

Agrégation

PROGRAMME DES TRAVAUX DIRIGÉS D'ALGÈBRE

RÉFÉRENCES PRINCIPALES

 Perrin (*Cours d'algèbre*)

 Biquard (*Algèbre I, notes de cours*),

https://www.math.ens.fr/enseignement/telecharger_fichier.php?fichier=3

 Audin (*Géométrie*)

CALENDRIER

Date	Intervenant	Sujet
10/09		Actions de groupes, Théorèmes de Sylow à lire Perrin (chap. I.5) ou Biquard (chap. 1)
10/09		Groupes diédraux ; produit semi-direct à lire Perrin (chap. I.6) ou Biquard (chap. 1)
17/09		Groupes d'ordre inférieur à 12 à lire groupes finis et Petits groupes
17/09		Simplicité à lire Perrin (chap. I.8)
24/09		
24/09		Irréductibilité des polynômes cyclotomiques sur \mathbb{Q} à lire Perrin (chap III.3 et III.4)
01/10		Généralités sur les corps à lire Perrin (chap III.1)
01/10		Théorie élémentaire des corps finis à lire Perrin (chap III.2)
08/10		
08/10		Endomorphismes semi-simples, endomorphismes unipotents à lire Matrices de passage ou Endomorphismes semi-simples ou Algèbre linéaire ou encore Endomorphismes semi-simples
15/10		Décomposition polaire des matrices à lire Décomposition polaire
15/10		Décomposition de Jordan-Chevalley à lire Jordan-Chevalley et Jordan-Chevalley explicite
22/10		Formes bilinéaires et sesquiliéaires à lire
22/10		Endomorphismes normaux à lire
05/11		Anneau $\mathbb{Z}/n\mathbb{Z}$: théorème chinois, automorphismes, indicatrice d'Euler, inversibles à lire Perrin (chap II)
05/11		Formes quadratiques sur les corps finis à lire Perrin (page 139 à 141)
12/11		quaternions à lire quaternions ou encore
12/11		coniques à lire coniques projectives

1. GROUPES

Lire le cours : Perrin (chap. I), Biquard (chap. 1),

- 1.1. **Actions de groupes, Théorèmes de Sylow.**
- 1.2. **Groupes diédraux ; produit semi-direct.**
- 1.3. **Groupes d'ordre inférieur à 12.**
- 1.4. **Simplicité.**
- 1.5. **Générateurs et simplicité de \mathfrak{A}_5 et \mathfrak{A}_n .**
- 1.6. **Groupes dérivés, résolubilité.**
- 1.7. **Générateurs de $SL(E)$, simplicité et résolubilité de $PSL(E)$.**
- 1.8. **Représentation linéaire des groupes finis.** Biquard (chap. 4)
- 1.9. **Théorème fondamental des fonctions symétriques.**

2. ANNEAUX ET ARITHMÉTIQUE

Lire le cours : Perrin (chap. II),

- 2.1. **Anneau $\mathbb{Z}/n\mathbb{Z}$: théorème chinois, automorphismes, indicatrice d'Euler, inversibles.**
- 2.2. **Irréductibilité des polynômes cyclotomiques sur \mathbb{Q} .**

3. THÉORIE DES CORPS

Lire le cours : Perrin (chap. III),

- 3.1. **Généralités sur les corps.**
- 3.2. **Théorie élémentaire des corps finis.**

4. ALGÈBRE LINÉAIRE

Lire le cours : Perrin (chap. IV),

- 4.1. **Décomposition de Jordan-Chevalley.**
- 4.2. **Endomorphismes cycliques et réduction de Frobenius.**
- 4.3. **Endomorphismes semi-simples, endomorphismes unipotents.**
- 4.4. **Endomorphismes normaux.**
- 4.5. **Décomposition polaire des matrices.**
- 4.6. **Exponentielle de matrices ; surjectivité de $\exp : M_n(\mathbb{C}) \rightarrow GL_n(\mathbb{C})$.**

5. ALGÈBRE SESQUILINÉAIRE

Lire le cours : Perrin (chap. V), Biquard (chap. 2)

- 5.1. **Généralités sur les formes bilinéaires et sesquilineaires.**
- 5.2. **Algorithme de Gram-Schmidt et décomposition QR (orthogonale \times triangulaire).**
- 5.3. **Algorithme de Gauß et loi d'inertie de Sylvester.**
- 5.4. **Endomorphismes orthogonaux et unitaires.**
- 5.5. **Endomorphismes symétriques et hermitiens.**

6. GÉOMÉTRIE AFFINE ET EUCLIDIENNE

Audin (Chapitre 1 et 2)

- 6.1. **Générateurs de $O(E)$, $SO(E)$ et simplicité de $PSO(E)$.**
- 6.2. **Isométries du cube ; isométries du tétraèdre. Éléments sur l'étude des sous-groupes finis de $SO_3(\mathbb{R})$.**
- 6.3. **Quaternions, $SO_3(\mathbb{R})$ et $SO_4(\mathbb{R})$.**
- 6.4. **Classification des coniques euclidiennes affines.** Lire le cours : Coste

SUGGESTIONS D'EXERCICES
ACTIONS DE GROUPES, THÉORÈMES DE SYLOW

Exercice 1 (Des petites questions).

On considère l'action d'un groupe G sur un ensemble E .

1. Montrer qu'un sous-ensemble de E est globalement stable par G si et seulement s'il est réunion d'orbites.
2. Montrer que deux éléments dans la même orbite ont des stabilisateurs conjugués.
3. Montrer que deux éléments conjugués dans le groupe G fixent le même nombre d'éléments.

Exercice 2 (La réciproque du théorème de Lagrange).

1. Le groupe symétrique \mathfrak{S}_5 a-t-il un élément d'ordre 6 ?
2. Chercher dans un groupe symétrique un contre-exemple à la réciproque du théorème de Lagrange sur l'ordre d'un élément dans un groupe.

Exercice 3.

On fixe une action d'un groupe G sur un ensemble fini E . On suppose que l'ordre de G est 15, que le cardinal de E est 17 et que E n'a pas de point fixé par tous les éléments du groupe G . Déterminer le nombre d'orbites et le cardinal de chacune d'elles.

Exercice 4.

1. Soit G un p -groupe agissant sur un ensemble fini E . Montrer que le cardinal de l'ensemble des points fixes de l'action est congru, modulo p , au cardinal de E .
2. En considérant une action de G sur lui-même, montrer que le théorème de Burnside : le centre d'un p -groupe non réduit à l'élément neutre n'est pas réduit à l'élément neutre.

Exercice 5 (Groupe dérivé).

Soit G un groupe. On appelle groupe des commutateurs de G et l'on note $D(G)$ le sous-groupe de G engendré par les éléments de la forme $xyx^{-1}y^{-1}$. Montrer que $D(G)$ est distingué dans G et que le quotient $G/D(G)$ est abélien. Montrer que $D(G)$ est le plus petit sous-groupe distingué de G tel que le quotient de G par ce sous-groupe soit abélien.

Exercice 6 (Groupe d'ordre p^2).

1. Montrer que si le quotient d'un groupe par son centre est cyclique alors le groupe est abélien, donc égal à son centre.
2. Montrer qu'un groupe d'ordre p^2 est abélien.

Exercice 7 (Groupe d'ordre p^3).

Soit G un groupe non abélien d'ordre p^3 où p est un nombre premier.

1. Montrer que le centre de G est d'ordre p et égal à son sous-groupe dérivé $Z(G) = D(G)$.
2. En déduire que le nombre de classes de conjugaison est $p^2 + p - 1$. (On pourra étudier l'action de G sur lui-même par conjugaison : ses points fixes, l'orbite des éléments, le stabilisateur des éléments et appliquer la formule de Burnside...)
3. Montrer que $G/Z(G)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
4. Montrer que tout sous-groupe de G d'ordre p^2 contient le centre $Z(G)$ de G , et que donc G n'est pas un produit semi-direct de son centre par son abélianisé. [Voir sur les groupes d'ordre \$p^3\$](#)

Exercice 8.

1. En comptant le nombre de base de \mathbb{F}_p^n déterminer le cardinal de $GL(n, \mathbb{F}_p)$.
2. Montrer que l'ensemble des matrices triangulaires supérieures strictes est un p -sous-groupe de Sylow de $GL(n, \mathbb{F}_p)$.

Exercice 9.

1. Vérifier que les p -Sylow de $GL(2, \mathbb{F}_p)$ sont monogènes.
2. Soit A et B deux matrices de $GL(2, \mathbb{F}_p)$ d'ordre p . Montrer que A est conjuguée à une puissance de B .

Exercice 10.

Soit p un nombre premier et m un entier non multiple de p . Soit G un groupe de cardinal $|G| = p^d m$.

1. Montrer que le nombre de p -Sylow de G divise m .
2. Montrer que pour tout $0 \leq i \leq d$, G possède un sous groupe d'ordre p^i .

Exercice 11.

Déterminer les sous-groupes de Sylow de $\mathbb{Z}/24\mathbb{Z}$.

Exercice 12 (Groupes de matrices sur \mathbb{F}_2).

1. Décrire un 2-Sylow de $GL_3(\mathbb{F}_2)$.
2. Soit $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Montrer que le polynôme minimal de A est irréductible de degré 3. En déduire que $GL_3(\mathbb{F}_2) \cap \mathbb{F}_2[A]$ est un 7-Sylow de $GL_3(\mathbb{F}_2)$.
3. Déterminer un 3-Sylow de $GL_3(\mathbb{F}_2)$ à l'aide de la matrice $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

GROUPES DIÉDRAUX ; PRODUIT SEMI-DIRECT

Exercice 13 (Exemples de sous-groupes caractéristiques).

1. Montrer qu'un p -Sylow distingué est caractéristique.
2. Soit H un sous-groupe distingué d'un groupe fini G tel que son ordre est premier avec son indice. Montrer alors que H est le seul sous-groupe d'ordre $|H|$ et donc que H est caractéristique.

Exercice 14 (Produit semi-direct interne).

Soit N un sous-groupe distingué d'un groupe G ($N \triangleleft G$) et H un sous groupe de G tel que $H \cap N = \{e_G\}$.

1. Montrer que NH est un sous-groupe de G .
2. On suppose désormais que $|G| = |N||H|$. Montrer que $\varphi : N \times H \rightarrow G, (n, h) \mapsto nh$ est une bijection.
3. Montrer que si on munit $N \times H$ de la loi

$$(n, h) \star (n', h') = (n(hn'h^{-1}), hh'),$$

alors $N \times H$ est un groupe et φ un isomorphisme de groupes.

Exercice 15 (Groupes d'automorphismes).

1. Montrer que les automorphismes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont obtenus par multiplication par un inversible de $(\mathbb{Z}/n\mathbb{Z}, \times)$.
2. Décrire un isomorphisme de $\mathbb{Z}/10\mathbb{Z}$ sur $(\mathbb{Z}/11\mathbb{Z})^*$.
3. Montrer que si G et H sont deux groupes d'ordre premiers entre eux, alors

$$Aut(G \times H) = Aut(G) \times Aut(H).$$

4. En déduire le groupe des automorphismes de $\mathbb{Z}/133\mathbb{Z}$.

5. Soit p un nombre premier et n un entier naturel non nul. Montrer que

$$\text{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = GL(n, \mathbb{F}_p).$$

6. Montrer que $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rightarrow \text{Bij}((1, 0), (1, 1), (0, 1))$ est un isomorphisme.

Exercice 16 (Exemple de produits semi-directs).

1. Montrer que, après avoir fixé un générateur de $(\mathbb{Z}/11\mathbb{Z})^*$, la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $\text{Aut}(\mathbb{Z}/11\mathbb{Z})$ revient à la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/10\mathbb{Z}$.
2. En déduire une structure de produit semi-direct sur $\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$.
3. Montrer que toutes les structures de produit semi-direct donnent des groupes isomorphes. *On pourra montrer que si $\varphi, \psi \in \text{Hom}(\mathbb{Z}/5\mathbb{Z}, \text{Aut}(\mathbb{Z}/11\mathbb{Z}))$ alors il existe $\gamma \in \text{Aut}(\mathbb{Z}/11\mathbb{Z})$ tel que $\psi(h) = \gamma \circ \varphi(h) \circ \gamma^{-1}$.*
4. Montrer que tous les morphismes de $\mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ sont de la forme $t \mapsto \{x \mapsto k^t x\}$ où k est un élément de $(\mathbb{Z}/q\mathbb{Z})^*$ d'ordre p .

GROUPES D'ORDRE INFÉRIEUR À 12

Exercice 17 (Des petites questions).

1. Soit p un nombre premier. Déterminer à isomorphisme près, tous les groupes d'ordre p .
2. Soit p un nombre premier. Déterminer à isomorphisme près, tous les groupes d'ordre p^2 .
3. Donner des exemples de groupes d'ordre 6 non abéliens.
4. Déterminer l'ordre des groupes diédraux D_n .
5. Déterminer l'ordre des groupes alternés \mathfrak{A}_n .

Exercice 18 (Étude de \mathfrak{S}_3).

Donner les structures de cycles possibles dans \mathfrak{S}_3 , le nombre d'éléments de \mathfrak{S}_3 ayant cette structure, et leur signature. Décrire les sous-groupes de \mathfrak{S}_3 , et ceux qui sont distingués dans \mathfrak{S}_3 .

Déterminer les sous-groupes de Sylow de \mathfrak{S}_3 .

Exercice 19 (Groupes d'ordre 6).

Soit G un groupe d'ordre 6.

1. Montrer que G admet un élément τ d'ordre 2 et un élément σ d'ordre 3.
2. Quelles sont les valeurs possibles de $\tau\sigma\tau$?
3. Déterminer, dans chacun des cas précédents, la structure de G à isomorphisme près.

Exercice 20 (Étude de \mathfrak{S}_4).

Donner les structures de cycles possibles dans \mathfrak{S}_4 , le nombre d'éléments de \mathfrak{S}_4 ayant cette structure, et leur signature. Déterminer les sous-groupes distingués de \mathfrak{S}_4 . En déduire que \mathfrak{A}_4 n'est pas un groupe simple, i.e. qu'il possède des sous-groupes distingués autres que $\{e\}$ et \mathfrak{A}_4 .

Déterminer les sous-groupes de Sylow de \mathfrak{S}_4 .

Exercice 21.

Soit p un nombre premier impair, on se propose de décrire les groupes d'ordre p^2 à isomorphisme près.

- (1) Soit G un groupe de cardinal p^2 , montrer que, ou bien G est cyclique ou bien tous les éléments différents de l'élément neutre sont d'ordre p .
- (2) Soit G un groupe non cyclique d'ordre p^2 , soit K un sous-groupe d'ordre p , montrer que K est distingué dans G et qu'il existe H sous-groupe d'ordre p tel que $K \cap H = \{e\}$. En déduire que G est isomorphe à un produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$.
- (3) Montrer que tout groupe de cardinal p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 22 (Groupes d'ordre pq).

Soit G un groupe d'ordre pq , où p et q sont deux nombres premiers distincts. On suppose que $p < q$.

1. Montrer qu'il n'y a qu'un q -Sylow Q et qu'il est distingué.
2. Montrer que G est produit semi-direct $Q \rtimes P$ où P est un p -Sylow de G .
3. Si p ne divise pas $q - 1$, déterminer la structure de G .
4. Si $p = 2$, déterminer le morphisme structurel $\varphi : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Déterminer alors la structure de G .
5. Si p divise $q - 1$, montrer qu'il n'y a qu'un seul produit semi-direct non abélien, à isomorphisme près.

Exercice 23 (Groupe non abélien d'ordre 8).

Soit G un groupe d'ordre 8.

1. Enumérer quatre groupes d'ordre 8, deux à deux non isomorphes, et même 5 si possible.
2. On suppose que tous les éléments de G sont d'ordre 2. Montrer que G est abélien. Soit a et b deux éléments non neutres distincts de G . Montrer que $\{e, a, b, ab\}$ est un sous-groupe d'ordre 4 de G . Déterminer un isomorphisme de G avec un groupe connu.
3. On suppose que G admet un élément a d'ordre 4. Soit b un élément hors du sous-groupe engendré par a . Montrer que $\langle a \rangle$ est distingué et que b^2 appartient à $\langle a \rangle$.
 - (a) Quel est l'ordre de b si $b^2 = a$ ou si $b^2 = a^3$? Conclure dans ce cas.
 - (b) Si $b^2 = e$, montrer que G est un produit semi-direct et en déduire un isomorphisme avec un groupe connu.
 - (c) Si tous les éléments hors de $\langle a \rangle$ ont un carré égal à a^2 , établir la liste des éléments et la table de multiplication de G à l'aide seulement de a et b .

Exercice 24 (Groupe non abélien d'ordre 8).

Soit G un groupe non abélien d'ordre 8.

1. Montrer que G contient un élément d'ordre 4. Soit H le sous-groupe qu'il engendre.
2. Montrer que si $G - H$ contient un élément d'ordre 2, G est un produit semi-direct. Après avoir vérifié que $\text{Aut}(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, montrer qu'il existe une unique structure de tel produit semi-direct non abélien.
3. Montrer que si $G - H$ n'a pas d'élément d'ordre 2, on retrouve la table de \mathbb{H}_8 en choisissant i l'élément d'ordre 4 qui engendre H et j un élément d'ordre 4 dans $G - H$. On pourra montrer que i^2 est le seul élément d'ordre 2 est qu'il est donc central. On le notera -1 .

Exercice 25 (Les groupes d'ordre 10).

Soit G un groupe d'ordre 10.

1. Montrer que G est un produit semi-direct.
2. Déterminer les automorphismes d'ordre 2 de $\mathbb{Z}/5\mathbb{Z}$.
3. En déduire les deux possibilités pour les classes d'isomorphismes de G .

Exercice 26 (Les groupes d'ordre 33).

Déterminer à isomorphisme près tous les groupes d'ordre 33. (On pourra déterminer le nombre de sous-groupe d'ordre 11 et le nombre de sous-groupe d'ordre 3.)

SIMPLICITÉ

<http://agreg-maths.univ-rennes1.fr/documentation/docs/Simple.pdf>

Exercice 27.

Montrer qu'un groupe d'ordre 63 n'est pas simple.

Exercice 28 (Les cycles d'ordre 3 engendrent \mathfrak{A}_n).

Soit n un entier naturel supérieur à 3, \mathfrak{S}_n le groupe symétrique de n lettres et \mathfrak{A}_n le groupe alterné.

1. Calculer les produits de transpositions $(a, b)(b, c)$, puis $(a, b)(c, d)$.
2. Montrer que les cycles d'ordre 3 engendrent \mathfrak{A}_n .

Exercice 29 (Groupes symétriques).

Soient n un entier naturel supérieur à 3.

1. Montrer que les permutations $(i, j)(j, k)$ et $(i, j)(k, l)$ s'écrivent comme produit de 3-cycles.
2. En déduire que le groupe alterné \mathfrak{A}_n est engendré par les 3-cycles.
3. Montrer que si $n \geq 5$, tous les 3-cycles sont conjugués dans \mathfrak{A}_n .

Exercice 30.

1. Le groupe \mathfrak{S}_n est-il simple ?
2. Le groupe $\mathbb{Z}/89\mathbb{Z}$ est-il simple ?
3. Le groupe $\mathbb{Z}/221\mathbb{Z}$ est-il simple ?

Exercice 31 (Simplicité de \mathfrak{A}_5).

- (1) Faire la liste des classes de conjugaison de \mathfrak{S}_n dans \mathfrak{A}_n en les dénombrant.
- (2) Montrer que les 3-cycles sont conjugués dans \mathfrak{A}_n .
- (3) Montrer que les éléments d'ordre 2 sont conjugués dans \mathfrak{A}_n .
- (4) Montrer que tout sous-groupe distingué H de \mathfrak{A}_n qui contient un élément d'ordre 5 les contient tous. (On remarquera que le groupe engendré par un élément d'ordre 5 est un Sylow.)
- (5) Montrer que tout sous-groupe distingué H de \mathfrak{A}_n non réduit à $\{\text{id}\}$ contient au moins deux types d'éléments en plus de l'identité. Montrer alors que $H = \mathfrak{A}_n$.

GROUPES DÉRIVÉS, RÉSOLUBILITÉ

On rappelle que le groupe dérivé $D(G)$ d'un groupe G est le groupe sous-groupe engendré par les commutateurs. C'est un sous-groupe caractéristique. On définit par récurrence le $k + 1$ ème groupe dérivé de G comme le groupe dérivé du k ème groupe dérivé $D^k(G)$ de G . On dit qu'un groupe est résoluble, si l'un des ses groupes dérivés est réduit à un élément.

Exercice 32 (Généralités).

1. Montrer que le groupe des matrices triangulaires supérieures de diagonale identité est résoluble.
2. Montrer que si H est un sous-groupe distingué d'un groupe G , alors G est résoluble si et seulement si H et G/H le sont. (On pourra commencer par le cas où G/H est abélien).
3. Montrer qu'un p -groupe est résoluble.

Exercice 33.

- (1) L'ensemble des permutations de profil $(\cdot, \cdot)(\cdot, \cdot)$ avec l'identité est-il un sous-groupe distingué de \mathfrak{A}_6 . (Justifier)
- (2) Donner l'exemple d'un groupe résoluble.
- (3) Donner si possible l'exemple d'un groupe simple résoluble.
- (4) Donner si possible l'exemple d'un groupe simple résoluble non abélien.

Exercice 34 (Groupe triangulaire supérieur).

- (1) Montrez que le groupe de Heisenberg H des matrices 3×3 triangulaires supérieures dont les coefficients diagonaux sont égaux à 1, est résoluble.
- (2) Montrez que le groupe B des matrices triangulaires supérieures 3×3 inversibles (coefficients diagonaux non nuls) est résoluble.

Exercice 35 (groupes dérivés de \mathfrak{S}_4).

Le but de l'exercice est de déterminer les groupes dérivés successifs de \mathfrak{S}_4 . On notera V_4 le sous-groupe des permutations de profil $(\cdot, \cdot)(\cdot, \cdot)$ (avec l'identité).

- (1) Montrer que $D(\mathfrak{S}_4) \subset \mathfrak{A}_4$.
- (2) Calculer les commutateurs $(1, 2)(1, 3)(1, 2)^{-1}(1, 3)^{-1}$ et $(1, 2, 3)(1, 2, 4)(1, 2, 3)^{-1}(1, 2, 4)^{-1}$.
- (3) Montrer que $D(\mathfrak{S}_4) = A_4$.
- (4) Montrer que $V_4 \subset D(\mathfrak{A}_4)$.
- (5) Vérifier que V_4 est distingué dans \mathfrak{A}_4 et que le quotient \mathfrak{A}_4/V_4 est un groupe abélien. En déduire que $D(\mathfrak{A}_4) \subset V_4$.
- (6) En déduire $D^2(\mathfrak{S}_4)$.
- (7) Calculer les autres groupes dérivés de \mathfrak{S}_4 .

Exercice 36 (Résolubilité).

1. Montrer que \mathfrak{S}_3 est résoluble.
2. Montrer que le groupe D_4 des permutations de profil $(\cdot, \cdot)(\cdot, \cdot)$ est un groupe abélien d'ordre 4 distingué dans A_4 . En déduire que \mathfrak{A}_4 et donc \mathfrak{S}_4 sont résolubles.
3. On suppose désormais $n \geq 3$. Soit c un 3 cycle. En considérant c^2 , montrer que c est un commutateur dans \mathfrak{S}_n . En déduire le sous groupe dérivé $D(\mathfrak{S}_n)$.
4. Montrer que pour $n \geq 5$, \mathfrak{A}_n et \mathfrak{S}_n ne sont pas résolubles.

Exercice 37 (Groupe d'ordre pqr).

Soit $p > q > r$ trois nombres premiers. Le but de l'exercice est de montrer qu'un groupe d'ordre pqr est résoluble.

- (1) Montrer qu'un groupe d'ordre pq est résoluble.
- (2) Soit G un groupe d'ordre pqr . Supposons qu'il n'admette pas de sous-groupe distingué. On note N_p (resp. N_q, N_r) le nombre de sous-groupes de Sylow d'ordre p (resp. q, r). Montrer que $m_p = qr, m_q \geq p$ et $m_r \geq q$.
- (3) Conclure.

GÉNÉRATEURS DE $SL(E)$, SIMPLICITÉ ET RÉVOLUBILITÉ DE $PSL(E)$

<http://agreg-maths.univ-rennes1.fr/documentation/docs/transvections.pdf>

Exercice 38 (Groupes linéaires).

Soit E un k -espace vectoriel. Soit f une forme linéaire sur E et a un élément non nul de $H = \ker(f)$. On appelle transvection associée à f et a l'application $u : E \rightarrow E, x \mapsto x + f(x)a$. On rappelle que les transvections de E engendrent $SL(E)$.

1. Soit u une transvection. En considérant une base (e_i) de E avec $e_{n-1} = a, (e_j)_{1 \leq j \leq n-1}$ base de H , et e_n tel que $f(e_n) = 1$, écrire la matrice de u .
2. Montrer que si u est une transvection, $\text{Ker}(u - Id) = H, \det u = 1, u$ n'est pas diagonalisable.
3. Montrer que si $\dim E \geq 3$, les transvections de E sont conjuguées dans $SL(E)$.
4. On suppose k de caractéristique différente de 2 et $\dim E \geq 3$. Montrer que

$$D(GL(E)) = D(SL(E)) = SL(E)$$

et donc que ni $GL(E)$, ni $SL(E)$ ne sont résolubles.

Exercice 39 (Groupe dérivé de $GL(3, \mathbb{F}_2)$ et de $SL(3, \mathbb{F}_2)$).

(1) Soit

$$t = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } s = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Montrer que le commutateur $tst^{-1}s^{-1}$ est une transvection.

(2) Rappeler la démonstration du fait que deux transvections de $SL(3, \mathbb{F}_2)$ sont conjuguées dans $SL(3, \mathbb{F}_2)$.

(3) Déterminer $D(SL(3, \mathbb{F}_2))$

(4) Déterminer $D(GL(3, \mathbb{F}_2))$.

Exercice 40 (Groupe dérivé de $GL(2, k)$).

On travaille dans $GL(2, k)$ pour un corps k qui a au moins 4 éléments. Soit $g \in GL(2, k)$. On notera i_g l'automorphisme intérieur donné par g .

(1) Démontrer qu'il existe un scalaire non nul $a \in k$ tel que $a^2 \neq 1$. Que se passe-t-il dans \mathbb{F}_2 et dans \mathbb{F}_3 ?

(2) Soit

$$t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } s = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Montrer que $T = tst^{-1}s^{-1}$ est une transvection.

(3) Soit τ une transvection de $SL(2, k)$. Il existe $g \in GL(2, k)$ tel que $\tau = i_g(T) := gTg^{-1}$. Calculer τ à l'aide de g , s et t et montrer que $D(SL(2, k))$ contient toutes les transvections.

(4) Déterminer $D(SL(2, k))$.

(5) Déterminer $D(GL(2, k))$.

Exercice 41 (Groupe dérivé de $GL(2, \mathbb{F}_3)$).

On travaille dans $GL(2, \mathbb{F}_3)$.

(1) Soit

$$t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Calculer $tst^{-1}s^{-1}$.

(2) Déterminer $D(GL(2, k))$. Noter que ce calcul ne suffit pas pour déterminer $D(SL(2, k))$.

REPRÉSENTATION LINÉAIRE DES GROUPES FINIS

http://agreg-maths.univ-rennes1.fr/journal/2018/representations_lineaires_des_groupes_finis.pdf

THÉORÈME FONDAMENTAL DES FONCTIONS SYMÉTRIQUES

https://math.unice.fr/~walter/L3_Alg_Arith/cours2.pdf
<http://agreg-maths.univ-rennes1.fr/documentation/docs/pol.pdf>

ANNEAU $\mathbb{Z}/n\mathbb{Z}$: THÉORÈME CHINOIS, AUTOMORPHISMES, INDICATRICE D'EULER, INVERSIBLES

Exercice 42.

Énoncer et démontrer le théorèmes des deux carrés. (voir par exemple <https://perso.univ-rennes1.fr/christophe.mourougane/enseignements/2010-11/AR3/polyAR3.pdf>)

Exercice 43 (Des petites questions).

1. L'entier 374 divise-t-il l'ordre du groupe $\mathbb{Z}/374\mathbb{Z}$? Le groupe $\mathbb{Z}/374\mathbb{Z}$ a-t-il un élément d'ordre 374? a-t-il un élément d'ordre 187?
2. Déterminer tous les diviseurs de 374? Le groupe $\mathbb{Z}/374\mathbb{Z}$ a-t-il un sous-groupe d'ordre chacun des diviseurs de 374?

IRRÉDUCTIBILITÉ DES POLYNÔMES CYCLOTOMIQUES SUR \mathbb{Q}

<http://agreg-maths.univ-rennes1.fr/documentation/docs/Cyclotomiques.pdf>

GÉNÉRALITÉS SUR LES CORPS

THÉORIE ÉLÉMENTAIRE DES CORPS FINIS

<https://lectures.lionel.fourquaux.org/2012-2013/thno/td1.pdf>

DÉCOMPOSITION DE JORDAN-CHEVALLEY

http://agreg-maths.univ-rennes1.fr/journal/2016/jordan_chevalley.pdf
http://agreg-maths.univ-rennes1.fr/documentation/docs/Jordan_algor.pdf

ENDOMORPHISMES CYCLIQUES ET RÉDUCTION DE FROBENIUS

<http://agreg-maths.univ-rennes1.fr/documentation/docs/Alg.Lin.pdf>
http://agreg-maths.univ-rennes1.fr/documentation/docs/endom_cycliques.pdf

ENDOMORPHISMES SEMI-SIMPLES, ENDOMORPHISMES UNIPOTENTS

<http://agreg-maths.univ-rennes1.fr/documentation/docs/matpass.pdf>
<http://agreg-maths.univ-rennes1.fr/documentation/docs/semisimples.pdf>
<http://agreg-maths.univ-rennes1.fr/documentation/docs/Alg.Lin.pdf>
http://agreg-maths.univ-rennes1.fr/documentation/docs/endom_semi_simples.pdf

Exercice 44 (Groupe unipotent).

1. À quel groupe le groupe U des matrices de la forme $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ avec $x \in \mathbb{R}$ est-il isomorphe ?
2. Est-ce un sous-groupe normal de $SL(2, \mathbb{R})$?
3. Déterminer l'inverse de $\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$.

ENDOMORPHISMES NORMAUX

DÉCOMPOSITION POLAIRE DES MATRICES

Exercice 45 (Décomposition polaire d'un endomorphisme).

Soit H un espace hermitien et a un endomorphisme inversible de H . Montrer que a s'écrit de façon unique sous la forme $a = hu$ où h est un endomorphisme auto-adjoint positif et u unitaire. Déterminer h et u pour l'endomorphisme a dont la matrice dans la base canonique de \mathbb{C}^2 est $\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$.

EXPONENTIELLE DE MATRICES ; SURJECTIVITÉ DE $\exp : M_n(\mathbb{C}) \rightarrow GL_n(\mathbb{C})$

<http://agreg-maths.univ-rennes1.fr/documentation/docs/Exponentielle.pdf>

GÉNÉRALITÉS SUR LES FORMES BILINÉAIRES ET SESQUILINÉAIRES

<http://agreg-maths.univ-rennes1.fr/documentation/docs/Quadrarev.pdf> <http://agreg-maths.univ-rennes1.fr/documentation/docs/matpass.pdf>

Exercice 46 (Forme alternée).

Une forme bilinéaire f sur un k -espace vectoriel E est dite alternée, si tout vecteur de E est isotrope. Soit (E, f) un k -espace vectoriel de dimension finie muni d'une forme bilinéaire alternée.

1. Soit (V, f) un k -espace vectoriel de dimension 2, muni d'une forme alternée non-dégénérée. Soit x un vecteur non nul. Montrer qu'il existe un vecteur isotrope y tel que $f(x, y) = 1$. On dit alors que (V, f) est un plan symplectique.
2. Soit V un sous-espace vectoriel de E . Montrer que si $(V, f|_V)$ est un espace non singulier (i.e. $f|_V$ non dégénérée) alors $E = V \oplus V^\perp$.

3. Montrer que E est somme directe orthogonale de droites isotropes et de plans symplectiques.
4. Montrer que tous les sous-espaces isotropes maximaux de E ont même dimension. Déterminer cette dimension en fonction de la dimension de E et du rang de f .
5. Retrouver ce résultat en utilisant le théorème de Witt symplectique : Soit (E, f) et (E', f') deux k -espaces vectoriels de dimension finie muni d'une forme symplectique (i.e. bilinéaire alternée non-dégénérée). On suppose (E, f) et (E', f') isométriques. Alors, toute isométrie d'un sous-espace de (E, f) sur un sous-espace de (E', f') se prolonge en une isométrie de (E, f) sur (E', f') .

Exercice 47.

Montrer qu'en dimension 2 le groupe symplectique d'une forme alternée non dégénérée est isomorphe au groupe spécial linéaire $SL(2, k)$.

Exercice 48.

1. Les formes bilinéaires symétriques données par les formes quadratiques suivantes sur \mathbb{F}_7^3 sont-elles équivalentes ?

$$q(x, y, z) = x^2 + 6y^2 + 2z^2$$

et

$$Q(x, y, z) = xy + 4z^2.$$

2. Montrer que deux formes quadratiques équivalentes sur un espace E prennent les mêmes valeurs dans k .
3. La forme q prend-elle toutes les valeurs de \mathbb{F}_7 ? Vérifier qu'elle prend les valeurs 3 et 5.

Exercice 49.

1. Montrer que deux formes quadratiques équivalentes sur un espace E prennent les mêmes valeurs dans k .
2. Soit dans tout l'exercice (E, f) un espace muni d'une forme bilinéaire symétrique non dégénérée de forme quadratique associée q . Montrer que si f admet un vecteur non nul isotrope, la forme q prend toutes les valeurs de k .
3. Montrer que E se décompose comme somme directe orthogonale de plans hyperboliques et d'un sous-espace sur lequel la forme quadratique n'a pas de vecteur isotrope non nul.
4. Montrer que le nombre de plans hyperboliques dans une telle décomposition est indépendant de la décomposition.

ALGORITHME DE GRAM-SCHMIDT ET DÉCOMPOSITION QR (ORTHOGONALE \times TRIANGULAIRE)

<http://agreg-maths.univ-rennes1.fr/documentation/docs/gramschmi.pdf>

ALGORITHME DE GAUSS ET LOI D'INERTIE DE SYLVESTER

ENDOMORPHISMES ORTHOGONAUX ET UNITAIRES

Soit $\langle \cdot, \cdot \rangle$ le produit hermitien canonique de \mathbb{C}^2 (i.e la forme sesquilinéaire (\mathbb{C} -linéaire par rapport au premier argument et \mathbb{C} -anti-linéaire par rapport au second) à symétrie hermitienne définie positive de matrice Id dans la base canonique)

$$\forall (X, Y) \in (\mathbb{C}^2)^2, \langle X, Y \rangle = {}^t X Id Y = {}^t X \bar{Y}.$$

On notera, pour toute matrice $M \in M(2, \mathbb{C})$, $M^* := {}^t \bar{M}$ l'adjoint de M i.e.

$$\forall (X, Y) \in (\mathbb{C}^2)^2, \langle MX, Y \rangle = \langle X, M^* Y \rangle.$$

On rappelle que le groupe spécial unitaire $SU(2)$ est le sous-groupe du groupe spécial linéaire complexe $SL(2, \mathbb{C})$ des matrices qui respectent le produit hermitien canonique de \mathbb{C}^2 i.e.

$$\begin{aligned} \forall (X, Y) \in (\mathbb{C}^2)^2, \langle PX, PY \rangle &= \langle X, Y \rangle. \\ SU(2) &:= \{P \in M(2, \mathbb{C}) / \det P = 1 \text{ et } P^* P = Id\}. \end{aligned}$$

Exercice 50 (Le groupe $SO(2)$).

1. Rappeler un isomorphisme de groupes entre $SO(2)$ et S^1 .

2. L'application $SO(2) \rightarrow SO(2), A \mapsto A^2$ est-elle un morphisme de groupes ? Déterminer son image et son noyau.

Exercice 51 (L'espace V des matrices anti-hermitiennes de trace nulle).

1. Déterminer la nature de l'espace vectoriel V des matrices anti-hermitiennes (i. e. $M^* := -M$) de $M(2, \mathbb{C})$ de trace nulle.
2. Écrire la forme générale d'une matrice de V à l'aide de trois nombres réels. En déduire une base de V .
3. Montrer que $\langle\langle P, P' \rangle\rangle := -\frac{1}{2}\text{trace}(PP')$ définit un produit scalaire sur V .

Exercice 52 (Le groupe $SU(2)$).

1. Soit $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SU(2)$. Montrer que $c = -\bar{b}$, $d = \bar{a}$ et $\bar{a}a + \bar{b}b = 1$ et écrire la forme générale d'une matrice P de $SU(2)$ à l'aide de deux nombres complexes, puis de quatre nombres réels.
2. En déduire un homéomorphisme de $SU(2)$ sur la sphère unité S^3 de \mathbb{C}^2 . (On munit ici S^3 de la topologie induite par celle de \mathbb{C}^2 et $SU(2)$ de la topologie induite par la topologie d'une norme sur l'espace vectoriel $M(2, \mathbb{C})$.)
3. Soit $-1 < c < 1$. Décrire topologiquement le sous-espace de $SU(2)$ des matrices de trace c , appelé "latitude c ".
4. Montrer que les latitudes sont des classes de conjugaison dans $SU(2)$. (On pourra remarquer que les éléments de $SU(2)$ sont associés à des endomorphismes normaux (i.e. qui commutent avec leur adjoint)).
5. Quelles sont les autres classes de conjugaison ?
6. Décrire topologiquement le sous-groupe D des matrices diagonales de $SU(2)$.

Exercice 53 (Les groupes $SO(3)$ et $SU(2)$).

1. Montrer que la classe de conjugaison C de $SU(2)$ des matrices de trace nulle (i.e. la latitude 0) est la sphère unité de l'espace euclidien $(V, \langle\langle \cdot, \cdot \rangle\rangle)$ des matrices anti-hermitienne de trace nulle.
2. Montrer que $SU(2)$ agit par conjugaison sur l'espace V .
3. Montrer que cette action est transitive.
4. En déduire un morphisme de groupes φ de $SU(2)$ dans le groupe orthogonal de $(V, \langle\langle \cdot, \cdot \rangle\rangle)$.
5. Déterminer le noyau de φ .
6. En utilisant la connexité de $SU(2)$ montrer que l'image de φ est incluse dans $SO(V)$.
7. Montrer que l'image par φ du sous-groupe D des matrices diagonales de $SU(2)$ est le sous-groupe des rotations de V qui fixent $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$.
8. En déduire l'image de φ .

ENDOMORPHISMES SYMÉTRIQUES ET HERMITIENS

<http://agreg-maths.univ-rennes1.fr/documentation/docs/dirprin.pdf>
<http://agreg-maths.univ-rennes1.fr/documentation/docs/matpass.pdf>

GÉNÉRATEURS DE $O(E)$, $SO(E)$ ET SIMPLICITÉ DE $PSO(E)$

ISOMÉTRIES DU CUBE ; ISOMÉTRIES DU TÉTRAÈDRE. ÉLÉMENTS SUR L'ÉTUDE DES SOUS-GROUPES FINIS DE $SO_3(\mathbb{R})$

Exercice 54.

On cherche à décrire le groupe G des isométries d'un plan affine euclidien qui conservent globalement un triangle $\mathcal{T} = ABC$ isocèle en A non équilatéral non aplati.

1. Déterminer deux éléments différents du groupe G .

2. Soit f un élément de G .
 - (a) Montrer que f a un point fixe.
 - (b) Montrer que $f(A) = A$ et que $(f(B) = B \text{ ou } f(B) = C)$.
 - (c) Montrer que f est soit l'identité soit une réflexion.
3. Écrire la table de multiplication du groupe G .

Exercice 55.

Soit D_8 le groupe des isométries du carré. Déterminer un morphisme injectif de groupes de D_8 dans \mathfrak{S}_4 . Les éléments $(1, 3)$ et $(1, 2, 3, 4)$ engendrent-ils le groupe symétrique \mathfrak{S}_4 ?

Exercice 56 (Sylow des groupes diédraux).

Soit \mathcal{P}_n un polygone régulier à n côtés dans le plan euclidien orienté. On appelle groupe diédral D_n le groupe des isométries de \mathcal{P}_n .

1. Parmi les translations, les rotations, les symétries orthogonales, et les symétries glissées (composées d'une symétrie orthogonale et d'une translation dans l'axe de la symétrie), décrire des isométries du plan qui conservent le polygone régulier \mathcal{P}_n .
2. Déterminer, à l'aide de l'action naturelle de D_n sur l'ensemble des sommets de \mathcal{P}_n , le cardinal de D_n . En déduire la liste complète des éléments de D_n .
3. On suppose n impair. Déterminer les 2-Sylow de D_n et vérifier (sans référence au cours) qu'ils sont conjugués.
4. On suppose $n = 6$. Déterminer un 2-Sylow de D_6 . Déterminer le nombre de 2-Sylow de D_6 . Déterminer deux sous-groupes d'ordre 2 de D_6 non conjugués dans D_6 . Donner un 3-Sylow de D_6 .

Exercice 57 (Sous-groupe fini de $SO(3)$).

1. Montrer le *théorème de Burnside* : soit G un groupe fini agissant sur un ensemble fini E . Alors le nombre N d'orbites est la moyenne des cardinaux des points fixes des éléments de G et aussi

$$N = \frac{1}{|G|} \sum_{g \in G} \text{card } \text{Fix}(\varphi(g)) = \frac{1}{|G|} \sum_{x \in E} \text{card } \text{stabil}(x).$$

On pourra considérer $\{(x, g) \in E \times G / g \cdot x = x\}$.

2. Soit G un sous-groupe fini de $SO(3)$. On considère son action sur la sphère unité. Soit X l'ensemble des points fixés par un des éléments de G différents de l'identité. Montrer que X est stable par l'action de G . Montrer que le stabilisateur d'un élément de X est un groupe cyclique. On notera N le nombre d'orbites de l'action de G sur X et n_j le cardinal du stabilisateur d'un élément de l'orbite O_j .
3. Montrer que

$$N|G| = 2(|G| - 1) + \text{card } X.$$

4. Montrer que

$$2 - \frac{2}{|G|} = \sum_{j=1}^N \left(1 - \frac{1}{n_j}\right).$$

5. En déduire que $N = 2$ ou $N = 3$.
6. Montrer que si $N = 2$, G est un sous-groupe cyclique de rotations.
7. Si $N = 3$, déterminer les possibilités pour les n_j .

QUATERNIONS, $SO_3(\mathbb{R})$ ET $SO_4(\mathbb{R})$

<http://agreg-maths.univ-rennes1.fr/documentation/docs/quater.pdf>
<http://agreg-maths.univ-rennes1.fr/documentation/docs/agreg-quater.pdf>

Exercice 58 (Représentation matricielle des nombres complexes et des quaternions).

1. Déterminer dans $M(2, \mathbb{R})$ une matrice I telle que $I^2 = -Id$.
2. En déduire un morphisme non nul d'anneaux de \mathbb{C} dans $M(2, \mathbb{R})$.
3. Soit

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{et} \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Établir la table de multiplication de $G := \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$. Est-ce un groupe ? Est-il cyclique ?

4. La sous-algèbre \mathbb{H} de $M(2, \mathbb{C})$ engendré par G est-elle commutative ? un corps gauche ?

CLASSIFICATION DES CONIQUES EUCLIDIENNES AFFINES

Coste (*Coniques, quadriques projectives*),

<http://agreg-maths.univ-rennes1.fr/documentation/docs/coquproj.pdf>

Exercice 59 (Droites et quadriques).

Une quadrique d'un espace projectif $P(V)$ est le lieu des zéros d'une forme quadratique f sur V .

1. Montrer que toute quadrique qui contient trois points distincts d'une droite d contient toute la droite d .
2. Déterminer la dimension de l'espace des quadriques de $P^3(K)$.
3. Soit d_1, d_2, d_3 trois droites de $P^3(K)$. Montrer qu'il existe une quadrique qui les contient.

Exercice 60.

On considère le plan euclidien muni d'un repère orthonormé (O, \vec{i}, \vec{j}) et la courbe (C) d'équation

$$4x^2 - 4xy + y^2 - 3x - y - 1 = 0$$

1. Montrer que (C) est une parabole.
2. Trouver un repère orthonormé $(S, \vec{u}_1, \vec{u}_2)$ tel que (C) ait une équation de la forme $x^2 = 2py$ dans ce repère.

Exercice 61.

1. Construire à la règle et au compas la tangente à un cercle \mathcal{C} passant par un point A hors du disque délimité par \mathcal{C} .
2. Soit maintenant \mathcal{C} et \mathcal{C}' deux cercles non concentriques. Construire les centres Ω et O des homothéties qui envoient \mathcal{C} sur \mathcal{C}' .
3. Construire deux tangentes communes à \mathcal{C} et à \mathcal{C}' .