Exercices d'algèbre
Agrégation interne 2014

N. Bédaride

Table des matières

1 Groupes

1.1 Généralités

Exercice 1. □ *Soit G un groupe fini de cardinal n et m un entier premier avec n. Montrer que, pour tout y élément de G, il existe un unique x élément de G tel que $x^m = y$.*
[[Utiliser le théorème de Bezout.]]

Exercice 2. *Soit $(G, .)$ un groupe fini de cardinal n. On suppose que, tout x élément de G, satisfait l'égalité $x^2 = e$.*

1. *Montrer que G est un groupe commutatif.*

2. *Soit $A = \{a_1, \ldots, a_p\}$ une partie génératrice de G, montrer que :*

$$\forall x \in G, \quad \exists(\varepsilon_1, \ldots, \varepsilon_p) \in (\mathbb{Z}/2\mathbb{Z})^p \text{ tels que, } x = a_1^{\varepsilon_1} \ldots a_p^{\varepsilon_p}.$$

3. *On suppose, dans les questions suivantes, que A est une partie génératrice de cardinal minimum p. Montrer que l'écriture :*

$$x = a_1^{\varepsilon_1} \ldots a_p^{\varepsilon_p}$$

est unique.

4. *Soit Φ l'application définie par :*

$$\begin{array}{rccc} \Phi : & G & \to & (\mathbb{Z}/2\mathbb{Z})^p \\ & x & \mapsto & (\varepsilon_1, \ldots, \varepsilon_p). \end{array}$$

Montrer que Φ est bien définie et que c'est un isomorphisme de groupes. En déduire que le cardinal de G est 2^p.

Exercice 3. ✠*Soit p un nombre premier fixé, soit*

$$U_p = \{exp(\frac{2i\pi a}{p^\alpha}),\ a \in \mathbb{Z},\ PGCD(a,p) = 1,\ \alpha \in \mathbb{N}\}$$

1. *Montrer que U_p est un groupe infini dont tous les éléments sont d'ordre fini. Trouver l'ordre de $exp(\frac{2i\pi a}{p^\alpha})$, pour a entier premier avec p et pour $\alpha \in \mathbb{N}$.*
2. *On va montrer que tout sous-groupe strict de U_p est cyclique.*
   (a) *Soit G_α le sous groupe engendré par $exp(\frac{2i\pi}{p^\alpha})$. Montrer que si $\beta \leq \alpha$ alors $G_\beta \subset G_\alpha$.*
   (b) *En déduire que $U_p = \bigcup G_\alpha$. On montrera que l'union est bien un groupe.*
   (c) *Soit H un sous groupe distinct de G_α pour tout α. Considérer pour α fixé un $x \in H$ qui n'est pas dans G_α, et raisonner par l'absurde pour conclure.*
3. *En déduire que U_p n'est pas le produit de deux sous-groupes.*

Exercice 4. *Soit G un groupe abélien fini, a et b deux éléments de G. On note $O(a)$ l'ordre de a et $O(b)$ l'ordre de b. Le but de l'exercice est de voir quelles sont les valeurs que peut prendre l'ordre de l'élément ab.*

1. *Soit p entier non nul tel que $(ab)^p = e$, soit m le PPCM de p et $O(a)$, n le PPCM de p et $O(b)$. Montrer que $O(a)$ divise n et que $O(b)$ divise m.*
2. *En déduire que lorsque $O(a)$ et $O(b)$ sont premiers entre eux, alors $O(ab) = O(a)O(b)$.*
3. *Montrer que le résultat précédent est faux en général.*
4. *Notons d le PGCD de $O(a)$ et $O(b)$ et M le PPCM de $O(a)$ et $O(b)$, en utilisant la première question, montrer que : $\frac{M}{d}$ divise $O(ab)$ et que $O(ab)$ divise M.*

5. *En choisissant des éléments convenables dans le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, vérifier que l'on peut avoir :*
$$\frac{M}{d} < O(ab) < M.$$
6. *Montrer qu'il existe toujours dans G un élément d'ordre M.*
7. *Si G est non abélien, donner un exemple avec a et b d'ordres 2 et ab d'ordre infini.*

Exercice 5. *Soit G groupe abélien d'ordre pq avec p, q deux nombres premiers distincts. Montrer que le groupe est cyclique.*

1.2 Groupe des permutations

Exercice 6. *Le but de l'exercice est de montrer que, pour $n \geq 3$, le centre du groupe $\mathcal{S}_n$ ($Z(\mathcal{S}_n)$) est réduit à l'identité.*

1. *Soit $i \in \{1 \dots n\}$, donner un exemple de permutation s telle que :*
$$\begin{cases} s(i) = i \\ et \\ \forall j \in \{1 \dots n\}, j \neq i \Longrightarrow s(j) \neq j. \end{cases}$$
2. *Soit $\sigma \in Z(\mathcal{S}_n)$, en utilisant le fait que $s \circ \sigma = \sigma \circ s$, montrer que $\sigma(i) = i$. Conclure que le centre de $\mathcal{S}_n$ est réduit à l'identité.*
3. *Déduire du résultat précédent que $\mathcal{S}_n$ n'a pas de sous-groupe distingué d'ordre 2.*

Exercice 7. *On dit qu'un groupe G agit sur un ensemble X de façon p transitive si, étant donnés $x_1, \dots, x_p$ éléments de X distincts et $y_1, \dots, y_p$ éléments de X distincts, il existe g élément de G tel que, pour tout i compris entre 1 et p, $g.x_i = y_i$.*

1. *Montrer que $\mathcal{S}_n$ agit n transitivement sur $\{1, \dots, n\}$.*
2. *Montrer que $\mathcal{A}_n$ agit $n-2$ transitivement sur $\{1, \dots, n\}$.*
3. *En déduire que, pour n supérieur ou égal à 5, les 3-cycles sont conjugués dans $\mathcal{A}_n$.*

Exercice 8 (Étude du groupe $\mathcal{A}_4$)**.** □

1. *Faire la liste des éléments de $\mathcal{A}_4$, donner leurs ordres.*
2. *Soit H l'ensemble formé de l'identité,*
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$
Montrer que H est un sous-groupe distingué de $\mathcal{A}_4$ isomorphe au groupe de Klein.

Exercice 9. ✠ *On considère le groupe $\mathcal{A}_5$.*

1. *Lister les éléments d'ordre $2, 3, 5$.*

2. *Montrer que les transpositions sont conjuguées dans ce groupe, ainsi que les trois cycles.*
3. *Montrer que si a, b sont deux 5 cycles, alors a est conjugué à b ou à b^2.*
4. *Calculer le nombre d'éléments d'ordre $2, 3, 5$.*
5. *Conclure que ce groupe est simple.*

Exercice 10. *Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.*

1.3 Action de groupes

Exercice 11. □ *On considère $u \in \mathbb{R}^2$ vecteur non nul.*

1. *Décrire l'action de D_n sur u.*
2. *Décrire l'action de $O(n)$ sur u.*
3. *Trouver les stabilisateurs de u pour ces actions.*

Exercice 12. □ *Soit G un groupe fini de cardinal n.*

1. *Montrer que l'action de G par translation sur lui même est fidèle.*
2. *En déduire que G s'injecte dans S_n.*

Exercice 13. *Soit $G = GL_2(\mathbb{R})$.*

1. *Quelle est l'orbite sous l'action par conjugaison de la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$?*
2. *Même question pour $\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$.*

Exercice 14. *Soit G un groupe fini à 21 éléments opérant sur un ensemble à 11 éléments. Montrer qu'il existe au moins un point fixe sous l'action de G.*

Exercice 15. *On cherche le nombre de colliers de 67 perles formés de 2 rouges, 7 bleues et 2 noires. et 56 bleues.*

1. *Montrer que l'on peut considérer les colliers comme des sommets colorés d'un polygone régulier à 67 côtés et que sur cet ensemble agit D_{67}.*
2. *Montrer que le nombre de colliers est égal au nombre d'orbites dans l'action du groupe.*
3. *Montrer que $n = \frac{1}{|G|} \sum_g |Fix(g)|$. C'est la formule de Burnside.*
4. *Calculer $|Fix(g)|$ en séparant les cas suivants que g soit une symétrie, l'identité ou une rotation.*
5. *Conclure.*

Exercice 16. *Montrer que le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ agit sur $\mathbb{Z}/8\mathbb{Z}$. Décrire les orbites et calculer leurs cardinaux via la formule des classes.*

Exercice 17. ✠ *[Théorème de Cauchy] Le but de l'exercice est de montrer, qu'étant donné G un groupe fini de cardinal n et p un diviseur premier de n, il existe un élément de G d'ordre p.*

1. *Soit $\mathcal{A}$ le sous-ensemble de G^p défini par :*
$$\mathcal{A} = \{(x_0, \ldots, x_{p-1}) \in G^p, \text{ tels que } x_0 \ldots x_{p-1} = e\}.$$
Montrer que $\mathcal{A}$ est en bijection avec G^{p-1}. En déduire que :
$card(\mathcal{A}) = n^{p-1}$.
2. *On définit l'application ϕ par :*
$$\phi : \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times \mathcal{A} & \to & \mathcal{A} \\ (\overline{k}, (x_0, \ldots, x_{p-1})) & \mapsto & (x_{(k)mod[p]}, \ldots, x_{(p-1+k)mod[p]}) \end{array}$$
Montrer que ϕ est bien définie et que c'est une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble $\mathcal{A}$.
3. *Soit $(x_1, \ldots, x_p) \in \mathcal{A}$, montrer que le stabilisateur de $(x_0, \ldots, x_{p-1})$ est égal à $\mathbb{Z}/p\mathbb{Z}$ si et seulement si :*
$x_0 = \cdots = x_{p-1}$ et x_1 est d'ordre 1 ou p.
4. *Appliquer la formule des classes et montrer que le nombre d'éléments d'ordre p de G est congru à -1 modulo p. En déduire qu'il y a, au moins, un élément d'ordre p.*
5. *Application*
Soit G un groupe fini d'ordre n et p un diviseur premier de n tel que : $\forall x \in G$, $x^p = e$. Montrer qu'il existe un nombre entier k tel que $card(G) = p^k$.
[[Supposer que n a un diviseur premier q différent de p et appliquer le théorème de Bezout à p et q.]]

1.4 Groupe diédral

Exercice 18. □ *On considère le groupe diédral D_n.*

1. *Montrer $D_n =< r, s | s^2 = r^n = srsr = 1 >$*
2. *Montrer que $D_n = \{Id, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$.*

Exercice 19. □ *Montrer que le centre de D_n est trivial si n est impair et engendré par $r^{n/2}$ sinon.*

Exercice 20. ✠ *On considère le groupe diédral D_n.*

1. *Si n est impair montrer que les sous groupes distingués sont D_n et les sous groupes de $\mathbb{Z}/n\mathbb{Z}$.*
2. *Si n est pair montrer qu'il y a aussi le sous groupe engendré par r^2, s et celui engendré par r^2, sr.*

Exercice 21. *On considère le groupe diédral D_n.*

1. *Si n est impair alors $D(D_n) = \mathbb{Z}/n\mathbb{Z}$*
2. *Si n est pair alors $D(D_n) =< r^2 >$.*

1.5 $\mathbb{Z}/n\mathbb{Z}$

Exercice 22 (Automorphismes de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit n un entier naturel supérieur ou égal à 2, montrer que le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (noté $Aut(\mathbb{Z}/n\mathbb{Z})$) est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.*
[[Considérer l'appplication qui, à un automorphisme ϕ, associe $\phi(1)$ et utiliser le fait que les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les inversibles de $\mathbb{Z}/n\mathbb{Z}$.]]

Exercice 23. *Montrer que, pour tout entier naturel non nul n, le groupe additif $\mathbb{Q}/\mathbb{Z}$ possède un seul sous-groupe d'ordre n.*
[[Considérer H un sous-groupe de $\mathbb{Q}/\mathbb{Z}$ d'ordre n et Π la projection canonique de $\mathbb{Q}$ dans $\mathbb{Q}/\mathbb{Z}$. En utilisant le fait que les sous-groupes de $\mathbb{R}$ sont soit denses, soit de la forme $a\mathbb{Z}$, montrer que $\Pi^{-1}(H)$ est de la forme $\frac{p}{q}\mathbb{Z}$, avec p et q entiers.]]

Exercice 24 (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. *Ecrire 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.*

Trois professeurs commencent leurs cours respectivement le lundi, mardi et jeudi. Le premier fait un cours tous les deux jours, le deuxième tous les trois et le dernier tous les cinq jours. Les cours qui tombent un dimanche sont reportés. Quand pour la première fois les trois enseignants auront ils à supprimer leurs cours le même jour ?

Exercice 25. ✠*[RSA] Soient p, q deux entiers et c, d tels que*

$$pq = n, cd = 1 \mod \varphi(n)$$

Le message est un élément $m \in \mathbb{Z}/n\mathbb{Z}$ et p, q, c sont cachés. On dit que l'on chiffre m en donnant m^c. On dit que l'on déchiffre y en donnant y^d.

1. *Si $x = m^c$, montrer que $x^d = m \mod n$ en utilisant le petit théorème de Fermat si m est premier avec n.*
2. *Pour $p = 7, q = 11, c = 13$ trouver un d qui convient.*
3. *Supposons que Bob envoie m à deux personnes ayant des clés différentes et premières entre elles. Montrer que la donnée de m^{c_1}, m^{c_2} permet de retrouver m.*

Exercice 26. □ *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 27. *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 28. *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 $\gcd(k, n) = d$.*

1.6 Classification

Exercice 29. *On considère un groupe G à 6 éléments.*

1. *Montrer que le groupe des automorphismes de $\mathbb{Z}/3\mathbb{Z}$ possède deux éléments. Soit ϕ l'automorphisme de $\mathbb{Z}/3\mathbb{Z}$ différent de l'identité, décrire ϕ.*
2. *En utilisant le théorème de Lagrange, montrer que G contient un élément d'ordre deux.*
3. *Décrire les morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans $Aut(\mathbb{Z}/3\mathbb{Z})$.*
4. *Décrire les éléments du groupe de permutations S_3.*
5. *Montrer que l'ensemble $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ peut être muni d'une structure de groupe à l'aide de ϕ.*
6. *En déduire la liste, à isomorphisme près, des groupes G possibles.*

Exercice 30. ✠ *On considère un groupe à 8 éléments :*

1. *Montrer que si le groupe est abélien et que tous ses éléments sont d'ordre 2, alors il est isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^3$.
2. *Montrer que si le groupe ne possède pas d'élément d'ordre 8 et un élément d'ordre 4, alors il est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
3. *A quelle condition est il isomorphe à* $\mathbb{Z}/8\mathbb{Z}$ *?*
4. *Montrer que* D_4 *est un groupe à 8 éléments dont le centre est isomorphe à* $\mathbb{Z}/2\mathbb{Z}$ *et calculer son quotient par le centre.*
5. *On considère* $Q = \{1, -1, i, -i, j, -j, k, -k\}$ *le groupe des quaternions. On rappelle que* $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$.
6. *Vérifier que c'est un groupe.*
7. *Calculer son centre et le quotient par le centre.*

Exercice 31. ✠ *Soit G un groupe d'ordre* p^2 *:*

1. *En utilisant une action de groupe montrer que le centre de G est non réduit à l'élément neutre.*
2. *En déduire que G est commutatif. [[On regardera le quotient de G par son centre.]]*
3. *En déduire une classification.*

2 Anneaux et corps

2.1 Généralités

Exercice 32.
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 33. □ *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 homomorphisme 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 34. *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 $\sqrt{I}$.*

2.2 Anneaux classiques

Exercice 35. *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.*

Exercice 36. *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 est stable par multiplication.*
3. *Dans la suite on se restreint au cas ou n est premier, noté p.*
4. *Montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.*
5. *Montrer que $\mathbb{Z}[i]/(p) \sim \mathbb{F}_p[X]/(X^2+1)$.*
6. *En déduire que $p \in \Sigma$ si et seulement si -1 est un carré de $\mathbb{F}_p$.*

Exercice 37. ✠ *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 38. ✠✠ *On considère l'ensemble* $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. *On pose* $\alpha = \frac{1+i\sqrt{19}}{2}$ *et* $N(z) = z\overline{z} = a^2 + ab + 5b^2$.

1. *Montrer que* $\alpha^2 = \alpha - 5$.
2. *Montrer que la norme* N *est multiplicative. En déduire* A^*.
3. *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.*
4. *Dans ce cas, que dire de* $L/(x)$ *?*
5. *Montrer que* A *ne peut être euclidien : Raisonner par l'absurde en considérant un morphisme de* A *dans* $\mathbb{F}_p$ *pour un* p *bien choisi.*

Exercice 39. ✠ *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 40. *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.*

2.3 Arithmétique

Exercice 41. *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 42.

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 43. *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 44. □ *Déterminer l'ensemble de tous les couples d'entiers* (m, n) *tels que*

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

Exercice 45. *Démontrer que le nombre* $7^n + 1$ *est divisible par* 8 *si* n *est impair ; dans le cas* n *pair, donner le reste de sa division par* 8.

Exercice 46. *Montrer que si* x *et* y *sont des entiers naturels tels que* x^2 *divise* y^2, *alors* x *divise* y. *Application : démontrer, par l'absurde, que* $\sqrt{2}$ *n'est pas rationnel.*

Exercice 47. *Montrer que pour tout* $n \in \mathbb{N}$:

$$n(n+1)(n+2)(n+3) \text{ est divisible par } 24,$$

$$n(n+1)(n+2)(n+3)(n+4) \text{ est divisible par } 120.$$

Exercice 48. *Trouver tous les entiers relatifs* n *tels que* $n^2 + n + 7$ *soit divisible par* 13.

2.4 Corps

Exercice 49. *Soit* $E = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}\}$

1. *Montrer que* E *est un sous corps de* $\mathbb{C}$.
2. *Déterminer les automorphismes de* E.

Exercice 50. *Soit* E *le* $\mathbb{Q}$ *espace vectoriel engendré par* $1, \sqrt{2}, \sqrt{3}$.

1. *Montrer qu'il est de dimension trois.*
2. *Soit* F *le* $\mathbb{Q}(\sqrt{2})$ *espace vectoriel engendré par* $1, \sqrt{3}$. *Montrer qu'il est de de dimension deux.*
3. *En déduire que* F *est un* $\mathbb{Q}$ *espace vectoriel de dimension quatre. On utilisera le fait que* $\mathbb{Q}(\sqrt{2})$ *est un corps.*

Exercice 51. *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 52. *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.*

3 Polynômes

3.1 Polynômes irréductibles, pgcd

Exercice 53. □ *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 54. *Trouver le pgcd dans $\mathbb{Z}/3\mathbb{Z}[X]$ et $\mathbb{Z}/5\mathbb{Z}[X]$ de $f = X^4 + 1$, $g = X^3 + X + 1$.*

Exercice 55. *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 56. ✠✠ *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 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 57. *(Application du précédent) En utilisant les réductions* $\bmod 2$ *ou* $\bmod 3$ *montrer que les polynômes suivant sont irréductibles dans $\mathbb{Z}[X]$:*

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

3.2 Racines

Exercice 58. *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 $r = \dfrac{p}{q}$ avec p et q premiers entre eux est une racine rationnelle de P alors p divise a_0 et q divise a_n.*

Exercice 59.

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 60. □ *On considère un polynôme $P(X) = a_n X^n + \dots a_0$. 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 $i \leq n$: $a_n S_i + \dots a_{n-1} S_1 + i a_{n-i} = 0$.*
2. *Montrer que l'on a pour tout entier $h \leq n$:*

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

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 61. □

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 62. *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. $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$.

3.3 Polynômes cyclotomiques

Exercice 63. □ *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 $\alpha \in \mathbb{N}^*$, $\Phi_{p^\alpha}(X) = \sum_{k=0}^{p-1} X^{k p^{\alpha-1}}$.*
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 $X^n - 1$ et $\frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$.*

Exercice 64. ✠ *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. *Ecrire 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 65. ✠✠ *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 66. ✠✠ *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 67. *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}.*

3.4 Fractions rationnelles

Exercice 68. □

1. *Décomposer $\frac{X^3-3X^2+X-4}{X-1}$ en éléments simples sur $\mathbb{R}$.*
2. *Décomposer $\frac{2X^3+X^2-X+1}{X^2-3X+2}$ en éléments simples sur $\mathbb{R}$.*
3. *Décomposer $\frac{X+i}{X^2+i}$ en éléments simples sur $\mathbb{C}$.*
4. *Décomposer $\frac{X}{(X+i)^2}$ en éléments simples sur $\mathbb{C}$.*
5. *Décomposer $\frac{X^2+1}{X^4+1}$ en éléments simples sur $\mathbb{R}$ et sur $\mathbb{C}$.*

Exercice 69. *On considère l'équation différentielle*

$$(1 + x^2)y = x(1 - x)y'$$

1. *Décomposer la fraction $\frac{1+x^2}{x(1-x)}$ en éléments simples*
2. *Résoudre l'équation sur $]1, +\infty[$*
3. *Trouver la solution telle que $y(2) = -\frac{2}{3}$.*

4 Combinatoire

Exercice 70. *Soit E un ensemble fini trouver le cardinal de $\{(A,B) \in E \times \mathcal{P}(E)\}$ si*
- $A \subset B$.
- $A \cap B = \emptyset$
- $A \cup B = E$
- $A \cap B = \emptyset, A \cup B = E$.

Exercice 71. ✠ *Soit E un ensemble à n éléments, on définit*

$$S_1 = \sum_{x \subset \mathcal{P}(E)} card x$$

$$S_2 = \sum_{x,y \subset \mathcal{P}(E)} card(x \cap y)$$

$$S_3 = \sum_{x,y \subset \mathcal{P}(E)} card(x \cup y)$$

1. *Montrer que $S_1 = n2^{n-1}, S_2 = n2^{2n-2}$.*
2. *Montrer que $S_2 + S_3 = 2^{n+1}S_1$.*
3. *En déduire S_3.*

Exercice 72. *Monter en utilisant des dénombrements que*

$$\sum_{i=0}^{k} \binom{n_1}{i}\binom{n_2}{k-i} = \binom{n_1+n_2}{k}$$

Exercice 73. *On considère les applications entre des ensembles à n et p éléments. On cherche le nombre de surjections notées $S(n,p)$.*

1. *Montrer que $S(n,p) = p!S_n^p$ ou S_n^p représente le nombre de partitions d'un ensemble à n éléments en p sous ensembles non vides.*
2. *Montrer alors que $S_{n+1}^p = S_n^{p-1} + pS_n^p$.*
3. *En déduire une récurrence sur $S(n,p)$.*
4. *En déduire que*
$$S(n,p) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^p.$$

Exercice 74. *On cherche le nombre D_n de dérangements : permutations de n éléments sans point fixe.*

1. *Montrer que $\sum_{k=0}^{n} C_n^k D_{n-k} = n!$ On décomposera une permutation en fonction du nombre de ses points fixes.*
2. *Calculer $\sum_{k=0}^{p} (-1)^k C_n^k C_{n-k}^{p-k}$ pour $0 \leq p \leq n$.*

3. *En déduire que* $D - n = n!(\sum_{k=0}^{n} \frac{(-1)^k}{k!})$. *On partira du membre de droite.*

Exercice 75. *On cherche le cardinal de* $S0_2(\mathbb{Z}/p\mathbb{Z})$ *pour* p *premier.*

1. *Montrer que cet ensemble est en bijection avec* $\{(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2 a^2 + b^2 = 1\}$
2. *Trouver le cardinal pour* $p = 2$.
3. *Si* -1 *n'est pas un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *montrer que le cardinal vaut* $1 + p$.
4. *Si* -1 *est un carré, montrer que le cardinal vaut* $p - 1$.

5 Références

- Perrin : Cours d'algèbre : 33-34-36-37-34-50-61-62-63-64
- Francinou-Gianella-Nicolas : 3-4-15-21-39-54-72-73
- Livre Licence de votre choix (Monnier, Liret-Martinet-Ramis...) : 38-41-47-53-55-56-61-64-66