utiliser le Théorème de Menelaüs. Soit  $(A, B, C)$  un triangle non dégénéré de  $\mathcal{P}$ . Soient  $D$  un point de la droite  $(B, C)$   $E$ , un point de  $(A, C)$ , resp.  $F$  un point de  $(A, B)$ . Alors  $(D, E, F)$  sont alignés ssi:

$$\frac{\overline{DB}}{\overline{DC}} \cdot \frac{\overline{EC}}{\overline{EA}} \cdot \frac{\overline{FA}}{\overline{FB}} = 1.$$

- (8) Montrer que l’ensemble des réels constructibles est un sous-corps de  $\overline{\mathbb{Q}} \cap \mathbb{R}$ .
- (9) Montrer que si  $\alpha$  est un réel positif constructible  $\sqrt{\alpha}$  est encore constructible. Indication: on pourra considérer le cercle dont un diamètre est le segment  $[(-1, 0), (\alpha, 0)]$ .
- (10) Soit  $(K_i)_{i=0, \dots, p}$  une tour d’extensions quadratiques. Montrer que les éléments de  $K_p$  sont constructibles, c’est à dire que V-5 est une condition nécessaire et suffisante de constructibilité.
- (11) Montrer que le degré d’un réel constructible est une puissance de 2.
- (12) Montrer que  $\sqrt[3]{2}$  n’est pas constructible. Pourquoi les mathématiciens grecs ne surent répondre à la demande de la Pythie de Delphes de donner la construction d’un autel deux fois plus grand que celui du temple d’Appolon?
- (13) Le pentagone régulier inscrit dans le cercle unité est composé des points  $(\cos(\frac{2k\pi}{5}), \sin(\frac{2k\pi}{5}))$ ,  $k = 0, \dots, 4$ . Montrer que ses sommets sont constructibles.
- (14) On se propose de montrer qu’il existe des réels algébriques de degré 4 sur  $\mathbb{Q}$  qui ne sont pas constructibles. On considère pour cela  $P = X^4 - 4X + 2$ .
  - (a) Montrer que  $P$  a deux racines réelles  $r_1, r_2$  qui sont irrationnelles.

- (b) Factorisant  $P$  dans  $\mathbb{R}[X]$  sous la forme  $P = (X^2 + aX + b)(X^2 + cX + d)$  montrer que  $t = b + d$  vérifie  $t^3 + 8t - 16 = 0$ .
- (c) Déterminer  $\deg_{\mathbb{Q}}(t)$ .
- (d) Prouver que  $P$  est irréductible sur  $\mathbb{Q}$  et déterminer le degré de  $r_1$  et  $r_2$  sur  $\mathbb{Q}$ .
- (e) Montrer que l'un des  $r_i$  au moins n'est pas constructible.

**Remarque.** La construction à la règle et au compas du pentagone régulier n'est pas tout à fait évidente. On a pu déterminer les polygones réguliers constructibles à la règle et au compas. Le nombre de cotés doit être  $2^p F_1 \dots F_k$  où les  $F_i$  sont des nombres de Fermat premiers distincts. Ainsi les polygones à 17, 257 et 65537 côtés sont constructibles. La construction à la règle et au compas du polygone régulier à 65537 côtés est réputée appartenir au musée des horreurs mathématiques.