Exercices d'algèbre
Agrégation interne 2015-16

N. Bédaride

Table des matières

1 Arithmétique

Exercice 1. □ *Déterminer l'ensemble de tous les couples d'entiers* (m, n) *tels que*

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

Exercice 2. *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 3. *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 4. *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 5. *Trouver tous les entiers relatifs n tels que $n^2 + n + 7$ soit divisible par 13.*

Exercice 6. *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 7. *On considère le développement en base 10 d'un nombre réel.*

1. *Montrer que si le développement est périodique, alors le nombre est rationnel.*
2. *En utilisant l'algorithme d'Euclide montrer que le développement d'un rationnel est ultimement périodique.*
3. *On pourra estimer la période d'un tel développement en fonction de p, q.*

Exercice 8.

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 9. *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 10 (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.*

Exercice 11. ✠*[RSA] Soient p, q deux nombres premiers et c, d deux entiers tels que*

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

Le message est un élément $m \in \mathbb{Z}/N\mathbb{Z}$ et p, q sont cachés. Les entiers N, c sont publics. On dit que l'on chiffre m en donnant $m^c \mod N$. On dit que l'on 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 si m est premier avec n.*
2. *Pour $p = 7, q = 11, c = 13$ trouver un d qui convient. En déduire comment Alice peut envoyer un message à Bob.*
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 calculer $m_1^{b_1} m_2^{-b_2}$ modulo N.*
   (c) *Conclure*

Exercice 12. □ *On considère des entiers $n_1, \ldots, n_k$ deux à deux premiers entre eux. Le but est de 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 $x = \sum_{i=1}^{k} a_i E_i$.*
4. *En déduire les autres solutions.*

Exercice 13. *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 ?

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 reporter leurs cours le même jour ?

2 Anneaux et corps

2.1 Généralités

Exercice 14. □ *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 15. *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 16. *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 17. *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. *Montrer qu'il suffit de trouver les entiers $n \in \Sigma$ premier, notés 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 18. ✠ *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 19. ✠✠ *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 $z = a + b\alpha$, 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 inversibles non nuls.)*
6. *Ici, que dire de $A/(x)$?*
7. *Montrer que A ne peut être euclidien en raisonnant par l'absurde :*
   — *Considérer un morphisme de A dans $\mathbb{F}_p$ pour un p bien choisi.*
   — *Soit β l'image de α par le morphisme. Trouver une équation vérifiée par β, conclure.*

Remarquons que cet anneau est principal (cf exercice).

Exercice 20. *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 Corps

Exercice 21. *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 22. *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 23. *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 24. *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 25. □ *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. $A = X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2 \quad$ *et* $\quad B = X^4 + 2X^3 + 2X^2 + 7X + 6$.
2. $A = X^6 - 2X^5 + 2X^4 - 3X^3 + 3X^2 - 2X \quad$ *et* $\quad B = X^4 - 2X^3 + X^2 - X + 1$.

Exercice 26. *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 27. *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 28. ✠✠ *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 de degré n 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 29. *(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 30. *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 31.

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 32. □ *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 symétriques fondamentaux et les sommes de Newton en les racines de P.*

1. *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 $h = n$.

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

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

3. *Montrer que l'on a pour tout entier $i \leq n$:*

$$a_n S_i = (-1)^i a_{n-1}\sigma_1 + \ldots a_1 \sigma_{i-1} + (-1)^{i-1} i a_{n-i}.$$

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

Exercice 33. □

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 34. *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 35. □ *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 $X^n - 1$ et $\frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$.*

Exercice 36. ✠ *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 37. *Montrer que pour tout entier non nul n il existe un polynôme T_n tel que pour tout θ réel.*

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

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 38. □

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 39. *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 Groupes

4.1 Généralités

Exercice 40. □ *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 41. *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 42. ✠*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 le minimum des entiers n tels que x soit dans G_n. Montrer que $H = U_p$.*
3. *En déduire que U_p n'est pas le produit de deux sous-groupes.*

Exercice 43. *Montrer que l'ordre de d dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $\frac{n}{\gcd(n,d)}$.*

Exercice 44. ✠ *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. On utilisera aussi l'exercice précédent.*
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 45. *Soit G groupe abélien d'ordre pq avec p, q deux nombres premiers distincts. Montrer que le groupe est cyclique.*

Exercice 46 (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 $\mathbb{Z}/n\mathbb{Z}$.]]

4.2 Groupe des permutations

Exercice 47. *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 48. *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 49 (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. Pour montrer qu'il est distingué, on étudiera les ordres des éléments.

Exercice 50. ✠ *On considère le groupe $\mathcal{A}_5$.*

1. *Dénombrer le nombre d'éléments d'ordre $2, 3$ ou 5.*
2. *Montrer que les transpositions sont conjuguées dans ce groupe, ainsi que les trois cycles.*
3. *Montrer que si a, b sont deux cycles d'ordre 5, alors a est conjugué à b ou à b^2.*
4. *Déduire que si a appartient à un sous groupe distingué, alors tous les cycles d'ordre 5 y sont aussi.*
5. *Prouver que les cycles d'ordre 5 ne sont pas tous conjugués. Trouver le nombre de classes de conjugaison des éléments d'ordre 5.*
6. *Conclure que ce groupe est simple en raisonnant par l'absurde.*

Exercice 51. *Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.*

4.3 Action de groupes

Exercice 52. *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 53. *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 54. ✠ *On cherche le nombre de colliers de 67 perles formés de 2 rouges, 7 bleues et 2 noires et 56 vertes.*

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 n est égal au nombre d'orbites dans l'action du groupe.*

3. *Montrer en considérant l'ensemble* $\{(g,x) \in G \times X \mid g.x = x\}$ *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. On utilisera à bon escient que* 67 *est impair, premier, et que* 7 *est impair.*
5. *Conclure.*

Exercice 55. □ *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 56. ✠ *[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*.]]*

4.4 Groupe diédral

Exercice 57. □ *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 58. □ *Montrer que le centre de D_n est trivial si n est impair et engendré par $r^{n/2}$ sinon.*

Exercice 59. ✠ *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 60. *On considère le groupe diédral D_n. Le groupe dérivé est noté $D(D_n)$.*

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

4.5 Classification

Exercice 61. *On considère un groupe G à 6 éléments.*

1. *En utilisant le théorème de Lagrange, montrer que G contient un élément d'ordre deux.*
2. *En utilisant un exercice précédent, montrer que G contient un élément d'ordre trois.*
3. *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.*
4. *Décrire les morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans $Aut(\mathbb{Z}/3\mathbb{Z})$.*
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. *Décrire les éléments du groupe de permutations S_3. Faire le lien avec la question précédente.*
7. ✠*En déduire la liste, à isomorphisme près, des groupes G à 6 éléments.*

Exercice 62. ✠ *On considère un groupe à 8 éléments :*

1. *Montrer que si tous ses éléments sont d'ordre 2, alors il est abélien et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.*
2. *Montrer que si le groupe est abélien, 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 $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$.*
   (a) *Vérifier que c'est un groupe.*
   (b) *Calculer son centre et le quotient par le centre.*

Exercice 63. ✠ *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.*

5 Combinatoire

Exercice 64. ✠✠*Pour quels entiers m, n a t on $\sum_{k=m}^{n} \frac{1}{k}$ entier ?*

Exercice 65. ✠ *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 66. *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 67. *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 68. *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 que l'on arrangera puis utilisera les questions précédentes.*

Exercice 69. *On cherche le cardinal de* $S0_2(\mathbb{Z}/p\mathbb{Z})$ *pour* p *premier.*

1. *Montrer que cet ensemble est en bijection avec* $\{(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid a^2 + b^2 = 1\}$
2. *Trouver le cardinal pour* $p = 2$.
3. *On considère l'application de* $\mathbb{Z}/p\mathbb{Z}$ *dans* S^1 *qui à* t *associe* $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$.
   (a) *Trouver son ensemble de définition en fonction de* p.
   (b) *Montrer qu'elle est injective.*
   (c) *Montrer que son image est incluse dans* $S^1 \setminus (-1, 0)$.
4. *Si* -1 *n'est pas un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *en déduire que le cardinal vaut* $1 + p$.
5. *Si* -1 *est un carré, en déduire que le cardinal vaut* $p - 1$.

Exercice 70. *Trouver le cardinal de* $GL_3(\mathbb{Z}/4\mathbb{Z})$.

Exercice 71. *On cherche le nombre de partitions* b_n *de* $\{1 \dots n\}$. *Montrer que l'on a*

$$b_n = \sum_{k=1}^{n-1} C_n^k b_{n-k}.$$

6 Références

— Perrin : Cours d'algèbre : 14, 17, 19, 28, 35, 36
— Francinou-Gianella-Nicolas
— Livre Licence de votre choix (Monnier, Liret-Martinet-Ramis...)