Exercices sur les anneaux
Agrégation externe 2015

N. Bédaride

Table des matières

1 Anneaux et corps

1.1 Généralités

Exercice 1.

1. *Soit* $D = \{f \in \mathbb{R}[X] : f'(0) = 0\}$. *Montrer que* D *n'est pas un idéal de l'anneau* $\mathbb{R}[X]$ *et que c'est un sous-anneau de l'anneau* $\mathbb{R}[X]$.
2. *Soit* $E = \{f \in \mathbb{R}[X] : f(0) = f'(0) = 0\}$. *Montrer que* D *n'est pas un sous-anneau de l'anneau* $\mathbb{R}[X]$ *et que c'est un idéal de l'anneau* $\mathbb{R}[X]$ *dont on donnera un générateur.*

Exercice 2. ✠✠ *On considère l'anneau des fonctions holomorphes sur* $\mathbb{C}$.

1. *Montrer qu'il est intègre. On utilisera que les zéros d'une fonction holomorphe non nulle sont sans point d'accumulation.*
2. *Caractériser les éléments irréductibles.*
3. *Montrer qu'il n'est pas factoriel.*

Exercice 3. □ *On définit* $A = \{a + jb : a, b \in \mathbb{Z}\}$ *où* $j = \exp(\frac{2i\pi}{3})$.

1. *Montrer que* A *est un sous-anneau de* $\mathbb{C}$. *On désigne par* $\mathcal{U}(A)$ *le groupe des éléments inversibles de* A *et enfin, on pose, pour tout* $z \in \mathbb{C}$, $N(z) = |z|^2$.
2. *(a) Montrer que si* $z \in A$ *alors* $N(z) \in \mathbb{Z}$.

(b) *Soit $z \in A$. Montrer que $z \in \mathcal{U}(A)$ si et seulement si $N(z) = 1$.*

(c) *Soient a et b des entiers. Montrer que si $N(a + jb) = 1$ alors $a, b \in \{-1, 0, 1\}$.*

3. *Décrire le groupe $\mathcal{U}(A)$ et en déterminer les éléments d'ordre 3.*
4. *Soit $\Phi : \mathbb{Q}[X] \to \mathbb{C}, P \mapsto P(j)$.*

(a) *Montrer que Φ est un morphisme d'anneaux.*

(b) *Déterminer le noyau de Φ (on pourra remarquer que $j^2 + j + 1 = 0$).*

(c) *Montrer que $Im\,\Phi = \{a + jb : a, b \in \mathbb{Q}\}$ et que c'est un sous-corps de $\mathbb{C}$.*

5. *Conclure que A est isomorphe à $\mathbb{Z}[X]/(X^2 + X + 1)$.*

Exercice 4. *Soit A un anneau commutatif et I un idéal de A.*
On note $\sqrt{I} = \{x \in A \text{ tq } \exists\, n \in \mathbb{N} \text{ tq } x^n \in I\}$ (radical de I).

1. *Montrer que $\sqrt{I}$ est un idéal de A.*
2. *Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.*
3. *Montrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I + J} \supset \sqrt{I} + \sqrt{J}$.*
4. *Exemple : $A = \mathbb{Z}$, $I = 3648\mathbb{Z}$. Trouver $\sqrt{I}$.*

Exercice 5. *Soit A un anneau . Un élément $a \in A$ est dit nilpotent s'il existe un entier n non nul tel que $a^n = 0$.*

1. *Montrer que si a est nilpotent, alors $1 - a$ est inversible.*
2. *Montrer que l'ensemble des nilpotents forme un idéal si A est commutatif, noté $Nil(A)$.*
3. *Montrer qu'il est contenu dans tout idéal premier.*
4. *Calculer $Nil(A)$ si $A = \mathbb{Z}/100\mathbb{Z}$.*

Exercice 6. *Soit A un anneau intègre. Un idéal I est dit maximal si $I \subset J$ avec J idéal implique que $J = A$.*

1. *Déterminer les idéaux maximaux de $\mathbb{Z}$ puis de $\mathbb{R}[X]$.*
2. *Montrer que I est maximal si et seulement si A/I est un corps.*

1.2 Anneaux classiques

Exercice 7. *On considère l'ensemble*

$$\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$$

1. *Montrer que c'est un anneau intègre.*
2. *Montrer que $z \mapsto \overline{z} = a - ib$ est un automorphisme d'anneaux.*
3. *Montrer que $z \mapsto N(z) = z\overline{z}$ est multiplicative.*
4. *Trouver $\mathbb{Z}[i]^*$.*

5. *Montrer que l'anneau est euclidien relativement à N. On utilisera la notion d'entier le plus proche d'un réel.*

Exercice 8. □ *On considère l'ensemble*

$$\Sigma = \{n \in \mathbb{N} | n = a^2 + b^2; a, b \in \mathbb{N}\}$$

1. *Montrer que si $n = 3 \mod 4$ alors n n'appartient pas à Σ.*
2. *Montrer que l'ensemble Σ est stable par multiplication.*
3. *En déduire qu'il suffit de caractériser les $p \in \Sigma$ avec p nombre premier.*
4. *Montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.*
5. *Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2+1)$.*
6. *En déduire que $p \in \Sigma$ si et seulement si -1 est un carré de $\mathbb{F}_p$.*

Exercice 9. ✠ *Le but est de montrer que -1 est un carré de $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p = 1 \mod 4$. Soit F^2 l'ensemble des éléments de $\mathbb{F}_p^*$ qui s'écrivent comme carré d'un élément.*

1. *Montrer que $x \in F^2 \iff x^{(p-1)/2} = 1$:*
   (a) *Considérer $x \mapsto x^2$. Montrer que c'est un morphisme et calculer son noyau.*
   (b) *Conclure par un argument de cardinalité.*
2. *En déduire le résultat.*

Exercice 10. ✠ *On considère l'ensemble $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. On pose $\alpha = \frac{1+i\sqrt{19}}{2}$ et $N(z) = z\overline{z}$.*

1. *Montrer que $\alpha^2 = \alpha - 5$.*
2. *Montrer que la norme N est multiplicative.*
3. *Si $z = a + b\alpha$ avec a, b entiers, montrer que $N(z) = a^2 + ab + 5b^2$.*
4. *Montrer que z est inversible si et seulement si $N(z) = 1$. En déduire A^*.*
5. *Montrer que si L est un anneau euclidien alors il existe x non inversible tel que la restriction à $L^* \cup \{0\}$ de la projection de L sur $L/(x)$ soit surjective. (On choisira x minimal pour la valuation parmi les non inversibles non nuls.)*
6. *Ici, que dire de $A/(x)$?*
7. *Montrer que A ne peut être euclidien en raisonnant par l'absurde.*

Exercice 11. ✠ *Avec les mêmes notations on va montrer que A est principal.*

1. *Montrer que $A/(2) \sim \mathbb{Z}[X]/(2, X^2 - X + 5) \sim (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1)$.*
2. *Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{Z}/2\mathbb{Z}[X]$.*
3. *En déduire que (2) est un idéal maximal.*
4. *Montrer que pour $a, b \in A$ non nuls il existe q, r tels que l'on ait*

— $r = 0$ *ou* $N(r) < N(b)$
— $a = bq + r$ *ou* $2a = bq + r$.

5. *Soit I un idéal et $x \in I$ un élément de valuation minimale. En utilisant les questions précédentes conclure que I est principal.*

Exercice 12. *On considère l'anneau $\mathbb{Z}[i\sqrt{5}]$.*

1. *Montrer que les inversibles de cet anneau sont de la forme $a+ib\sqrt{5}$ avec $a^2+5b^2 = \pm 1$.*
2. *Montrer que 3 est irréductible.*
3. *Conclure que l'anneau n'est pas factoriel en choisissant le bon élément.*

1.3 Pgcd et arithmétique

Exercice 13. *Soit A un anneau principal et commutatif.*

1. *Montrer que a divise b si et seulement si $(b) \subset (a)$.*
2. *La relation a divise b définit elle un ordre sur A ?*

Exercice 14. *Soit A un anneau principal et commutatif.*

1. *Montrer que $(a) = (b)$ si et seulement si il existe $u \in A^*$ tel que $b = au$.*
2. *Soit $\delta \in A$, montrer l'équivalence entre $\delta = pgcd(a, b)$ et $d|\delta \iff d|a, d|b$.*

Exercice 15. *On considère $Z_2 = \{\frac{p}{q} \in \mathbb{Q}^*, q \text{ impair}\} \cup \{0\}$.*

1. *Montrer que c'est un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$.*
2. *Calculer Z_2^* et montrer que l'idéal $2Z_2$ est l'unique idéal maximal de Z_2.*
3. *Montrer que $Z_2/2Z_2 \sim \mathbb{F}_2$.*
4. *Soit x, y, z rationnels tels que $x^2 + y^2 + z^2 = 1$. Montrer que l'on a $x, y, z \in Z_2$.*

Exercice 16.

1. *Montrer que $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si les entiers k et n sont premiers entre eux.*
2. *On pose $n = 10$ et soit G le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.*
   (a) *Donner la liste des éléments de G.*
   (b) *Quel est l'ordre de $\overline{3}$? G est-il cyclique ?*

Exercice 17. *Soit l'anneau $A = \mathbb{Z}/91\mathbb{Z}$.*

1. *Déterminer les diviseurs de zéro de l'anneau A.*
2. *Résoudre dans A l'équation $x^2 + \overline{2}x - \overline{3} = \overline{0}$.*

Exercice 18 (Calendriers)**.** *On considère deux nombres a, b premiers entre eux et f l'isomorphisme entre $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. On prend $a = 8, b = 21$.*

1. *Écrire une relation de Bezout entre a, b.*
2. *Donner un multiple de a congru à 1 modulo 21.*

3. *Donner un multiple de b congru à 1 modulo 8.*
4. *Déduire une méthode pour trouver rapidement un antécédent quelconque par f d'un élément.*

Exercice 19. ✠*[RSA] Soient p, q deux nombres premiers, posons $N = pq$. Soient c, d deux entiers tels que*

$$cd = 1 \mod \varphi(N)$$

Alice veut envoyer un message à Bob. Le message est un élément $m \in \mathbb{Z}/N\mathbb{Z}$ et p, q sont cachés. Bob choisit p, q. Les entiers N, c sont rendus publics. Alice chiffre m en donnant $m^c \mod N$. Bob déchiffre y en donnant $y^d \mod N$.

1. *Si $x = m^c$, montrer que $x^d = m \mod N$ en utilisant le petit théorème de Fermat.*
2. *Pour $p = 7, q = 11, c = 13$ trouver un d qui convient.*
3. *La signature est la donnée de m^d. Si Alice donne sa clé publique (N, c) et la signature, expliquer comment Bob peut vérifier que le message crypté vient d'Alice ?*
4. *Supposons que Bob envoie m à deux personnes ayant des clés c_1, c_2 différentes et premières entre elles. On va montrer que la donnée de m^{c_1}, m^{c_2} permet de retrouver m :*
   (a) *Montrer que c_1 est inversible modulo c_2. Notons le b_1.*
   (b) *Considérons $b_2 = \frac{b_1 c_1 - 1}{c_2}$ modulo N et trouver une combinaison des chiffrements congrue à m modulo N.*
   (c) *Conclure.*

Exercice 20. □ *On considère des entiers $n_1, \ldots, n_k$ deux à deux premiers entre eux. Résoudre le système*

$$\begin{cases} x = a_1 \mod n_1 \\ \vdots \\ x = a_k \mod n_k \end{cases}$$

On posera $n = \prod_{i=1}^{k} n_i$ et $N_i = \frac{n}{n_i}$.

1. *Montrer que pour tout entier i les nombres n_i, N_i sont premiers entre eux. Ecrire la relation de Bezout.*
2. *En déduire qu'il existe des nombes $E_1, \ldots, E_k$ tels que $E_i = 1 \mod n_i, E_i = 0 \mod n_j$ si $j \neq i$.*
3. *Conclure qu'une solution vaut*

$$x = \sum_{i=1}^{k} a_i E_i.$$

Exercice 21. *Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois.*

Celui-ci recevrait alors trois pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier quatre pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors cinq pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Exercice 22. *On considère la fonction φ de $\mathbb{N}^*$ dans lui même définie par :*
$\varphi(n)$ est le nombre d'entiers naturels inférieurs à n et premiers avec lui.

1. *Si n est premier calculer $\varphi(n), \varphi(n^a)$ avec a entier.*
2. *Soient p, q entiers premiers entre eux, en étudiant un morphisme d'anneaux montrer que*
$$\varphi(pq) = \varphi(p)\varphi(q)$$
3. *Montrer que si $n \geq 3$ alors $\varphi(n)$ est pair.*
4. *Montrer que $\sum_{d|n} \varphi(d) = n$. Pour un diviseur de n on cherchera le nombre d'entiers $k \leq n$ tels que $\gcd(k, n) = d$.*

Exercice 23. $\square$ *Déterminer l'ensemble de tous les couples d'entiers (m, n) tels que*

$$955m + 183n = 1.$$

1.4 Corps

Exercice 24. *Soit E le $\mathbb{Q}$ espace vectoriel engendré par $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.*

1. *On considère l'endomorphisme de E donné par $f : x \mapsto (\sqrt{2}+\sqrt{3})x$. Écrire la matrice de f dans la base $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.*
2. *Calculer le polynôme caractéristique de f.*
3. *En utilisant le théorème de Cayley Hamilton en déduire un polynôme annulateur de $\sqrt{2} + \sqrt{3}$.*

Exercice 25. *Soit α un nombre algébrique.*

1. *Montrer qu'il existe un unique polynôme de $\mathbb{Q}[X]$ de degré minimal et de coefficient dominant 1 annulant α.*
2. *En déduire que si Q est un polynôme rationnel satisfaisant $Q(\alpha) \neq 0$ il existe un polynôme h de $\mathbb{Q}[X]$ tel que $\frac{1}{Q(\alpha)} = h(\alpha)$.*
3. *En déduire que $\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$ espace vectoriel de dimension finie.*

Exercice 26. *On considère le corps $\mathbb{K} = \mathbb{Q}(2^{1/3}, j)$.*

1. *Déterminer le degré de $\mathbb{K}$ sur $\mathbb{Q}$ et l'exprimer comme corps de décomposition d'un polynôme bien choisi.*
2. *Trouver tous les sous-corps de $\mathbb{K}$ ainsi que leurs degrés.*

2 Polynômes

2.1 Polynômes irréductibles, pgcd

Exercice 27. □ *Calculer le pgcd D des polynômes A et B définis ci-dessous dans $\mathbb{Z}[X]$. Trouver des polynômes U et V tels que $D = AU + BV$.*

1. $A = X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2$ *et* $B = X^4 + 2X^3 + 2X^2 + 7X + 6$.
2. $A = X^6 - 2X^5 + 2X^4 - 3X^3 + 3X^2 - 2X$ *et* $B = X^4 - 2X^3 + X^2 - X + 1$.

Exercice 28. *Trouver le pgcd dans $\mathbb{Z}/3\mathbb{Z}[X]$ puis dans $\mathbb{Z}/5\mathbb{Z}[X]$ de $f = X^4 + 1$, $g = X^3 + X + 1$.*

Exercice 29. *Montrer que f est irréductible dans $\mathbb{Q}[X]$ en utilisant le critère d'Eisenstein :*

1. $f = X^4 - 8X^3 + 12X^2 - 6X + 2$;
2. $f = X^5 - 12X^3 + 36X - 12$;
3. $f = X^4 - X^3 + 2X + 1$;
4. $f = X^{p-1} + \cdots + X + 1$, *où p est premier.*

Exercice 30. ✠ *Soit k un corps et P un polynôme sur k de degré n. Soit K un corps contenant k, tel que ce soit un espace vectoriel sur k de dimension m.*

1. *Si P est irréductible sur k et x une racine de P dans K, montrer que $m \geq n$ en considérant $k[x]$.*
2. *Si $P = QR$ montrer qu'un des deux polynômes Q, R est de degré inférieur à $n/2$, considérer un de ses facteurs irréductibles et montrer que P a une racine dans un corps de dimension inférieure à $n/2$.*

On a donc montré que P est irréductible sur k s'il n'a pas de racine dans une extension de degré inférieur à $n/2$.

Exercice 31. *(Application du précédent) En utilisant les réductions* $\bmod 2$ *ou* $\bmod 3$ *montrer que les polynômes suivant sont irréductibles dans $\mathbb{Z}[X]$:*

$$X^5 - 6X^3 + 2X^2 - 4X + 5, 7X^4 + 8X^3 + 11X^2 - 24X - 455.$$

2.2 Racines

Exercice 32. *Soit $P \in \mathbb{R}[X]$ montrer l'équivalence :*

— *Pour tout réel t, on a $P(t) \geq 0$.*

— *Il existe deux polynômes réel Q, R tels que $P = Q^2 + R^2$.*

On utilisera le fait que les polynômes vérifiant la deuxième condition forment un ensemble stable par multiplication.

Exercice 33. *Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme à coefficients entiers premiers entre eux (c'est à dire tels que les seuls diviseurs communs à tous les a_i soient -1 et 1). Montrer que si $r = \frac{p}{q}$ avec p et q premiers entre eux est une racine rationnelle de P alors p divise a_0 et q divise a_n.*

Exercice 34.

1. *Montrer que le polynôme $P(X) = X^5 - X^2 + 1$ admet une unique racine réelle et que celle-ci est irrationnelle.*
2. *Montrer que le polynôme $Q(X) = 2X^3 - X^2 - X - 3$ a une racine rationnelle (qu'on calculera). En déduire sa décomposition en produit de facteurs irréductibles dans $\mathbb{C}[X]$.*

Exercice 35. □ *On considère un polynôme $P(X) = a_n X^n + \ldots a_0$. On note $\sigma_i, S_i, 1 \leq i \leq n$ les polynômes symmétriques fondamentaux et les sommes de Newton en les racines de P.*

1. *Montrer que l'on a pour tout entier $i \leq n$: $a_n S_i + \ldots a_{n-1} S_1 + i a_{n-i} = 0$.*
2. *Montrer que l'on a pour tout entier $h \leq n$:*

$$(-1)^h h \sigma_h = \sum_{i=0}^{h-1} (-1)^{-i-1} \sigma_i S_{h-i}.$$

   On commencera par le cas $h = n$.

3. *Montrer que l'on a pour tout entier $h \geq n+1$:*

$$0 = \sum_{i=0}^{n} (-1)^{-i-1} \sigma_i S_{h-i}.$$

4. *Vérifier les formules pour $P(X) = X^2 - X + 1$ et pour $Q(X) = (X-1)(X-2)(X+1)$.*

Exercice 36. □

1. *Calculer la somme des carrés des racines de l'équation $X^3 + 2X - 3 = 0$.*
2. *Calculer $x_1^3 x_2 + x_1 x_2^3 + x_2^3 x_3 + x_2 x_3^3 + x_3^3 x_1 + x_3 x_1^3$, où x_1, x_2, x_3 sont les racines de l'équation $X^3 - X^2 - 4X + 1 = 0$.*

Exercice 37. *Exprimer à l'aide des polynômes symétriques fondamentaux :*

1. $(x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2)$;
2. $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$;
3. $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$.

2.3 Polynômes cyclotomiques

Exercice 38. □ *Pour $n \in \mathbb{N}^*$, soit $\mathcal{P}_n$ l'ensemble des racines n-èmes primitives de l'unité dans $\mathbb{C}$. On pose $\Phi_1(X) = X-1$ et $\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n}(X-\zeta)$. Φ_n est appelé le n-ème polynôme cyclotomique (son degré est $\varphi(n)$ où φ est l'indicateur d'Euler).*

1. *Démontrer :* $(\forall\ n \in \mathbb{N}^*)\ X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. *En déduire, par récurrence, que $\Phi_n(X)$ a tous ses coefficients dans $\mathbb{Z}$.*
3. *Calculer explicitement $\Phi_n(X)$ pour $n \leq 16$.*
4. *Démontrer que, pour p premier et $\alpha \in \mathbb{N}^*$, $\Phi_{p^\alpha}(X) = \sum_{k=0}^{p-1} X^{kp^{\alpha-1}}$.*
5. *Montrer que le degré de Φ_n est égal à $\varphi(n)$.*
6. *Montrer que, si $d < n$ et d divise n, alors $X^d - 1$ divise $X^n - 1$ dans $\mathbb{Z}[X]$, puis que $\Phi_n(X)$ divise les polynômes $X^n - 1$ et $\frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$.*

Exercice 39. ✠✠ *Le but est de montrer que Φ_8 est réductible dans tout corps fini.*

1. *Donner la décomposition de Φ_8 dans $\mathbb{F}_2$.*
2. *Donner la décomposition de Φ_8 dans $\mathbb{F}_3$.*
3. *Écrire toutes les décompositions possibles de Φ_8 comme produit de deux polynômes de degré deux sur $\mathbb{C}$.*
4. *Montrer que pour tout nombre premier $p \geq 3$ si x est racine de Φ_8 dans $\mathbb{F}_p$ alors x est racine de $X^8 - 1$.*
5. *Montrer que le groupe $\mathbb{F}_{p^2}^*$ contient toujours un élément d'ordre 8. On admettra que ce groupe est cyclique. En déduire que Φ_8 admet une racine sur $\mathbb{F}_{p^2}$.*
6. *Déduire que Φ_8 est réductible dans $\mathbb{F}_p$ en utilisant un exercice précédent.*

Exercice 40. ✠✠ *L'objectif est de montrer que tout polynôme cyclotomique est irréductible sur $\mathbb{Z}$. Soit x une racine primitive n-ème de l'unité et p un nombre premier ne divisant pas n. Appelons f, g les polynômes minimaux de x, x^p sur $\mathbb{Q}$.*

1. *Montrer que f, g sont à coefficients entiers.*
2. *On va montrer que $f = g$*
   (a) *Montrer que x est racine de $g(X^p)$. En déduire que $f(X)$ divise $g(X^p)$ dans $\mathbb{Z}$.*
   (b) *Montrer que $g(X^p) = (g(X))^p$ dans $\mathbb{Z}/p\mathbb{Z}$.*
   (c) *En déduire que la réduction modulo p de Φ_n a une racine double si $f \neq g$.*
   (d) *Conclure que $f = g$.*
3. *En déduire que f admet toutes les racines primitives de l'unité comme zéros.*

Exercice 41. ✠✠ *L'objet de l'exercice est de démontrer le théorème de Wedderburn : tout corps fini est commutatif. On considère K un corps gauche fini et $Z(K)$ son centre, de cardinal q.*

1. *Montrer que $Z(K)$ est un corps commutatif.*
2. *Montrer que K est un $Z(K)$-espace vectoriel de dimension finie, notée n. Donner alors le cardinal de K en fonction de q et n.*
3. *Soit $a \in K \setminus \{0\}$. On note $C_a = \{x \in K \mid ax = xa\}$.*
   Montrer que C_a est un corps gauche, puis que c'est un $Z(K)$-espace vectoriel de dimension finie d divisant n (on montrera pour cela que K est un C_a-espace vectoriel et l'on étudiera sa dimension).
4. *On fait opérer le groupe multiplicatif K^* sur lui-même par automorphismes intérieurs. Trouver l'orbite de a s'il est dans $Z(K)$.*
5. *Si a n'est pas dans $Z(K)$ montrer que son orbite a un cardinal égal à $\frac{q^n-1}{q^d-1}$ pour un certain d divisant n.*
6. *En déduire :*

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{d_i} - 1} \text{ avec, pour tout } i,\ d_i | n.$$

7. *En déduire que $\Phi_n(q)$ divise $q - 1$.*
8. *Soit x une racine complexe de Φ_n montrer que $|q - x| > q - 1$ si $x \neq 1$. En déduire $|\Phi_n(q)| > q - 1$.*
9. *En déduire que $n = 1$.*

Exercice 42. *Soit θ un réel. Montrer que pour tout entier non nul n il existe un polynôme T_n tel que*

$$T_n(\cos\theta) = \cos(n\theta)$$

1. *Calculer T_1, T_2, T_3.*
2. *Trouver le degré de T_n.*
3. *Montrer que $T_n \circ T_m = T_{nm}$.*
4. *Montrer que son coefficient dominant vaut 2^{n-1}.*

2.4 Résultant, Polynômes à plusieurs variables

Exercice 43. ✠ *Soit A un anneau factoriel et P, Q deux polynômes de $A[X]$ de degré respectif m et n strictement positifs. On note $P \wedge Q$ le pgcd de P et Q.*

1) Montrer que $P \wedge Q$ est un polynôme non constant si et seulement si il existe deux polynômes U et V tels que $degU < n$, $degV < m$ et $UP + VQ = 0$.

2) On désigne par $A[X]_d$ le A module libre des polynômes de degré inférieur ou égal à d. Soit f l'application A linéaire suivante (le produit de modules est un module ...) :

$$f : (U, V) \in A[X]_{n-1} \times A[X]_{m-1} \to UP + VQ \in A[X]_{m+n-1}$$

On appelle résultant de P et Q, et l'on note $Res\,(P,Q)$ le déterminant de l'application f calculée dans les bases

$$((X^{n-1},0),...,(1,0),(0,X^{m-1}),...,(0,1)) \quad et \quad (X^{m+n-1},...,1).$$

Notons $P = p_mX^m + ... + p_0$ et $Q = q_nX^n + ... + q_0$. Montrer que

$$Res\,(P,Q) = \begin{vmatrix} p_m & p_{m-1} & \cdots & & p_0 & & & \\ & p_m & p_{m-1} & \cdots & & p_0 & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & p_m & p_{m-1} & \cdots & & p_0 \\ q_n & q_{n-1} & \cdots & & q_0 & & & \\ & q_n & q_{n-1} & \cdots & & q_0 & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & q_n & q_{n-1} & \cdots & & q_0 \end{vmatrix}.$$

Les n premières lignes sont construites à partir des coefficients de P, les m dernières à partir de ceux de Q. Les entrées non spécifiées sont nulles.

3) *Montrer que $P \wedge Q$ est un polynôme non constant si et seulement si $Res\,(P,Q) = 0$ (on pourra considérer le corps des fractions de A et l'application $\widehat{f} : K[X]_{n-1} \times K[X]_{m-1} \to K[X]_{m+n-1}$ construite sur le modèle de f).*

Exercice 44. *Soient a, b deux nombres algébriques de polynômes minimaux f, g. Calculer les deux résultants suivant*

$$Res_Y(f(X), g(Y-X)), Res_Y(f(X), g(Y/X)X^{deg(g)})$$

En déduire un polynôme minimal de $a+b$ et de ab. On remarquera que $g(Y/X)$ n'est pas un polynôme.

Exercice 45.

1. *Montrer que l'idéal $< X, Y >$ n'est pas principal dans $\mathbb{Q}[X,Y]$.*
2. *Montrer que l'idéal (X) est premier non maximal dans $\mathbb{Q}[X,Y]$.*

Exercice 46. *Montrer que dans $\mathbb{R}^n$ le complémentaire des zéros d'un polynôme non nul est dense.*

3 Références

— Perrin : Cours d'algèbre :
— Francinou-Gianella-Nicolas :
— Livre Licence de votre choix (Monnier, Liret-Martinet-Ramis...) :