UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

Année universitaire 2014–2015

Licence 3ème année, HLMA501

Algèbre linéaire et théorie des groupes (Algèbre Générale 1)

Responsable du module : Sylvain Brochard

Sylvain Brochard
Bureau 307 (bâtiment 9)
Tél. : 04 67 14 35 51
Courriel : sylvain.brochard@univ-montp2.fr
Permanence : le mardi de 12h15 à 13h45

Département de Mathématiques
Université de Montpellier
Année universitaire 2014–2015

Plan du cours

I : Algèbre linéaire

1. Endomorphismes trigonalisables
2. Endomorphismes nilpotents
3. Applications (suites récurrentes linéaires, systèmes d'équations différentielles, exponentielle de matrice)

II : Théorie des groupes

4. Groupes : définition, morphismes, produits.
5. Sous-groupes.
6. Actions de groupes.
7. Groupe symétrique, groupes diédraux.
8. Classes modulo un sous-groupe, formule des classes.
9. Sous-groupes distingués, groupe quotient.
10. Groupes monogènes, groupes cycliques.
11. Théorèmes de Sylow. Groupes simples.

Références

L'algèbre linéaire comme la théorie des groupes sont des sujets extrêmement classiques. Il y a donc beaucoup d'ouvrages de référence. Je vous en propose deux ci-dessous mais bien sûr d'autres livres feraient parfaitement l'affaire. N'hésitez pas à chercher un peu dans les rayonnages de la BU. Pour la théorie des groupes, un polycopié de cours sera aussi distribué.

Algèbre linéaire : *Cours d'algèbre*, de Roger Godement, publié chez Hermann. Les paragraphes 34 (Vecteurs propres et valeurs propres) et 35 (Forme canonique d'une matrice) contiennent l'essentiel de ce que nous ferons en cours.

Théorie des groupes : *Éléments de théorie des groupes*, de Josette Calais.

Modalités de contrôle des connaissances

L'examen final aura lieu en janvier et durera 2h (la seconde session aura lieu en juin). La traditionnelle « règle du max » est utilisée pour calculer la note finale du module. Votre note finale sera donc

$$\max\left(E\,,\,\frac{3E+2CC}{5}\right)$$

où E est la note obtenue à l'examen final et CC est votre note de contrôle continu. Cette dernière (sur 20) est obtenue à partir des évaluations suivantes.

Examen partiel 1. Il aura lieu le mardi 14 octobre de 9h45 à 11h15 dans l'amphi 5.01. ..... **7 points**

Examen partiel 2. Il aura lieu le vendredi 28 novembre de 15h à 16h30 dans l'amphi 10.01. ... **7 points**

Interros. Il y aura deux petits contrôles de 20 minutes portant sur des questions de cours ou bien des exercices d'application immédiate. Les dates vous seront communiquées en temps utile. ..... **4 points**

Travail fourni en TD. Il sera évalué par l'enseignant de TD suivant des modalités de son choix, par exemple en se basant sur les critères suivants : efforts fournis pendant les séances, préparation des exercices à la maison, passage au tableau, assiduité, etc. ..... **2 points**

Étudiants en situation de handicap

Les étudiants en situation de handicap sont invités à venir m'en parler ou à se renseigner auprès du SAEPH pour connaître les possibilités d'aménagement.

Méthode de travail

Il existe bien sûr de nombreuses méthodes de travail différentes. L'une d'entre elles, par exemple, consiste à :

1. Venir régulièrement en cours et en TD.
2. Prendre des notes consciencieusement, même si l'on ne comprend pas tout (voire rien du tout), sans interrompre le prof. Ainsi on pourra toujours relire les notes plus tard.
3. Essayer de chercher un peu les exercices en TD (lorsque l'enseignant en laisse le temps), et profiter aussi de ce temps pour feuilleter les notes du cours magistral, en attendant la correction de l'exercice.
4. À l'approche de l'examen, commencer à relire les corrections, en tout cas au moins celles des « exercices type », puis essayer de les refaire.

Cette méthode est très répandue. L'expérience montre pourtant qu'elle **NE MARCHE PAS !** Elle « marchait » peut-être au lycée, voire en L1 ou L2 (et encore, ses adeptes auraient certainement pu avoir de meilleurs résultats en procédant autrement), mais en L3 on attend un niveau de compréhension supérieur. Il vous sera demandé, non seulement d'assimiler des connaissances et des techniques nouvelles, mais aussi de savoir utiliser ces connaissances et techniques pour résoudre *des problèmes nouveaux*. En particulier, l'examen final comportera majoritairement des exercices nouveaux (c'est-à-dire réellement différents de ceux vus en TD), que vous pourrez résoudre en utilisant les résultats et méthodes vues en cours et en TD. La résolution de ces exercices commence bien souvent par une phase de recherche au cours de laquelle on tâtonne un peu. Il faut généralement un peu (parfois beaucoup) d'imagination et d'esprit d'initiative pour trouver une solution. Il est **essentiel** de s'entraîner à cette phase de recherche, sans quoi vous ne pourrez probablement même pas commencer les exercices proposés. C'est pourquoi je vous propose plutôt la méthode de travail suivante.

1. Venez systématiquement en cours et en TD.
2. *Avant* chaque CM, lisez dans un livre ou dans le poly de cours les paragraphes qui correspondent au contenu du CM. Ainsi vous profiterez beaucoup mieux des explications orales en CM.
3. *Pendant* le CM, efforcez-vous activement de *tout* comprendre. Vous gagnerez ainsi beaucoup de temps à la maison. N'hésitez pas à interrompre l'enseignant pour lui demander des explications sur un ou plusieurs points obscurs (tout le monde vous en sera reconnaissant, à commencer par vos camarades qui n'ont sans doute pas compris non plus).
4. Après le CM, relisez vos notes de cours, et efforcez-vous de les comprendre en profondeur. Voici par exemple ce que vous pouvez faire pour améliorer votre compréhension du cours.
   (a) Pour chaque définition, essayez de trouver deux ou trois exemples pour être sûr que vous comprenez bien de quoi on parle. (Généralement le prof a donné lui-même quelques exemples pertinents...)
   (b) Essayez de faire chaque démonstration vous-même avant de la lire (au minimum, essayez de trouver des idées pour commencer). Puis lisez-la, en prenant garde à bien comprendre chaque argument, ainsi que la structure et l'articulation globale de la preuve. Essayez d'en retenir les idées maîtresses de manière à être en mesure de la retrouver (mais surtout ne l'apprenez pas par cœur, c'est parfaitement inutile). Vous alimentez ainsi votre réservoir à idées : en effet les exercices peuvent souvent être résolu en utilisant des idées ou des stratégies qui ont déjà servi dans le cours (ou sont proches).
   (c) Pour chaque énoncé (théorème, proposition, etc.) et chaque hypothèse de cet énoncé, posez-vous les deux questions suivantes : 1) Où cette hypothèse a-t-elle servi dans la démonstration ? 2) Cette hypothèse est-elle vraiment nécessaire ? (Souvent elle l'est... donc essayez de trouver un contre-exemple à l'énoncé lorsque l'on supprime l'hypothèse en question.)
   (d) À l'instar des démonstrations, chaque exemple traité en cours peut être vu comme un exercice résolu. Donc pour chacun d'entre eux, notez la question, puis cachez vos notes et essayez de retrouver la solution (éventuellement de tête si vous ne voulez pas y passer trop de temps...).
5. *Avant* chaque séance de TD, cherchez activement à résoudre les exercices qui seront corrigés pendant la séance de TD. C'est absolument essentiel, et ça vous fera progresser même (ou surtout) si vous n'arrivez pas à résoudre l'exercice. Faites preuve d'opiniâtreté (l'examen ne sera pas plus facile...). Ne laissez tomber qu'après avoir noirci plusieurs feuilles de brouillon.
6. *Pendant* le TD, soyez aussi actif possible. Cherchez en permanence à résoudre les exercices. Efforcez-vous de bien comprendre les solutions de ceux que vous n'aviez pas réussi à résoudre seul. N'hésitez pas à confronter vos idées avec celles de votre voisin (en *chuchotant*, pour respecter le travail des autres).
7. *Après* le TD, reprenez les exercices que vous n'aviez pas réussi à résoudre et posez-vous les deux questions suivantes : 1) Pourquoi n'ai-je pas réussi à le résoudre ? 2) Par quel cheminement de pensée aurais-je pu trouver tout seul la solution ? Ré-essayez quelques semaines plus tard (sans regarder la solution bien sûr).

Chapitre 1 : Endomorphismes trigonalisables (2CM, 2TD)

Contenu du cours. Quelques rappels sur les notions de valeur propre, vecteur propre, polynôme caractéristique, polynôme minimal, lemme des noyaux, diagonalisation (sans preuves). Définition d'un endomorphisme trigonalisable, caractérisation par le polynôme caractéristique. Sous-espaces caractéristiques.

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)

1. Donner la définition d'un endomorphisme trigonalisable.
2. Donner la définition des sous-espaces caractéristiques d'un endomorphisme.
3. À quelle condition sur son polynôme caractéristique χ_A une matrice A est-elle trigonalisable ?
4. Vrai ou faux ? (Donner une preuve ou un contre-exemple.)
   a) Si un endomorphisme f est diagonalisable, alors il est trigonalisable.
   b) Si un endomorphisme f est trigonalisable, alors il est diagonalisable.
   c) Si f est diagonalisable, alors χ_f est scindé à racines simples.
   d) Si f est trigonalisable, alors χ_f est scindé.
5. Les matrices suivantes sont-elles diagonalisables sur $\mathbb{R}$? trigonalisables sur $\mathbb{R}$? Et sur $\mathbb{C}$?

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

Exercice 1.1 (révisions sur la diagonalisation)

Déterminer pour quelles valeurs des paramètres a, $b \in \mathbb{R}$ les matrices suivantes sont diagonalisables :

$$A = \begin{pmatrix} 2 & a & 1 \\ 0 & -1 & b \\ 0 & 0 & 2 \end{pmatrix} \quad B = \begin{pmatrix} 3 & 0 & \dots & 0 & 1 \\ 0 & 3 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 3 & 0 \\ 0 & \dots & \dots & 0 & a \end{pmatrix} \quad C = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 2-a & a-2 & a \end{pmatrix}$$

On suppose $a = 2$. Calculer C^k pour tout $k \in \mathbb{N}$.

Exercice 1.2 (révisions sur la diagonalisation)

Soit $A := \begin{pmatrix} -5 & 3 \\ 6 & -2 \end{pmatrix}$. Montrer qu'il existe une matrice B telle que $B^3 = A$.

Exercice 1.3

Soit $A \in M_n(\mathbb{C})$, et $\lambda_1, \dots, \lambda_p$ les valeurs propres de A, de multiplicités $\alpha_1, \dots, \alpha_p$. Montrer que pour tout $k \geq 1$ on a $\mathrm{Tr}(A^k) = \sum_{i=1}^p \alpha_i \lambda_i^k$ et $\det(A^k) = \prod_{i=1}^p \lambda_i^{k\alpha_i}$. Lorsque $n = 2$, exprimer le polynôme caractéristique de A en fonction de $\mathrm{Tr}(A)$ et $\det(A)$. Montrer que ce résultat est vrai pour $A \in M_n(K)$, pour tout sous-corps K de $\mathbb{C}$. (*Il s'étend en fait à tout corps K*).

Exercice 1.4

Soit $A \in M_n(\mathbb{R})$. Montrer que si λ est valeur propre complexe de A alors $\bar{\lambda}$ l'est aussi avec la même multiplicité, et que si $v \in E_\lambda$ alors $\bar{v} \in E_{\bar{\lambda}}$. Application : déterminer une matrice réduite diagonale $A' \in M_n(\mathbb{C})$ semblable à

$$A = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

ainsi qu'une matrice de passage de A à A'.

Chapitre 2 : Endomorphismes nilpotents (2CM, 2TD)

Contenu du cours. Définition d'un endomorphisme nilpotent, indice de nilpotence. Caractérisations par le polynôme caractéristique ou le polynôme minimal. Un endomorphisme est nilpotent si et seulement s'il est trigonalisable et si 0 est sa seule valeur propre. Décomposition de Dunford. Étude des nilpotents par les noyaux itérés. Réduction de Jordan (sans preuve).

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Les matrices suivantes sont-elles nilpotentes ? Si oui, donner l'indice de nilpotence.

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 2 & -2 & 1 \\ 2 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

2. Énoncer le théorème de décomposition de Dunford.
3. Énoncer le théorème de réduction de Jordan.
4. Quelle est la décomposition de Dunford des matrices suivantes ?

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

5. À quelle condition sur son polynôme caractéristique un endomorphisme est-il nilpotent ?
6. Soit $A \in M_n(\mathbb{R})$. On suppose que $(A - \lambda \mathrm{Id})^n = 0$. Quelle est la décomposition de Dunford de A ?

Exercice 2.1
Soit

$$A_1 = \begin{pmatrix} 3 & -1 & 1 \\ 2 & 0 & 1 \\ 1 & -1 & 2 \end{pmatrix}, \; A_2 = \begin{pmatrix} 13 & -5 & -2 \\ -2 & 7 & -8 \\ -5 & 4 & 7 \end{pmatrix}.$$

1. Déterminer la décomposition de Jordan-Dunford de A_1 et A_2.
2. Calculer le polynôme minimal de A_1 et A_2.

Exercice 2.2
Déterminer toutes les matrices $A \in M_2(\mathbb{R})$ telles que $A^3 - 7A^2 + 15A - 9\mathrm{I}_2 = 0$.

Exercice 2.3
Montrer qu'un endomorphisme diagonalisable et nilpotent est nul.

Exercice 2.4
Montrer qu'une matrice $M \in M_n(\mathbb{C})$ est nilpotente si, et seulement si, pour tout $k \geq 1$ on a $\mathrm{tr}(M^k) = 0$.

Exercice 2.5
Montrer que la somme de deux endomorphismes nilpotents et qui commutent est un endomorphisme nilpotent.

Exercice 2.6
Soit $A \in M_6(\mathbb{C})$. On suppose que $P_A(X) = (X-2)^4(X-3)^2$ et $m_A(X) = (X-2)^2(X-3)$.

1. Que peut-on dire des dimensions des espaces propres de A ?
2. Quelles sont les formes de Jordan possibles pour A ?

Exercice 2.7
(*Construction d'une base de Jordan*).

1. Soit $f \in \mathrm{End(E)}$. On suppose que sa réduite de Jordan est formée par un seul bloc de Jordan,

$$J(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}.$$

   On pose $g = f - \lambda id_E$. Montrer qu'on obtient une base $\{v_1, \ldots, v_n\}$ de E dans laquelle la matrice de f est $J(\lambda)$ en prenant $v_n \in E \setminus \mathrm{Ker} g^{n-1}$, et $v_i = g(v_{i+1})$ pour tout $i = 1, \ldots, n-1$.
2. Déterminer une réduite de Jordan et une matrice de passage pour les matrices

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 4 & 1 & -2 \\ 2 & 1 & 2 & -1 \\ 1 & 2 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ -1 & 4 & 1 & -2 \\ 2 & 1 & 2 & -1 \\ 1 & 2 & 1 & 0 \end{pmatrix}.$$

Exercice 2.8

Soit f un endomorphisme nilpotent. Montrer que les conditions suivantes sont équivalentes :

1. L'ordre de f est égal à n (la dimension de E), c'est-à-dire $m_f(X) = X^n$.
2. Il existe un vecteur $x \in E$ non nul tel que la famille $\{x, f(x), f^2(x), \ldots, f^{n-1}(x)\}$ est une base de E (on dit que f est *cyclique*).
3. Il existe une base b de E dans laquelle $Mat(f)_b$ est un bloc de Jordan.

Exercice 2.9

Soit A la matrice de $M_4(\mathbb{R})$ suivante :

$$\begin{pmatrix} -2 & -1 & 1 & 2 \\ 1 & -4 & 1 & 2 \\ 0 & 0 & -5 & 4 \\ 0 & 0 & -1 & -1 \end{pmatrix}.$$

1. Montrer que $\chi_A(X) = (X+3)^4$. (*Indication : au lieu de développer le déterminant, regarder s'il n'y a pas une combinaison linéaire judicieuse des lignes pour le calculer plus facilement.*)
2. A est-elle diagonalisable ?
3. Déterminer une réduite de Jordan de A. (*Indication : commencer par calculer les dimensions des noyaux* $\ker M$, $\ker M^2, \ldots$ *pour* $M := A + 3I_4$.)
4. Préciser une matrice de passage pour cette réduction de Jordan.
5. Sans faire de calculs, et en utilisant la réduite de Jordan, donner le polynôme minimal de A.
6. En déduire que A^{-1} peut s'écrire comme un polynôme (du 2nd degré) en A.

Chapitre 3 : Applications (1CM, 2TD)

Contenu du cours. Calcul des puissances d'une matrice. Suites récurrentes linéaires. Systèmes d'équations différentielles. Exponentielle de matrice.

Exercice 3.1

Calculer l'exponentielle des matrices suivantes.

$$A = \begin{pmatrix} 1 & 4 & -2 \\ 0 & 6 & -3 \\ -1 & 4 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 2 & -3 \\ 5 & 1 & -5 \\ -3 & 4 & 0 \end{pmatrix}.$$

Exercice 3.2

Soit $M \in M_n(\mathbb{C})$. Donner une condition nécessaire et suffisante sur M pour que $\exp(tM)$ tende vers 0 quand $t \to +\infty$.

Exercice 3.3

Soit

$$A_1 = \begin{pmatrix} 3 & -1 & 1 \\ 2 & 0 & 1 \\ 1 & -1 & 2 \end{pmatrix}.$$

Résoudre le système différentiel $\frac{\mathrm{d}X}{\mathrm{d}t} = A_1 X$.

Exercice 3.4

Résoudre le système différentiel suivant :

$$\begin{cases} x'(t) &= x(t) + 4y(t) - 2z(t) \\ y'(t) &= 6y(t) - 3z(t) \\ z'(t) &= -x(t) + 4y(t) \end{cases}$$

Exercice 3.5

Résoudre de deux manières la récurrence linéaire suivante

$$u_{n+3} = -12u_n + 16u_{n+1} - 7u_{n+2}.$$

1. En calculant les puissances d'une matrice bien choisie (qu'il faudra donc d'abord réduire...).
2. En appliquant directement les résultats du cours sur les suites récurrentes linéaires.

Chapitre 4 : Groupes : définition, morphismes produits (2CM, 1TD)

Contenu du cours. Définition d'un groupe. Neutre, inverse, règles de calcul dans un groupe. Groupes commutatifs. Exemples de groupes : groupes de nombres ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.), groupes de transformations (permutations, isométries, etc.), groupes de matrices. Produit de groupes. Morphismes de groupes. Isomorphismes, automorphismes. « Propriété universelle du produit ». « Propriété universelle du groupe $\mathbb{Z}$ ».

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Donner la définition d'un groupe.
2. Montrer que l'élément neutre d'un groupe est unique.
3. De même, montrer que le symétrique (ou *inverse*) d'un élément $g \in G$ est unique.
4. $(\mathbb{N}^*, \times)$ est-il un groupe ?
5. Si $f : G \to H$ est un morphisme de groupes, montrer à partir de la définition que pour tout $x \in G$ et pour tout $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

Exercice 4.1

On considère sur $\mathbb{R}$ la loi de composition définie par $x \star y = x + y - xy$. Cette loi est-elle associative, commutative ? Admet-elle un élément neutre ? Un réel x admet-il un inverse pour cette loi ? Donner une formule pour la puissance n-ième d'un élément x pour cette loi.

Exercice 4.2

Soit E un ensemble muni d'une loi $\star$ associative
(i) admettant un élément neutre à gauche e (i.e. $\forall x \in E \quad e \star x = x$) et
(ii) tel que tout élément possède un inverse à gauche (i.e. $\forall x \in E \quad \exists y \in E \quad y \star x = e$).
Montrer que E est un groupe pour la loi $\star$.

Exercice 4.3

Montrer que l'ensemble des matrices carrées à n lignes et n colonnes de déterminant non nul est un groupe pour la multiplication.

Exercice 4.4

On considère l'ensemble E des matrices carrées à coefficients réels de la forme

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, \quad a \in \mathbb{R}^\times, \quad b \in \mathbb{R}$$

muni du produit des matrices.

(a) Montrer que E est ainsi muni d'une loi de composition interne associative.

(b) Déterminer tous les éléments neutres à droite de E.

(c) Montrer que E n'admet pas d'élément neutre à gauche.

(d) Soit e un élément neutre à droite. Montrer que tout élément de E possède un inverse à gauche pour cet élément neutre, i.e.

$$\forall g \in E \quad \exists h \in E \quad hg = e.$$

Exercice 4.5

Soit G un groupe dans lequel tout élément x vérifie $x^2 = e$. Montrer que G est commutatif.

Exercice 4.6

Parmi les paires $(G, \cdot)$ ci-dessous, déterminer celles qui sont des groupes :

1. $G = \mathbb{R}$, $x \cdot y = x + y - 3$;
2. $G = \mathbb{R}$, $x \cdot y = x - y + 5$;
3. $G = \mathbb{R}$, $x \cdot y = xy^2$;

4. $G =]-1,1[$, $x \cdot y = \frac{x+y}{xy+1}$;
5. $\mathbb{Q}^\times$, $x \cdot y = xy$;
6. $\{2^n \mid n \in \mathbb{Z}\}$, $x \cdot y = xy$;
7. $\{\frac{1+2m}{1+2n} \mid n, m \in \mathbb{Z}\}$, $x \cdot y = xy$.

Exercice 4.7

Montrer que l'application exponentielle $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est un isomorphisme de groupes. Qu'en est-il de l'application $\exp : (\mathbb{C}, +) \to (\mathbb{C}^*, \times)$?

Exercice 4.8

Déterminer tous les groupes d'ordre ≤ 5. En déduire qu'un groupe non commutatif possède au moins 6 éléments. Montrer que le groupe symétrique S_3 est non commutatif.

Exercice 4.9

Soit G un groupe tel que l'application $x \to x^{-1}$ soit un morphisme. Montrer que G est commutatif.

Chapitre 5 : Sous-groupes (2CM, 2TD)

Contenu du cours. Définition d'un sous-groupe. Définitions équivalentes. Noyau, image d'un morphisme. Intersections de sous-groupes. Centre, centralisateur. Un morphisme est injectif si et seulement si son noyau est trivial. Sous-groupe engendré par une partie d'un groupe. Sous-groupes de $\mathbb{Z}$. Sous-groupes de $(\mathbb{R}, +)$. Ordre d'un élément. Théorème de Lagrange. Sous-groupe engendré dans le cas commutatif. Sous-groupe dérivé.

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Soient G un groupe et H un sous-groupe de G. Montrer que l'application d'« inclusion » $i : H \to G$ donnée par $i(x) = x$ est un morphisme de groupes.
2. Soit $f : G \to H$ un morphisme de groupes. Si G' est un sous-groupe de G, montrer que son image $f(G')$ est un sous-groupe de H.
3. Soit $f : G \to H$ un morphisme de groupes. Donner la définition du noyau de f et montrer que c'est un sous-groupe de G.
4. Soit G un groupe. Quel est le noyau de l'identité de G ?
5. À quelle condition sur G a-t-on $C(G) = G$?
6. Si G est un groupe *commutatif*, montrer que l'ensemble des éléments d'ordre fini de G est un sous-groupe de G.
7. Soit G un groupe. Quel est le sous-groupe de G engendré par l'ensemble vide ?
8. Donner la définition du sous-groupe dérivé d'un groupe G.

Exercice 5.1

Soit G un groupe d'ordre pair. Montrer qu'il existe un élément $x \in G$, $x \neq e$ tel que $x^2 = e$.

Exercice 5.2

Soit G un groupe et H, K deux sous-groupes de G.

(a) Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

(b) Montrer qu'un groupe ne peut être la réunion de deux sous-groupes propres.

Exercice 5.3

Montrer que dans un groupe G, toute partie non vide finie stable par la loi de composition est un sous-groupe. Donner un contre-exemple à la propriété précédente dans le cas d'une partie infinie.

Exercice 5.4

Soit G un groupe abélien et a et b deux éléments d'ordres finis. Montrer que ab est d'ordre fini et que l'ordre de ab divise le ppcm des ordres de a et b. Montrer que si les ordres de a et b sont premiers entre eux, l'ordre de ab est égal au ppcm des ordres de a et de b.

Exercice 5.5

Soient G un groupe et H et K deux sous-groupes de G. On note $HK := \{hk \mid h \in H, k \in K\}$.

(a) Montrer sur un exemple dans $G = \mathfrak{S}_3$ qu'en général les ensembles HK et KH ne sont pas égaux et ne sont pas des sous-groupes de G.

(b) Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$.

(c) Montrer que si H et K sont finis alors $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Exercice 5.6

Déterminer tous les sous-groupes du groupe symétrique S_3.

Exercice 5.7

Montrer que dans un groupe d'ordre 35, il existe un élément d'ordre 5 et un élément d'ordre 7.

Exercice 5.8

Soit G un groupe multiplicatif (c'est-à-dire dont la loi est notée multiplicativement). Soient a et b deux éléments

de G. Montrer que si ab est d'ordre fini, alors ba l'est également et son ordre est celui de ab.

Exercice 5.9

Montrer qu'un groupe fini dont l'ordre est un nombre premier est cyclique.

Exercice 5.10

Soit G un groupe, H un sous-groupe de G, et $x, y \in G$. On note $xH := \{xh \mid h \in H\}$. Montrer que les assertions suivantes sont équivalentes : (i) $xH = yH$; (ii) $xH \cap yH \neq \emptyset$; (iii) $y^{-1}x \in H$.

Exercice 5.11

Soient H et K des sous-groupes d'un groupe G d'élément neutre e. On considère l'application

$$\begin{array}{rccc} f: & H \times K & \longrightarrow & G \\ & (h,k) & \longmapsto & hk. \end{array}$$

Montrer que f est un isomorphisme de groupes si et seulement si $G = HK$, $H \cap K = \{e\}$, et pour tous $h \in H$ et $k \in K$ on a $hk = kh$.

Exercice 5.12

Quels sont les entiers $n \in \mathbb{Z}$ tels que $\mathbb{Z}$ soit engendré par n ?

Chapitre 6 : Groupe opérant sur un ensemble (2CM, 2TD)

Contenu du cours. Définition d'une action (à gauche, à droite). Action de $\mathfrak{S}(E)$ sur un ensemble E. Exemples (en particulier : actions d'un sous-groupe par translations ou par conjugaison). Stabilisateur, points fixes, actions libres, orbites, actions transitives. Les stabilisateurs des points d'une même orbite sont conjugués les uns des autres. Ensemble quotient (noté $G\backslash E$ pour une action à gauche et E/G pour une action à droite de G sur E, sauf dans le cas d'une action d'un sous-groupe par conjugaison).

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Donner la définition d'une action à gauche d'un groupe G sur un ensemble X.
2. Si G opère à gauche sur X par $(g,x) \mapsto gx$, montrer que l'on obtient une action à droite en posant $x*g = g^{-1}x$.
3. Montrer qu'il revient au même de se donner une action à gauche de G sur X, ou un morphisme de groupes de G dans $\mathfrak{S}(X)$.
4. Rappeler les définitions des mots ou expressions suivants : stabilisateur, action libre, orbite, action fidèle, action transitive.
5. Soit G un groupe agissant à gauche sur un ensemble X et soient $x, y \in X$ deux points dans une même orbite. Montrer que les stabilisateurs G_x et G_y sont conjugués.

Exercice 6.1

(a) Soit G un groupe et H un sous-groupe. Montrer que la formule

$$g.g'H = gg'H$$

définit une action de G sur l'ensemble quotient G/H. Déterminer le fixateur d'une classe gH.

(b) Soit G un groupe et X et Y deux ensembles sur lesquels G agit (on parlera de G-ensembles). Soit f une application de X dans Y. On dira que f est compatible à l'action de G (ou que f est un morphisme de G-ensembles) si pour tout élément x de X et tout g dans G, $f(g.x) = g.f(x)$. Montrer que si f est bijective et compatible à l'action de G il en est de même de f^{-1}. On dira dans ce cas que f est un isomorphisme de G-ensembles.

(c) Soit G un groupe agissant transitivement sur un ensemble X (i.e. pour tout couple d'éléments x et y de X il existe au moins un élément g du groupe tel que $g.x = y$). Montrer qu'il existe un sous-groupe H de G tel que X soit isomorphe en tant que G-ensemble à G/H (on prendra pour H le fixateur d'un point quelconque de X).

(d) i) Soit H et K deux sous-groupes de G. Montrer qu'il existe une application f de G/H vers G/K compatible avec l'action de G si et seulement si H est contenu dans un conjugué de K. Montrer que dans ce cas f est surjective. Montrer que G/H et G/K sont isomorphes en tant que G-ensembles si et seulement si H et K sont conjugués dans G.

ii) Soit X et Y deux G-ensembles transitifs. Montrer qu'il existe une application de X vers Y compatible avec l'action de G si et seulement si il existe deux éléments x et y de X et Y tels que le fixateur de x soit contenu dans un conjugué du fixateur de y. Montrer que X et Y sont isomorphes si et seulement si les fixateurs de x et de y sont conjugués dans G.

Exercice 6.2

Montrer que tout groupe fini G est isomorphe à un sous-groupe de $\mathfrak{S}_n$, où n est l'ordre de G.

Exercice 6.3

Soit φ une action d'un groupe G sur un ensemble X.

1. Montrer que $G_{g(x)} = gG_xg^{-1}$, où $g \in G$ et G_x désigne le stabilisateur du point x.
2. Si l'action φ est transitive et fidèle et G est abélien alors montrer que φ est simplement transitive.

Exercice 6.4

Soit $G =< \gamma_1, \gamma_2 >$ le sous-groupe des transformations du plan complexe $\mathbb{C}$ engendré par $\gamma_1 : z \mapsto z+1$ et $\gamma_2 : z \mapsto z+i$.

1. Montrer que $G \cong \mathbb{Z}^2$ et G agit isométriquement sur $\mathbb{C}$.
2. Trouver un ensemble fondamental F pour cette action et l'ensemble d'orbites $\mathbb{C}/\sim = \mathbb{C}/G = \overline{F}/\sim$ en identifiant les points équivalents sur le bord de $\overline{F}$.

Exercice 6.5

Parmi les applications ψ définies ci-dessous, déterminer celles qui définissent une action à gauche de G sur E, et dans ce cas préciser ses orbites et l'ensemble quotient :

1. $G = n\mathbb{Z}$, $E = \mathbb{Z}$, $\psi : (nk, a) \mapsto a + nk$.
2. $G = p\mathbb{Z} \times q\mathbb{Z}$, $E = \mathbb{Z} \times \mathbb{Z}$, $\psi : ((pk, ql), (a, b)) \mapsto (a + pk, b + ql)$.
3. $G = \mathbb{Z}$, $E = \mathbb{R}$, $\psi : (n, x) \mapsto x+n$ (*utiliser l'homomorphisme* $\exp(2\pi i \cdot) : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ *pour identifier l'ensemble quotient*).
4. $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$, $E = \mathbb{C}$, $\psi : \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, z \right) \mapsto az^2 + b$.
5. $G = GL_n(\mathbb{C})$, $E = M_n(\mathbb{C})$, $\psi : (P, A) \mapsto PA$; montrer que l'orbite de $A \in M_n(\mathbb{C})$ est formée par les matrices de $M_n(\mathbb{C})$ dont le noyau est égal à $\ker(A)$. Même question avec $\psi : (P, A) \mapsto AP$, $\psi : (P, A) \mapsto AP^{-1}$, et $\psi : (P, A) \mapsto PAP^{-1}$.

Exercice 6.6

On dit que deux ensembles E, E' munis chacun d'une action à gauche d'un groupe G sont isomorphes si il existe une bijection $f : E \to E'$ telle que $f(g \cdot x) = g \cdot f(x)$.

Soit E un ensemble muni d'une action à gauche *transitive* d'un groupe G, ie. telle que pour tous x, $y \in E$ il existe $g \in G$ tel que $g \cdot x = y$. Montrer que pour tout $p \in E$, E est isomorphe à $G/\mathrm{Stab}_G(p)$ muni de l'action de G par translation.

Exercice 6.7

1) Montrer que $GL_n(\mathbb{R})$ agit naturellement à gauche sur $\mathbb{R}^n$. Déterminer les orbites. Décrire le stabilisateur du premier vecteur de la base canonique.
2) Mêmes questions pour l'action à gauche de $O_n(\mathbb{R})$ sur $\mathbb{R}^n$.

Chapitre 7 : Groupe symétrique, groupes diédraux (2CM, 2TD)

Contenu du cours. Généralités sur le groupe symétrique. Théorème de Cayley. Orbites, points fixes, support d'une permutation. Cycles. Décomposition d'une permutation en cycles à supports disjoints. Type d'une permutation. Conjugaison des cycles. Deux permutations sont conjuguées si et seulement si elles ont le même type. Ordre d'une permutation. Transpositions. Les transpositions engendrent $\mathfrak{S}_n$. Signature. Groupe diédral d'ordre $2n$ (noté D_n) : définition comme groupe des isométries d'un polygône régulier à n côtés, caractérisations.

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)

1. Décomposer la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 6 & 4 & 3 & 5 & 2 & 9 & 7 & 1 \end{pmatrix}$$

en cycles à supports disjoints.

2. Montrer que le cycle $(1, 2, 3)$ est d'ordre 3.

3. Vrai ou faux ?

a) Dans $\mathfrak{S}_8$, les permutations $(1, 2)(3, 4, 5)$ et $(3, 5, 7)(4, 6)$ sont conjuguées.
b) Les permutations de a) sont d'ordre 5.
c) Les cycles engendrent $\mathfrak{S}_n$.
d) Les transpositions engendrent $\mathfrak{S}_n$.
e) Pour $n \geq 3$, les 3-cycles engendrent $\mathfrak{S}_n$.
f) Pour $n \geq 4$, les 4-cycles engendrent $\mathfrak{S}_n$.

4. Donner au moins deux définitions possibles de la signature. Est-ce un morphisme de groupes ?

5. Pour quelles valeurs de n le groupe diédral D_n est-il commutatif ?

6. Soit $\sigma \in S_n$ et $c = (a_1\ a_2\ \ldots\ a_k)$ un cycle. Quelle est la nature de la permutation $\sigma \circ c \circ \sigma^{-1}$?

Exercice 7.1

(a) Montrer que le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles. En déduire que A_n est engendré par les 3-cycles.

(b) Montrer que $A_n =< (123), (124), \ldots, (12n) >$.

Exercice 7.2

Montrer par récurrence qu'on peut écrire toute permutation $\sigma \in \mathfrak{S}_n$ distincte de l'identité comme produit d'au plus $(n-1)$ transpositions.

Exercice 7.3

Déterminer toutes les classes de conjugaison des permutations dans S_5 (on considérera leur décomposition en cycles). Déterminer tous les sous-groupes distingués de S_5.

Exercice 7.4

On considère l'action à gauche de $\mathfrak{S}_n$ sur lui-même par conjugaison. Déterminer les orbites et l'ensemble quotient.

Exercice 7.5

Dans le groupe symétrique S_4 on considère les sous-ensembles suivants :

$$H = \{\sigma \in S_4 \,|\, \sigma(\{1, 2\}) = \{1, 2\}\}$$

$$K = \{\sigma \in S_4 \,|\, \forall a, b \quad a \equiv b \ [\text{mod } 2] \Rightarrow \sigma(a) \equiv \sigma(b) \ [\text{mod } 2]\}$$

Montrer que H et K sont des sous-groupes de S_4. Les décrire.

Exercice 7.6

Déterminer le groupe des isométries de l'espace affine euclidien de dimension 3 qui laissent invariant un cube.

Exercice 7.7

Soient σ et τ deux transpositions de $\{1, \ldots, n\}$. Montrer que $\sigma \circ \tau$ est d'ordre 1, 2 ou 3.

Exercice 7.8

Soit $\sigma \in S_5$ défini par

$$\sigma = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{matrix}$$

(a) Ecrire la décomposition de σ en produit de cycles de supports disjoints. Quelle est la signature de σ ?

(b) Donner la liste des éléments de $< \sigma >$. Déterminer $< \sigma > \cap A_5$.

Exercice 7.9

Montrer que toute permutation d'ordre 10 dans S_8 est impaire.

Exercice 7.10

Expliciter les 24 rotations de l'espace laissant un cube de sommets $A_1, A_2, \ldots, A_8$ invariant.
Décomposer en cycles les permutations de S_8 correspondantes.
Ecrire les produits "typiques" de 2 quelconques de ces permutations.

Exercice 7.11

Déterminer la décomposition canonique et l'ordre de la permutation :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 10 & 7 & 6 & 2 & 9 & 3 & 4 & 8 \end{pmatrix} \in \mathfrak{S}_{10}.$$

Calculer la signature de σ de deux manières différentes.

Exercice 7.12

Montrer que l'ordre d'une permutation impaire est un nombre pair.

Exercice 7.13

Pour tout $n \in \mathbb{N}^*$, calculer la signature de la permutation $[n\ n-1\ n-2 \ldots\ 3\ 2\ 1] \in S_n$.

Exercice 7.14

Soit E l'ensemble des cycles de longueur n de $\mathfrak{S}_n$, où $n \geq 3$ est impair. On considère l'action par conjugaison de $\mathfrak{S}_n$ sur E.
1) Rappeler le nombre d'éléments de E.
2) Comment une permutation σ agit-elle sur un cycle c ?
3) Combien y a-t-il d'orbites ?
4) Décrire le stabilisateur du cycle $(1, 2, \ldots, n)$.

Chapitre 8 : Classes modulo un sous-groupe, formule des classes (3CM, 3TD)

Contenu du cours. Classes à gauche et à droite modulo un sous-groupe. Représentants d'une classe. Théorème de Lagrange. Indice d'un sous-groupe. Si un groupe G opère à gauche sur un ensemble X, pour tout $x \in X$ on a une bijection naturelle de G/G_x vers l'orbite de x. Formule des classes. Applications à des questions de dénombrement. Application aux p-groupes : le centre d'un p-groupe non trivial est non trivial.

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Énoncer et démontrer le théorème de Lagrange.
2. Si G est un groupe fini et si m est un entier naturel divisant $|G|$, existe-t-il un sous-groupe de G d'ordre m ? (Donner une preuve ou un contre-exemple.)
3. Donner la définition de l'indice d'un sous-groupe.
4. Soit $f : G \to G'$ un morphisme de groupes, et soit $H = \operatorname{Ker} f$. Montrer que, pour tout $x \in G$, $xH = Hx = f^{-1}(f(x))$.
5. Énoncer la formule des classes.
6. Montrer que le centre d'un p-groupe non trivial est non trivial.

Exercice 8.1

Soit G un groupe, H un sous-groupe de G, et G/H l'ensemble des classes à gauche de G modulo H. Rappeler la définition de l'action de G sur G/H par translation à gauche. Déterminer le noyau de l'homomorphisme $G \to Bij(G/H)$ qui définit cette action.

Exercice 8.2

Soit G un groupe, et H_1 et H_2 deux sous-groupes de G d'indices finis dans G. Montrer que $H_1 \cap H_2$ est d'indice fini dans G.

Exercice 8.3

Soient G un groupe et H un sous-groupe d'indice fini dans G. On définit sur G la relation xRy si et seulement si $x \in HyH$.

(a) Montrer que R est une relation d'équivalence et que toute classe d'équivalence pour la relation R est une union finie disjointe de classes à gauche modulo H.

Soit $HxH = \bigcup_{1 \leq i \leq d(x)} x_i H$ la partition de la classe HxH en classes à gauche distinctes.

(b) Soit $h \in H$ et i un entier compris entre 1 et $d(x)$; posons $h * x_i H = h x_i H$. Montrer que cette formule définit une action transitive de H sur l'ensemble des classes $x_1 H, \ldots, x_{d(x)} H$ et que le fixateur de $x_i H$ dans cette action est $H \cap x_i H x_i^{-1}$. En déduire que

$$d(x) = [H : H \cap xHx^{-1}]$$

et qu'en particulier $d(x)$ divise l'ordre de G.

(c) Montrer que H est distingué dans G si et seulement si $d(x) = 1$ pour tout $x \in G$.

(d) On suppose que G est fini et que $[G : H] = p$, où p est le plus petit nombre premier divisant l'ordre de G. Le but de cette question est de montrer que H est distingué dans G.

(i) Montrer que pour tout $x \in G$, $d(x) \leq p$. En déduire que $d(x) = 1$ ou $d(x) = p$.

(ii) Montrer que si H n'est pas distingué dans G, il existe une unique classe d'équivalence pour la relation R et que $G = H$, ce qui contredit l'hypothèse $[G : H] = p$.

Exercice 8.4

Soit G un groupe fini agissant sur un ensemble fini X.

(a) On suppose que toute orbite contient au moins deux éléments, que $|G| = 15$ et que $\operatorname{card}(X) = 17$. Déterminer le nombre d'orbites et le cardinal de chacune.

(b) On suppose que $|G| = 33$ et $\text{card}(X) = 19$. Montrer qu'il existe au moins une orbite réduite à un élément.

Exercice 8.5

Soit K un corps fini à q éléments, $GL(n, K)$ l'ensemble des matrices (n, n) inversibles à coefficients dans K. Montrer par récurrence sur n que $|GL(n, K)| = (q^n - 1)(q^n - q)...(q^n - q^{n-1})$ en considérant l'action de $Aut(K^n)$ sur l'espace vectoriel K^n (de base $\{v_1, ..., v_n\}$), l'orbite et le stabilisateur d'un vecteur de base (v_1 par exemple).

Exercice 8.6

Pour $n = n_1 + \cdots + n_s$ combien y a-t-il de partitions de l'ensemble $\{1, \ldots, n\}$ en s parties de cardinaux $n_1, \ldots, n_s$?

Exercice 8.7

Compter le nombre de sous-espaces vectoriels de dimension 3 dans $(\mathbb{Z}/7\mathbb{Z})^5$.

Exercice 8.8 (Formule de Burnside)

Soient X un ensemble fini et G un groupe fini agissant sur X. Pour tout $g \in G$ on note X^g l'ensemble des points fixes de X sous g, c'est-à-dire

$$X^g = \{x \in X \mid g.x = x\}.$$

Démontrer la « formule de Burnside » :

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

où $G\backslash X$ désigne l'ensemble quotient de X par G. (Cette formule permet donc de calculer le nombre d'orbites en fonction des cardinaux des X^g.)

Exercice 8.9

Combien peut-on faire de colliers différents avec 4 perles bleues, 4 perles blanches et 4 perles rouges ?

Exercice 8.10

De combien de manières différentes peut-on colorier un cube avec les couleurs rouge, blanc et bleu ?

Chapitre 9 : Sous-groupes distingués, groupes quotients (3CM, 4TD)

Contenu du cours. Définition(s) d'un sous-groupe distingué (on dit aussi « invariant » ou « normal »). On note $H \lhd G$. Structure de groupe sur le quotient G/H (où H sous-groupe distingué de G). « Propriété universelle du quotient ». Définition d'un groupe simple. Espace vectoriel quotient. Isomorphisme naturel $G/\mathrm{Ker}\, f \simeq \mathrm{Im}\, f$. Abélianisé d'un groupe. Groupe des automorphismes intérieurs. Description des sous-groupes d'un groupe quotient. « Théorèmes d'isomorphismes ».

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Soit H un sous-groupe de G. Si H est contenu dans le centre de G, est-il distingué ? (Donner une preuve ou un contre-exemple.)
2. Donner la définition d'un sous-groupe distingué.
3. Montrer que le noyau d'un morphisme de groupes est toujours distingué.
4. Énoncer la propriété universelle du quotient.
5. Soit H un sous-groupe distingué d'un groupe G.
a) Quelle classe modulo H est l'élément neutre du groupe G/H ?
b) On prend $G = \mathbb{Z}$ et $H = 8\mathbb{Z}$. Dans la bijection vue en cours entre l'ensemble des sous-groupes de G/H et l'ensemble des sous-groupes de G contenant H, à quels sous-groupes de $\mathbb{Z}$ correspondent les sous-groupes suivants de $\mathbb{Z}/8\mathbb{Z}$: $\{8\mathbb{Z}, 2+8\mathbb{Z}, 4+8\mathbb{Z}, 6+8\mathbb{Z}\}$, $\{8\mathbb{Z}, 4+8\mathbb{Z}\}$, $\mathbb{Z}/8\mathbb{Z}$?

Exercice 9.1 (Sous-groupes distingués : autour des définitions)

1. Donner une condition sur un groupe G qui implique que tout sous-groupe de G est distingué dans G.
2. Soit G un groupe, et H un sous-groupe de G.
   (a) Montrer que si $[G : H] = 2$, alors H est un sous-groupe distingué de G.
   (b) Si $H \lhd G$, et K est un sous-groupe de G contenant H, alors $H \lhd K$.
   (c) On a défini en cours H comme un sous-groupe distingué de G par la condition : pour tout $x \in G$, $xH = Hx$. Montrer que cette condition équivaut à : pour tout $x \in G$, $xH \subset Hx$, ou encore : pour tout $x \in G$, $Hx \subset xH$, ou encore : pour tout $x \in G$, $xHx^{-1} \subset H$.

Exercice 9.2

Montrer qu'un groupe abélien fini d'ordre divisible par p a toujours un élément d'ordre p.

Exercice 9.3

1. Soit G un groupe, H un sous-groupe de G. Montrer que les propriétés suivantes sont équivalentes :
   i) $\forall g \in G : gHg^{-1} \subset H$.
   ii) $\forall g \in G : gHg^{-1} = H$.
   iii) $\forall g \in G : gH = Hg$.
2. En déduire que tout sous-groupe d'indice 2 est distingué.

Exercice 9.4

Soient $T = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) : a, c \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R} \right\}$ et $U = \left\{ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in \mathbb{R} \right\}$.

1. Montrer que T est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.
2. Montrer que U est un sous-groupe distingué de T.

Exercice 9.5
Soit G un groupe et H un sous-groupe. On suppose que le produit de deux classes à gauche modulo H est une classe à gauche modulo H. Montrer que H est distingué dans G.

Exercice 9.6 (Relations d'équivalence compatibles avec la loi de groupe)
Soit G un groupe et $\simeq$ une relation d'équivalence sur G. On suppose que cette relation est compatible avec la loi de groupe, c'est-à-dire que

$$\forall x, y \in G \quad \forall x', y' \in G \quad x \simeq x' \quad \text{et} \quad y \simeq y' \quad \text{alors} \quad xy \simeq x'y'$$

Montrer que la classe H de l'élément neutre 1 est un sous-groupe distingué de G et que

$$\forall x, x' \in G \quad x \simeq x' \quad \text{est} \quad \text{équivalent} \quad \text{à} \quad x'x^{-1} \in H$$

Exercice 9.7
Soit G un groupe et $K \subset H \subset G$ deux sous-groupes. On suppose que H est distingué dans G et que K est caractéristique dans H (i.e. stable par tout automorphisme de H). Montrer qu'alors K est distingué dans G.

Donner un exemple de groupe G et de deux sous-groupes $K \subset H \subset G$, H étant distingué dans G et K étant distingué dans H, mais K n'étant pas distingué dans G.

Exercice 9.8
Soit $f : G \to H$ un morphisme de groupes finis. Soit G' un sous-groupe de G. Montrer que l'ordre de $f(G')$ divise les ordres de G' et de H.

Exercice 9.9
Soit G un groupe et H un sous groupe distingué de G d'indice n. Montrer que pour tout $a \in G$, $a^n \in H$. Donner un exemple de sous-groupe H non distingué de G pour lequel la conclusion précédente est fausse.

Exercice 9.10
Soit G un groupe fini et H un sous-groupe distingué d'ordre n et d'indice m. On suppose que m et n sont premiers entre eux. Montrer que H est l'unique sous-groupe de G d'ordre n.

Exercice 9.11
Montrer que $\mathrm{SL}_n(\mathbb{R})$ est un sous-groupe distingué du groupe $\mathrm{GL}_n(\mathbb{R})$ et que le groupe quotient est isomorphe à $\mathbb{R}^\times$.

Exercice 9.12
On considère les groupes suivants :

$$T = \{z \in \mathbb{C} \,|\, |z| = 1\} \quad \mu_n = \{z \in \mathbb{C} \,|\, z^n = 1\} \quad \mu_\infty = \{z \in \mathbb{C} \,|\, \exists n \quad z^n = 1\}$$

(a) Montrer les isomorphismes suivants :

$$\mathbb{R}/\mathbb{Z} \simeq T \quad \mathbb{C}^\times/\mathbb{R}^\times_{>0} \simeq T \quad \mathbb{C}^\times/\mathbb{R}^\times \simeq T \quad T/\mu_n \simeq T \quad \mathbb{C}^\times/\mu_n \simeq \mathbb{C}^\times$$

(b) Montrer que $\mu_\infty \simeq \mathbb{Q}/\mathbb{Z}$. Quels sont les sous-groupes finis de μ_∞ ?

(c) Montrer qu'un sous-groupe de type fini de $\mathbb{Q}$ contenant $\mathbb{Z}$ est de la forme $\frac{1}{q}\mathbb{Z}$. En déduire la forme des sous-groupes de type fini de $\mathbb{Q}/\mathbb{Z}$ et de μ_∞.

Exercice 9.13
Soit G un sous-groupe d'indice fini du groupe multiplicatif $\mathbb{C}^\times$. Montrer que $G = \mathbb{C}^\times$.

Exercice 9.14
Soit G un groupe et H un sous-groupe contenu dans le centre $Z(G)$ de G. Montrer que H est distingué dans G et que, si le groupe quotient G/H est cyclique, $G = Z(G)$.

Exercice 9.15
Montrer qu'un groupe d'ordre p^2 où p est un nombre premier est abélien.

Exercice 9.16
(a) Soit G un groupe et H un sous-groupe distingué de G. On note φ la surjection canonique $\varphi : G \to G/H$. Montrer que l'ordre d'un élément x de G est un multiple de l'ordre de $\varphi(x)$.

(b) Pour tout $x \in G$ on pose τ_x l'application de G dans G définie par $\tau_x(y) = xyx^{-1}$. Montrer que τ_x est un automorphisme de G et que l'application

$$x \to \tau_x$$

est un morphisme de groupes de G dans $\mathrm{Aut}(G)$. Quel est le noyau de ce morphisme ?

(c) On suppose que G est fini et que H est un sous-groupe distingué dont l'ordre est le plus petit nombre premier p divisant l'ordre de G. Montrer que pour tout $x \in G$ l'ordre de la restriction à H de τ_x est un diviseur de $p-1$ et de l'ordre de G. En déduire que τ_x restreint à H est l'identité pour tout x et donc que H est contenu dans le centre de G.

Exercice 9.17

Déterminer tous les sous-groupes de $\mathbb{Z}/8\mathbb{Z}$.

Exercice 9.18

Montrer que le groupe-quotient $\mathbb{C}/\mathbb{R}$ est isomorphe à $\mathbb{R}$.

Exercice 9.19

Décrire le groupe-quotient $\mathbb{R}^*/\mathbb{R}_+^*$ et montrer qu'il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Exercice 9.20

Montrer que tout quotient d'un groupe monogène est monogène.

Exercice 9.21

Soit G un groupe ; on note $D(G)$ (ou $[G,G]$) le groupe engendré par les éléments de la forme $[g,h] = ghg^{-1}h^{-1}$; $g, h \in G$.

1. Montrer que $D(G)$ est distingué dans G.
2. Montrer que $G/D(G)$ est commutatif. On note ce quotient G_{ab} et on l'appelle *l'abélianisé* de G.
3. Plus généralement montrer qu'un sous-groupe distingué H de G contient $D(G)$ si et seulement si G/H est commutatif. (Autrement dit, $D(G)$ est le plus petit sous-groupe distingué de G tel que le quotient de G par ce sous-groupe soit abélien. Ou encore : G_{ab} est le plus grand quotient abélien de G.)
4. Soit $\pi : G \to G/[G,G]$ la projection canonique. Montrer que si K est un groupe abélien et $\varphi : G \to K$ un homomorphisme de groupes, alors il existe un unique homomorphisme $\bar{\varphi} : G/[G,G] \to K$ tel que $\bar{\varphi} \circ \pi = \phi$.
5. Déduire de la question 4 une bijection entre les homomorphismes de groupes $G \to \mathbb{C}^*$ et les homomorphismes de groupes $G/[G,G] \to \mathbb{C}^*$.
6. *Exemple.* Montrer que $[\mathfrak{S}_n, \mathfrak{S}_n] = \mathcal{A}_n$ (le groupe alterné). En déduire le groupe quotient $(\mathfrak{S}_n)_{ab}$.

Exercice 9.22

Soit G un groupe ; on note, pour tout $g \in G$ φ_g l'application $x \mapsto gxg^{-1}$ de G dans lui-même et $\mathrm{Int}(G) = \{\varphi_g ; g \in G\}$.

1. Montrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.
2. Soit $f : G \to \mathrm{Int}(G)$ l'application $g \mapsto \varphi_g$. Montrer que f est un homomorphisme de groupe. Calculer $\mathrm{Ker}(f)$.
3. En déduire que $G/Z(G)$ est isomorphe à $\mathrm{Int}(G)$.

Exercice 9.23

Soit G un groupe, $C(G)$ son centre, et

$$\begin{array}{rccl} \varphi : & G & \longrightarrow & \mathrm{Aut}(G) \\ & g & \longmapsto & (g' \mapsto gg'g^{-1}) \ . \end{array}$$

1. Vérifier que φ est un morphisme de groupes. On note $\mathrm{Inn}(G)$ l'image de φ.
2. Montrer que φ induit un isomorphisme de groupes $G/C(G) \cong \mathrm{Inn}(G)$.

3. Justifier que le groupe quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ est bien défini.

Exercice 9.24

Soit $\mathbb{K}$ un corps.

1. Montrer que $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$ est un morphisme de groupes.
2. On note $SL_n(\mathbb{K}) = \ker(\det)$. Dire pourquoi $SL_n(\mathbb{K})$ est un sous-groupe distingué de $GL_n(\mathbb{K})$ et montrer que $GL_n(\mathbb{K})/SL_n(\mathbb{K}) \cong \mathbb{K}^*$.
3. Reconnaître $GL_1(\mathbb{K})$ et $SL_1(\mathbb{K})$.
4. Montrer que les matrices diagonales (resp. triangulaires supérieures) de $GL_n(\mathbb{K})$ forment un sous-groupe. Sont-ils distingués ?
5. Montrer que $Z(GL_n(\mathbb{K}))$ est le sous-groupe formé par les homothéties.

Exercice 9.25

1) Montrer que pour tout morphisme de groupes $f : G \to G'$ on a $H \lhd G \Rightarrow f(H) \lhd f(G)$ et $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$.
2) Donner un sous-groupe distingué non trivial de $GL_n(\mathbb{K})$ et $\mathfrak{S}_n$. Préciser leur indice.
3) Donner un exemple dans $\mathfrak{S}_n$, $n > 2$, d'un sous-groupe non distingué.

Exercice 9.26

Soit $f : G \to G'$ un homomorphisme de groupes, et H un sous-groupe de G. Montrer que $f^{-1}(f(H)) = H\mathrm{Ker}(f)$. Justifier de deux manières différentes que $H\mathrm{Ker}(f)$ est un sous-groupe de G.

Exercice 9.27

Soit U le groupe des nombres complexes de module 1, $n \in \mathbb{N}^*$, et U_n le sous-groupe de U formé par les racines n-ièmes de 1. En utilisant le morphisme $z \mapsto z^n$, montrer que U/U_n est isomorphe à U.

Exercice 9.28

Soit H le sous-groupe de $\mathfrak{S}_3$ engendré par le cycle $\sigma = (1, 2, 3)$.

1. Montrer que H est le seul sous-groupe distingué de $\mathfrak{S}_3$ d'ordre 3.
2. Déterminer le groupe quotient $\mathfrak{S}_3/H$.
3. Quels sont les sous-groupes de $\mathfrak{S}_3$ d'ordre 2 ?

Exercice 9.29

Soit H un sous-groupe distingué de S_n contenant une transposition. Montrer que $H = S_n$.

Chapitre 10 : Groupes monogènes, groupes cycliques (1CM, 2TD)

Contenu du cours. Définition et caractérisations des groupes monogènes. Un groupe monogène infini est isomorphe à $\mathbb{Z}$. Un groupe est dit cyclique s'il est monogène et fini. Il est alors isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier $n > 0$. « Propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ », et endomorphismes de $\mathbb{Z}/n\mathbb{Z}$. Lemme chinois et décomposition de $\mathbb{Z}/n\mathbb{Z}$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$. Fonction indicatrice d'Euler (ou « indicateur d'Euler »). Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Donner la définition d'un groupe monogène.
2. En utilisant le lemme chinois, décomposer $\mathbb{Z}/48\mathbb{Z}$ en un produit de p-groupes (pour différents nombres premiers p...).
3. Calculer $\varphi(36)$ et $\varphi(40)$.
4. Calculer $\varphi(20)$. Faire la liste des générateurs de $\mathbb{Z}/20\mathbb{Z}$.
5. Faire la liste des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.
6. Énoncer la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ et en déduire le nombre de morphismes de groupes de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 10.1

Soit G un groupe, e l'élément neutre de G, et $x \in G$ un élément d'ordre fini r.

1. Montrer que pour tout $m \in \mathbb{Z}$ on a $x^m = e$ si, et seulement si, r divise m.
2. Montrer que pour tout $n \in \mathbb{Z}$ l'ordre de l'élément x^n est égal à r/d, où $d = \text{pgcd}(r, n)$. (*On pourra commencer par montrer que l'ordre de* x^n *divise* r/d.)

Exercice 10.2

Soit p premier et $r \in \mathbb{N}^*$. Montrer que les sous-groupes de $\mathbb{Z}/p^r\mathbb{Z}$ sont emboités pour l'inclusion, puis que $\mathbb{Z}/p^r\mathbb{Z}$ a exactement $p^r - p^{r-1}$ éléments générateurs.

Exercice 10.3

Soit n un entier, et $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa factorisation en puissances de nombres premiers distincts. Montrer que l'application

$$\begin{array}{rccc} f : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}) \\ & a \bmod(n) & \longmapsto & (a \bmod(p_1^{\alpha_1}), \dots, a \bmod(p_k^{\alpha_k})) \end{array}$$

est un isomorphisme de groupes. En déduire la formule $\varphi(n) = n \prod_{i=1}^{k}(1 - 1/p_i)$. (NB : donc si $m \wedge n = 1$, alors $\varphi(m)\varphi(n) = \varphi(mn)$.)

Exercice 10.4

Déterminer tous les morphismes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ dans le groupe $(\mathbb{C}^*, \times)$.

Exercice 10.5

(Une caractérisation des groupes cycliques.) On a vu en cours que les sous-groupes d'un groupe cyclique sont en bijection avec les diviseurs positifs de son ordre. Soit G un groupe fini d'ordre n, tel que pour tout diviseur positif d de n il existe *au plus* un sous-groupe H_d de G d'ordre d. On va montrer que G est cyclique.

1. Pour tout diviseur positif d de n on pose $G_d = \{g \in G \mid ordre(g) = d\}$. Montrer que les ensembles G_d non vides forment une partition de G, et que si G_d est non vide, alors tout élément de G_d engendre H_d. Dans ce cas, quel est le cardinal de G_d ?
2. Soit $\varphi : \mathbb{N}^* \to \mathbb{N}$ la fonction d'Euler, et $n \in \mathbb{N}^*$. Vérifier l'identité $\sum_{d|n} \varphi(d) = \sum_{(n/d)|n} \varphi(n/d)$. En utilisant la définition de φ, en déduire la *formule d'Euler* : $\sum_{d|n} \varphi(d) = n$. Conclure.

Exercice 10.6

Montrer qu'un groupe G dont les seuls sous-groupes sont G et $\{e_G\}$ est cyclique et que son ordre est premier.

Exercice 10.7

Montrer que tout entier $n > 0$ divise toujours $\varphi(2^n - 1)$ (où φ est la fonction indicatrice d'Euler).

Exercice 10.8

Etant donnés deux entiers $m, n > 0$, déterminer tous les morphismes de groupe de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, puis tous les automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 10.9

Soit p un nombre premier. Montrer qu'un groupe abélien fini, dont tous les éléments différents de l'élément neutre sont d'ordre p, est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.

Chapitre 11 : Théorèmes de Sylow. Groupes simples. (2CM, 3TD)

Contenu du cours. Pour un nombre premier p et un groupe fini G, définition des p-sous-groupes de G et des p-sous-groupes de Sylow de G (en abrégé, on dira p-Sylow de G). Énoncé et preuve des théorèmes de Sylow : le nombre des p-Sylow de G est congru à 1 modulo p, et divise m (où $|G| = mp^r$ avec m premier à p). Deux p-Sylow quelconques de G sont conjugués. (En cours, version plus générale concernant tous les p-sous groupes de G.) Définition des groupes simples. Utilisation des théorèmes de Sylow pour montrer que certains groupes ne sont pas simples. Simplicité de A_5. Éventuellement (suivant le temps disponible), simplicité de $SO_3(\mathbb{R})$ ou de $PSL_n(K)$.

Exemples de questions de cours (à faire après avoir lu, compris, relu puis rangé ses notes de cours, et avant les séances de TD)
1. Énoncer les théorèmes de Sylow.
2. Donner la définition d'un p-Sylow.
3. Si G est un groupe d'ordre 50, combien peut-il avoir de p-Sylow pour $p = 2, 3, 5, 7, 11$?
4. Soit G un groupe fini d'ordre mp^r avec p premier et $1 < m < p$. Montrer que G admet un sous-groupe distingué d'ordre p^r.
5. Donner la définition d'un groupe simple.
6. Pour quelles valeurs de n le groupe alterné A_n est-il simple ? (sans preuve)
7. Un groupe d'ordre 68 peut-il être simple ?

Exercice 11.1

Soient G un groupe fini et H un sous-groupe distingué de G. Montrer que si H et G/H sont des p-groupes, il en est de même de G.

Exercice 11.2

Soit G un p-groupe et H un sous-groupe distingué de G. Montrer que $H \cap Z(G)$ n'est pas réduit à l'élément neutre.

Exercice 11.3

Soit G un p-groupe d'ordre p^r.

(a) Montrer que pour tout entier $k \leq r$, G possède un sous-groupe distingué d'ordre p^k.

(b) Montrer qu'il existe une suite $G_0 = \{1\} \subset G_1 \subset \ldots \subset G_r = G$ de sous-groupes G_i distingués d'ordre p^i $(i = 1, \ldots, r)$.

(c) Montrer que pour tout sous-groupe H de G d'ordre p^s avec $s < r$, il existe un sous-groupe d'ordre p^{s+1} de G qui contient H.

Exercice 11.4

Soit G un groupe d'ordre $2p$, où p est un nombre premier supérieur ou égal à 3. Montrer que G contient un unique sous-groupe H d'ordre p et que ce sous-groupe est distingué. Vérifier que les seuls automorphismes d'ordre 2 d'un groupe cyclique d'ordre p sont l'identité et le passage à l'inverse. En déduire que le groupe G est soit cyclique, soit non commutatif, auquel cas il possède deux générateurs s et t vérifiant les relations $s^p = 1$, $t^2 = 1$ et $tst^{-1} = s^{-1}$.

Exercice 11.5

Soient G un groupe et H un sous-groupe distingué de G. On se donne un nombre premier p et l'on suppose que H admet un unique p-Sylow S. Montrer que S est distingué dans G.

Exercice 11.6

Soient G un groupe et H un sous-groupe distingué de G. On se donne un nombre premier p et un p-Sylow P

de G. Montrer que $H \cap P$ est un p-Sylow de H et que HP/H est un p-Sylow de G/H.

Exercice 11.7

Montrer qu'un groupe d'ordre 200 n'est pas simple.

Exercice 11.8

Pour p un nombre premier, déterminer le nombre de p-sous-groupes de Sylow du groupe symétrique $\mathfrak{S}_p$.

Exercice 11.9

(a) Donner l'ensemble $\mathcal{D}$ des ordres possibles des éléments du groupe alterné A_5 et pour chaque $d \in \mathcal{D}$, indiquer le nombre d'éléments de A_5 d'ordre d.

(b) Montrer que, pour $d = 2$ et $d = 3$, les éléments d'ordre d sont conjugués, et que les sous-groupes d'ordre 5 sont conjugués.

(c) Déduire une preuve de la simplicité de A_5.

Exercice 11.10

Déterminer les sous-groupes de Sylow du groupe alterné A_5.

Exercice 11.11

Soit G un groupe simple d'ordre 60.

(a) Montrer que G admet 6 5-Sylow, et que l'action de conjugaison sur ses 5-Sylow définit un morphisme injectif $\alpha : G \to S_6$, une fois une numérotation des 5-Sylow de G choisie. Montrer que l'image $\alpha(G) = H$ est contenue dans A_6.

(b) On considère l'action de A_6 par translation à gauche sur l'ensemble $A_6/.H$ des classes à gauche. Montrer qu'elle définit un isomorphisme $\varphi : A_6 \to A_6$, une fois une numérotation des éléments de $A_6/.H$ choisie.

(c) Montrer que $\varphi(H)$ est le fixateur de la classe de l'élément neutre H, et en conclure que $G \simeq A_5$.

Exercice 11.12

Soient p et q deux nombres premiers et G un groupe d'ordre p^2q. On suppose que $p^2 - 1$ n'est pas divisible par q et que $q - 1$ n'est pas divisible par p. Montrer que G est abélien.

Exercice 11.13

Soient p et q deux nombres premiers. Montrer qu'il n'existe pas de groupe simple d'ordre p^2q.

Exercice 11.14

Soit G un groupe d'ordre 15. On va montrer que G est cyclique, donc que $G \cong \mathbb{Z}/15\mathbb{Z}$.

1. Montrer qu'il existe un unique sous-groupe H_3 de G d'ordre 3 et un unique sous-groupe H_5 de G d'ordre 5.
2. Montrer que l'ensemble H_3H_5 est un sous-groupe de G.
3. Montrer que H_3H_5 est cyclique. Conclure.

Exercice 11.15

Soit G un groupe d'ordre 255. On va montrer que G est cyclique.

1. Montrer que G admet un seul sous-groupe d'ordre 17. On note L ce sous-groupe.
2. Montrer que G admet un sous-groupe K d'ordre 3, et un sous-groupe H d'ordre 5. Montrer que l'un au moins des deux groupes K et H est distingué dans G. En déduire que HK, HL et KL sont des sous-groupes cycliques de G. (*On pourra calculer leur ordre et raisonner comme dans l'exercice 11.14.*)
3. Montrer que HKL est un sous-groupe de G. Donner son ordre. Montrer qu'il est abélien. Conclure.

Exercice 11.16

Soit G un groupe non commutatif d'ordre 8.

(a) Montrer que G contient un élément a d'ordre 4 et que le sous-groupe H de G engendré par a est distingué dans G.

(b) On suppose ici qu'il existe un élément b de $G \setminus H$ qui est d'ordre 2. Soit K le sous-groupe engendré par b. Montrer que dans ce cas G est isomorphe au produit semi-direct de H par K, le générateur b de K agissant sur H via l'automorphisme $x \to x^{-1}$. Le groupe est alors isomorphe au groupe diédral D_4.

(c) Dans le cas contraire, soit b un élément d'ordre 4 de G n'appartenant pas à H. Montrer que a^2 est le seul élément d'ordre 2 de G, que le centre $Z(G)$ de G est égal à $\{1, a^2\}$. On pose $-1 = a^2$. Montrer que a et b vérifient les relations suivantes : $a^2 = b^2 = -1$, $bab^{-1} = a^{-1}$. Enfin on pose $ab = c$. Vérifier les relations suivantes :

$$a^2 = b^2 = c^2 = -1 \quad ab = -ba = c \quad bc = -cb = a \quad ca = -ac = b$$

(l'écriture $-x$ signifiant ici $(-1)x$). Ce dernier groupe est le groupe des quaternions.

Exercice 11.17

Soient $p < q$ deux nombres premiers distincts et G un groupe d'ordre pq. Montrer que G admet un unique q-Sylow Q qui est distingué et que $G = QP$, où P est un p-Sylow de G. Montrer que G est isomorphe au produit semi-direct d'un groupe cyclique d'ordre q par un groupe cyclique d'ordre p. Montrer que si $q - 1$ n'est pas divisible par p, ce produit semi-direct est en fait un produit direct.

Exercice 11.18

Déterminer tous les groupes d'ordre au plus égal à 10 à isomorphisme près.

Indications de solutions

[I 1.1] Regarder les valeurs propres, et les dimensions des espaces propres.

[I 1.2] Montrer d'abord que A est diagonalisable.

[I 1.5] On pourra chercher une autre valeur propre « évidente » (penser par exemple à sommer toutes les colonnes).

[I 2.4] Utiliser l'exercice 1.3.

[I 2.5] Utiliser la formule du binôme de Newton.

[I 3.5] Le polynôme caractéristique doit être égal à $(X-2)^2(X-3)$.

[I 4.1] Les premières questions ne présentent aucune difficulté. Pour la dernière, le plus difficile (et le plus intéressant) est de deviner la formule. Pour cela, calculer la puissance n-ième pour $n = 1, 2, 3, 4, 5 \ldots$.

[I 4.2] On pourra montrer les points suivants :
(a) $x \star y = e \Rightarrow y \star x = e$
(b) L'élément neutre à gauche est unique.
(c) L'élément neutre à gauche est un élément neutre à droite aussi.
(d) Tout élément est inversible.

[I 4.3] Pour l'existence d'un inverse pour toute matrice $n \times n$ de déterminant non nul, noter que $\det(A) \neq 0$ entraîne que la matrice A est inversible (comme matrice) et que la matrice A^{-1}, qui est de déterminant $1/\det(A) \neq 0$ est alors l'inverse de A pour le groupe en question.

[I 4.4] Aucune difficulté.

[I 4.8] Standard.

[I 4.9] $(xy)^{-1} = x^{-1}y^{-1} \Rightarrow xy = yx$.

[I 5.1] Considérer la partition de G en sous-ensembles du type $\{x, x^{-1}\}$.

[I 5.7] Commencer par analyser l'ordre possible des éléments de G.

[I 7.3] **Rappel :** De façon générale, on dit qu'une permutation $\omega \in S_n$ est de type 1^{r_1}-2^{r_2}-$\cdots$-d^{r_d} où $d, r_1, \ldots, r_d$ sont des entiers ≥ 0 tels que $r_1 + \cdots + r_d = n$, si dans la décomposition de ω en cycles à support disjoints, figurent r_1 1-cycles (ou points fixes), r_2 2-cycles, ... et r_d d-cycles. En utilisant la question (c), il n'est pas difficile de montrer que deux permutations sont conjuguées dans S_n si et seulement si elles sont de même type. Les classes de conjugaison de S_n correspondent donc exactement à tous les types possibles.

On obtient ainsi facilement les classes de conjugaison de S_5. Soit maintenant H un sous-groupe distingué non trivial de S_5. Dès que H contient un élément de S_5, il contient sa classe de conjugaison ; H est donc une réunion de classes de conjugaison. En considérant toutes les classes possibles que peut contenir H, on montre que $H = A_5$ ou $H = S_5$. Par exemple, si H contient la classe 1-2-2, alors H contient $(1\,2)\,(3\,4) \times (1\,3)\,(2\,5) = (1\,4\,3\,2\,5)$ et donc la classe des 5-cycles. D'après l'exercice 7.1, H contient alors A_5. Le groupe H est donc A_5 ou S_5. Les autres cas sont similaires.

[I 7.4] On montrera que l'ensemble quotient est en bijection avec l'ensemble des partitions de n, ie. l'ensemble des suites décroissantes d'entiers positifs non nuls $\lambda_1, \ldots, \lambda_k$ tels que $\lambda_1 + \ldots + \lambda_k = n$.)

[I 7.8] Aucune difficulté.

[I 7.12] Une puissance impaire d'une permutation impaire ne peut pas être égale à 1.

[I 8.6] Le groupe $\mathfrak{S}_n$ agit transitivement sur l'ensemble de ces partitions.

[I 8.7] Faire agir $GL_n(\mathbb{F}_7)$ sur l'ensemble des sous-espaces en question. L'action est transitive donc le nombre de sous-espaces est $\operatorname{Card} GL_n$ divisé par le cardinal des stabilisateurs. Le stabilisateur d'un sev est isomorphe au groupe des matrices triangulaires supérieures par blocs, on montrera qu'il est de cardinal $|GL_3|.|GL_2|.q^6$. On trouve finalement $\frac{(q^5-1)(q^4-1)}{(q^2-1)(q-1)}$. Remarque : plus simplement, on peut aussi regarder l'application (surjective) de l'ensemble des familles libres à trois éléments vers l'ensemble des sev en question qui à une famille associe l'espace engendré. Les fibres sont toutes de même cardinal, égal à $|GL_3|$.

[I 8.8] On pourra calculer de deux manières différentes le cardinal de l'ensemble $S = \{(g, x) \in G \times X \mid g.x = x\}$.

[I 8.9] La difficulté tient au fait que l'on peut tourner (rotations), ou retourner les colliers. Pour attaquer le problème, on introduit l'ensemble X des « colliers numérotés ». C'est-à-dire que l'on fixe 12 emplacements sur le collier, que l'on numérote, et l'on compte d'abord le nombre de manières de répartir les perles sur ces 12 emplacements. Il y en a $\binom{12}{4}.\binom{8}{4} = 495 \times 70 = 34650$. Maintenant, deux tels colliers numérotés doivent être considérés comme identiques si l'on peut passer de l'un à l'autre par une rotation ou une symétrie (en oubliant les numéros). On fait donc agir le groupe diédral D_{12} sur l'ensemble X des 34650 colliers numérotés, et le nombre cherché est simplement le nombre d'orbites pour cette action (puisque deux colliers numérotés sont en fait identiques si et seulement s'ils sont dans la même orbite). On utilise la formule de Burnside vue à l'exercice 8.8 pour calculer ce nombre d'orbites.

[I 8.10] On procèdera comme dans l'exercice 8.9, en utilisant la description du groupe des isométries du cube vue en 7.6.

[I 9.2] Pour chaque $x \in G$, notons A_x le sous-groupe de G engendré par x. Son ordre est l'ordre $o(x)$ de x. Définir un morphisme surjectif du produit B des A_x vers G. Ceci montre que G est isomorphe à un quotient de B. En particulier son ordre divise celui de B, donc p divise le cardinal de B et il y a au moins un élément dont l'ordre est multiple de p. On en déduit facilement le résultat.

[I 9.8] $f(G')$ est un sous-groupe de H isomorphe à $G'/(\ker(f) \cap G')$.

[I 9.11] Le morphisme « déterminant » de $\mathrm{GL}_n(\mathbb{R})$ dans $\mathbb{R}^\times$ est surjectif et de noyau $\mathrm{SL}_n(\mathbb{R})$.

[I 9.14] Si ζ est un élément de G dont la classe modulo H engendre G/H, alors tout élément de G peut s'écrire $h\zeta^m$ avec $h \in H$ et $m \in \mathbb{Z}$.

[I 9.15] On pourra utiliser le fait que le centre d'un p-groupe est non trivial, et l'exercice 9.14 avec $H = Z(G)$.

[I 9.16] Les questions (a) et (b) ne présentent aucune difficulté. Pour la question (c), noter que, pour tout $x \in G$, on a $(\tau_x)^{|G|} = 1$, et que la restriction de τ_x à H appartient à $\mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ (et déterminer le groupe d'automorphismes de $\mathbb{Z}/p\mathbb{Z}$).

[I 9.21] Aucune difficulté. Observer que tout conjugué d'un commutateur est un commutateur et qu'un quotient G/H est abélien si et seulement si pour tous $u, v \in G$, on a $uvu^{-1}v^{-1} \in H$.

[I 10.7] Trouver l'ordre de 2 modulo $2^n - 1$.

[I 10.8] L'ensemble $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ des morphismes de groupe de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien pour l'addition naturelle des morphismes. On note δ le pgcd de m et n et m' et n' les entiers m/δ et n/δ. Si $p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ désigne la surjection canonique, la correspondance associant à tout $f \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ l'élément $f \circ p(1)$ induit un isomorphisme de groupe entre $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ et le sous-groupe $n'\mathbb{Z}/n\mathbb{Z}$ du groupe additif $\mathbb{Z}/n\mathbb{Z}$, lequel est isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$.

L'ensemble $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la composition. La correspondance précédente induit un isomorphisme entre $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

[I 11.1] $|G| = |G/H|\,|H|$.

[I 11.3] Pour les trois énoncés (a), (b) et (c), raisonner par récurrence sur r en utilisant le fait que le centre d'un p-groupe n'est pas trivial.

[I 11.5] Pour tout $g \in G$, gSg^{-1} est un p-Sylow de $gHg^{-1} = H$ et donc $gSg^{-1} = S$.

[I 11.9] Pour le (c), pour $H \neq \{1\}$ sous-groupe distingué de A_5, raisonner sur les éléments d'ordre 2, 3 et 5 contenus dans H.

[I 11.10] L'identification de chacun des p-Sylow ne pose pas de difficulté. Observer ensuite que les sous-groupes de Sylow sont deux à deux d'intersection réduite à $\{1\}$ et determiner leur nombre en comptant les éléments d'ordre 2, 3 et 5.

[I 11.13] Soit G un groupe d'ordre p^2q qu'on suppose simple. On distinguera deux cas : $p > q$ et $p < q$. Dans le premier, montrer que G admet q p-Sylow d'ordre p^2 et que l'action par conjugaison de G sur les p-Sylow définit un morphisme injectif $G \hookrightarrow S_q$ et aboutir à une contradiction. Dans le second, raisonner sur le nombre de q-Sylow pour aboutir à une contradiction (on sera notamment amené à éliminer le cas $p = 2$ et $q = 3$).

[I 11.17] Les théorèmes de Sylow montrent qu'il n'y a qu'un seul q-Sylow, nécessairement distingué. La suite est standard. Pour le dernier point, utiliser que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ (exercice 10.8) et donc que $\mathbb{Z}/p\mathbb{Z}$ ne peut agir non trivialement sur $\mathbb{Z}/q\mathbb{Z}$ que si p divise $q - 1$.