Université Aix-Marseille 2019–2020

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

TD1 : GÉNÉRALITÉS SUR LES GROUPES

Notation. On rappelle que, pour tout groupe G, $|G|$ désigne son cardinal et $Z(G)$ son centre, c'est-à-dire l'ensemble des éléments qui commutent avec tous les autres éléments ; que pour tout $g \in G$, $|g|$ désigne l'ordre de g ; et que, pour tout $X \subset G$, $\langle X \rangle$ est le plus petit sous-groupe de G contenant X.

Exercice 1. Soit G un groupe fini de cardinal. On suppose que, tout g élément de G, satisfait l'égalité $g^2 = e$.

1. Montrer que G est un groupe abélien.
2. On suppose que G est engendré par $A = \{a_1, \ldots, a_p\} \subset G$, montrer que :
$$\forall g \in G, \quad \exists (\epsilon_1, \ldots, \epsilon_p) \in (\mathbb{Z}/2\mathbb{Z})^p \text{ tels que, } g = a_1^{\epsilon_1} \ldots a_p^{\epsilon_p}.$$
3. On suppose, dans cette question, que A est une partie génératrice de cardinal minimum p. Montrer que l'écriture :
$$g = a_1^{\epsilon_1} \ldots a_p^{\epsilon_p}$$
est unique.
4. Montrer qu'il existe une famille génératrice de cardinal fini minimal. On supposera dans la suite que A est une telle famille.
5. Soit Φ l'application définie par :
$$\begin{array}{rccc} \Phi : & G & \to & (\mathbb{Z}/2\mathbb{Z})^p \\ & x & \mapsto & (\epsilon_1, \ldots, \epsilon_p). \end{array}$$
Montrer que Φ est bien définie et que c'est un isomorphisme de groupes. En déduire que le cardinal de G est 2^p.

Exercice 2. Soit G un groupe fini de cardinal n et m un entier premier avec n. Montrer que, pour tout g élément de G, il existe un unique h élément de G tel que $h^m = g$.

Exercice 3. Soit G un groupe abélien fini, a et b deux éléments de G. Le but de l'exercice est de voir quelles sont les valeurs que $|a.b|$ peut prendre en fonction de $|a|$ et $|b|$.

1. Soit p entier non nul tel que $(ab)^p = e$, soit m le ppcm de p et $|a|$, n le ppcm de p et $|b|$. Montrer que $|a|$ divise n et que $|b|$ divise m.
2. En déduire que lorsque $|a|$ et $|b|$ sont premiers entre eux, alors $|a.b| = |a|.|b|$.
3. Montrer que le résultat précédent est faux sans cette hypothèse.
4. Notons d le pgcd de $|a|$ et $|b|$ et M le ppcm de $|a|$ et $|b|$. En utilisant la première question, montrer que : $\frac{M}{d}$ divise $|a.b|$ et que $|a.b|$ divise M.
5. En choisissant des éléments convenables dans le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, vérifier que l'on peut avoir :
$$\frac{M}{d} < |a.b| < M.$$
6. Montrer qu'il existe toujours dans G un élément d'ordre M.
7. Si G est non abélien, donner un exemple avec a et b d'ordres 2 et $a.b$ d'ordre infini.

Exercice 4. Soit G groupe abélien d'ordre pq avec p, q deux nombres premiers distincts.

1. Soit $g \in G$ d'ordre p.
   (a) Montrer que $G/\langle g \rangle$ est un groupe cyclique.

(b) Soit $\widetilde{h} \in {}^{G}/_{\langle g \rangle}$ un élément non trivial et h un relevé de $\widetilde{h}$ dans G. Déterminer le cardinal de gh.

2. Montrer que G est cyclique.

Exercice 5. On dit qu'un groupe G est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$. On dit de plus qu'il est *cyclique* s'il est aussi de cardinal fini ; on appelle alors *ordre* de G le cardinal de G.

1. Soit G un groupe monogène et $H \subset G$ un sous-groupe.
   (a) Montrer que, si G est non-cyclique, alors H est soit trivial, soit monogène non-cyclique.
   (b) Montrer que, si G est cyclique, alors H est cyclique et l'ordre de H divise l'ordre de G.
2. Soit G un groupe monogène engendré par $g \in G$.
   (a) Montrer que, si G est non-cyclique, alors les seuls générateurs de G sont g et g^{-1}.
   (b) Montrer que, si G est cyclique d'ordre $n \in \mathbb{N}^*$, alors les seuls générateurs de G sont les g^k, avec $k \in [\![1, n-1]\!]$ premier avec n.
3. Soit G un groupe d'ordre p premier.
   (a) Montrer que G est cyclique.
   (b) Montrer que tout élément non nul de G est générateur.

Exercice 6. Montrer que tout sous-groupe d'indice 2 est distingué.

Exercice 7. Soit p un nombre premier, on pose

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

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

Exercice 8. Faire la liste, à isomorphisme près, des groupes de cardinal inférieur ou égal à 7.

Exercice 9. Soit n un entier naturel supérieur ou égal à 2, montrer que le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (noté $Aut(\mathbb{Z}/n\mathbb{Z})$) est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

Exercice 10. Montrer qu'un sous-groupe $H \subset G$ d'un groupe G est distingué ssi il existe un groupe G' et un morphisme de groupes $f : G \longrightarrow G'$ tel que $H = \mathrm{Ker}(f)$.

Exercice 11. Montrer que la relation $\lhd$ définie sur les groupes n'est ni une relation d'équivalence, ni une relation d'ordre.

Exercice 12. Soit G_1 et G_2 deux groupes.

1. Montrer que $G_1 \times G_2 \cong G_2 \times G_1$.
2. Montrer que $G_1 \lhd G_1 \times G_2$ et que ${}^{(G_1 \times G_2)}/_{G_1} \cong G_2$.
3. (a) A-t-on $G_1 \lhd G_1 \rtimes_\varphi G_2$ et ${}^{(G_1 \rtimes_\varphi G_2)}/_{G_1} \cong G_2$ pour tout morphisme $\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1)$?
   (b) A-t-on $G_2 \lhd G_1 \rtimes_\varphi G_2$ et ${}^{(G_1 \rtimes_\varphi G_2)}/_{G_2} \cong G_1$ pour tout morphisme $\varphi : G_2 \longrightarrow \mathrm{Aut}(G_1)$?

Exercice 13. Soit G un groupe. On appelle *commutateur* de G tout élément de la forme $[x,y] := x^{-1}.y^{-1}.x.y$ avec $x, y \in G$, et on note $D(G) \subset G$ le sous-groupe, appelé *dérivé*, engendré par ces commutateurs.

1. Montrer que $D(G) = \{e\}$ ssi G est abélien.
2. Montrer que $D(G) \lhd G$.
3. Montrer que ${}^{G}/_{D(G)}$ est abélien.

4. Montrer que, pour tout $H \lhd G$, ${}^{G}/_{H}$ est abélien ssi $D(G) \subset H$.

Exercice 14. Soit G un groupe. On dit que deux éléments $g_1, g_2 \in G$ sont *conjugués* s'il existe $h \in G$ tel que $g_1 = h^{-1}.g_2.h$.

1. Montrer que la relation définie par $(g_1 \sim g_2) \Leftrightarrow (g_1, g_2$ conjugués) est une relation d'équivalence.

On appelle *classes de conjugaisons* les classes de la relation $\sim$ et on note $\mathcal{C}$ l'ensemble des classes d'équivalence.

Soit a une action de G sur un ensemble X.

2. Montrer que si $g_1, g_2 \in G$ sont conjugués, alors il existe une bijection entre les points fixes de g_1 pour a et ceux de g_2 pour a.

Pour toute classe de conjugaison $c \in \mathcal{C}$, on note n_c son cardinal, et k_c le cardinal commun des ensembles des points fixes pour a de ses éléments. On note aussi N l'ordre de G et K le nombre d'orbite de a.

3. Montrer que $KN = \sum_{c \in \mathcal{C}} k_c n_c$.

Exercice 15. Montrer qu'action transitive et fidèle par un groupe abélien est simplement transitive.

Exercice 16. Soit G un groupe.

1. Montrer que, pour tout $g \in G$, l'application $\mathrm{conj}_g : \begin{array}{ccc} G & \longrightarrow & G \\ g' & \longmapsto & g^{-1}.g'.g \end{array}$ est un automorphisme de groupe.

On note $\mathrm{Int}(G) := \left\{\mathrm{conj}_g \mid g \in G\right\}$ et on appelle *automorphismes intérieurs* ses éléments.

2. Montrer que $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.
3. Montrer que $\mathrm{Int}(G) \cong {}^{G}/_{Z(G)}$.

Exercice 17. Soit $p \in \mathbb{N}^*$ un nombre premier et G un groupe fini tel que p divise $|G|$. On note $\Omega := \left\{(g_1, \ldots, g_p) \in G^p \mid g_1.\cdots.g_p = e\right\}$.

1. Montrer que ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ agit sur Ω par permutation circulaire des termes des p–uplets.
2. Montrer que les orbites pour cette action sont de cardinal 1 ou p.
3. Déterminer le cardinal de l'orbite de $(e, \ldots, e)$.
4. (théorème de Cauchy) En déduire qu'il existe au moins $p-1$ éléments de G d'ordre p.

Exercice 18. Soit $p \in \mathbb{N}^*$ un nombre premier. On dit qu'un groupe est un *p–groupe* si son cardinal est une puissance de p. On dit qu'un sous-groupe $H \subset G$ est un *p–Sylow* de G si c'est un p–groupe de cardinal maximal, càd tel que $p \nmid \frac{|G|}{|H|}$. Dans ce qui suit, on notera $\mathbb{F}_p$ le corps ${}^{Z}/_{p\mathbb{Z}}$ muni des addition et multiplication usuelles.

1. (a) Montrer que le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$ est $p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n}(p^k - 1)$.
   (b) Montrer que les matrices triangulaires supérieures ayant des 1 sur la diagonale forment un p–Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.
2. Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$, $H \subset G$ un sous-groupe et $S \subset G$ un p–Sylow de G. On considère l'action par translation à gauche de H sur l'ensemble des classes à gauche de S.
   (a) Montrer que, pour toute classe à gauche $g.S$, $\mathrm{Stab}(g.S) = g.S.g^{-1} \cap H$.
   (b) Montrer que, pour tout $g \in G$, $\mathrm{Stab}(g.S)$ est p–groupe dont la cardinal divise celui de H.
   (c) Soit $g \in G$, montrer que, si $\mathrm{Stab}(g.S)$ n'est pas un p–Sylow de H, alors p divise $|\mathcal{O}(g.S)|$.
   (d) Montrer qu'il existe $g \in G$ tel que $g.S.g^{-1} \cap H$ est un p–Sylow de H.
3. (a) Montrer que, pour tout n, il existe un monomorphisme de groupe enyoyant $\mathfrak{S}_n$ dans $\mathrm{GL}_n(\mathbb{F}_p)$.
   (b) Montrer que, pour tout groupe G de cardinal $n \in \mathbb{N}^*$, il existe un monomorphisme de groupe envoyant G dans $\mathrm{GL}_n(\mathbb{F}_p)$.
   (c) (premier théorème de Sylow) Montrer que tout groupe fini possède au moins un p–Sylow.
4. (a) Montrer que si S_1 et S_2 sont deux p–Sylow d'un groupe fini G, alors il existe $g \in G$ tel que $g.S_1.g^{-1} \cap S_2$ soit un p–Sylow de S_2.
   (b) (deuxième théorème de Sylow) Montrer que tous les p–Sylow d'un groupe fini sont conjugués.

(c) Montrer qu'un p–Sylow d'un groupe fini G est distingué ssi il est l'unique p–Sylow de G.
(d) Montrer qu'un groupe fini G agit par conjugaison sur l'ensemble de ses p–Sylow et que cette action ne possède qu'une seule orbite.
(e) (troisième théorème de Sylow, partie un) Montrer que le nombre de p–Sylow d'un groupe fini G divise $|G|$.

5. (a) Soit G un p–groupe agissant sur un ensemble X. Montrer que $|X| \cong |\mathrm{Fix}(G)|$ $[p]$.
   (b) Soit S un p–Sylow d'un groupe fini G. On considère l'action par conjugaison de S sur l'ensemble des p–Sylow de G et on fixe $S' \in \mathrm{Fix}(S)$.
      i. Montrer que $S' \lhd \langle S \cup S' \rangle$.
      ii. Montrer que S et S' sont des p–Sylow de $\langle S \cup S' \rangle$ et en déduire que $S' = S$.
   (c) (troisième théorème de Sylow, partie deux) Montrer que le nombre de p–Sylow d'un groupe fini G est congru à 1 modulo p.
6. Soit G un groupe de cardinal p^2q avec p et q deux nombres premiers distincts.
   (a) Montrer que G n'est pas simple.
   (b) Montrer que, si $q \nmid p^2 - 1$ et $p \nmid q - 1$, alors G est abélien.

Exercice 19. Montrer que le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ agit sur $\mathbb{Z}/8\mathbb{Z}$. Décrire les orbites et calculer leurs cardinaux en utilisant la formule des classes.

Exercice 20. Soit G un groupe fini à 21 éléments opérant sur un ensemble à 11 éléments. Montrer qu'il existe au moins un point fixe sous l'action de G.

Exercice 21. On cherche le nombre de colliers de 67 perles formés de 2 rouges, 7 bleues et 2 noires et 56 vertes.

1. Montrer que l'on peut considérer les colliers comme des sommets colorés d'un polygone régulier à 67 côtés et que sur cet ensemble agit le groupe dihédral D_{67}.
2. Montrer que le nombre de colliers n est égal au nombre d'orbites dans l'action du groupe.
3. Calculer $|Fix(g)|$ en séparant les cas suivants que g soit une symétrie, l'identité ou une rotation. On utilisera à bon escient que 67 est impair, premier, et que 7 est impair.
4. Conclure.

Université Aix-Marseille 2019–2020

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

TD2 : GROUPES DE PERMUTATION

Exercice 1.

1. Décomposer $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 4 & 9 & 10 & 2 & 5 & 8 & 1 & 7 \end{pmatrix}$, puis calculer son ordre et sa signature.
2. Ecrire la permutation $(1324) \in \mathfrak{S}_4$ comme produits d'au plus 3 transpositions.

Exercice 2.

1. Déterminer le nombre
   (a) d'éléments d'ordre 8 dans $\mathfrak{S}_{42}$;
   (b) d'éléments d'ordre 20 dans $\mathfrak{S}_{15}$.
2. Montrer qu'une permutation d'ordre 14 dans $\mathfrak{S}_{10}$ possède un unique point fixe et est de signature -1.

Exercice 3. Soit $n \in \mathbb{N}^*$. On tire au hasard une permutation $\sigma \in \mathfrak{S}_n$. En supposant que les permutations sont équiréparties, calculer la probabilité que

1. σ fixe n ;
2. σ n'ait aucun point fixe ;
3. σ fixe exactement éléments avec $k \in \{1, \dots, n\}$;
4. σ possède un élément d'ordre au moins $\frac{n}{2}$.

Exercice 4. Montrer que, pour $n \geq 4$, $\mathcal{A}_n$ est engendré par les $(n-2)$ 3–cycles $(123), (124), \dots, (12n)$.

Exercice 5. Soit $n \geq 3$ un entier. Le but de l'exercice est de montrer que le centre $Z(\mathcal{S}_n)$ du groupe $\mathcal{S}_n$ est réduit à l'identité.

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

Exercice 6. Soit $G \subset \mathfrak{S}_n$ agissant transitivement sur $\{1, \dots, n\}$. Pour tout $i \in \{1, \dots, n\}$, on note $G_i \subset G$ le sous-ensemble des éléments fixant i.

1. Montrer que G_i est un sous-groupe d'indice n.
2. Montrer que $\cup_i^n G_i \neq G$.
3. En déduire qu'il existe un élément de G agissant sans point fixe.

Exercice 7.

1. Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.
2. Trouver les morphismes de S_n dans S_{n-1} pour $n \geq 5$. En déduire qu'un sous-groupe de S_n d'indice n est isomorphe à S_{n-1}.
3. Trouver les morphismes de S_n dans $\mathbb{Z}/3\mathbb{Z}$.

Exercice 8. Un des but de l'exercice est de montrer que tous les 3–cycles sont conjugués dans $\mathcal{A}_n$ dès lors que $n \geq 5$.

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

1. Montrer que $\mathcal{S}_n$ agit n–transitivement sur $\{1, \dots, n\}$.

2. Montrer que $\mathcal{A}_n$ agit $(n-2)$–transitivement sur $\{1,\dots,n\}$.
3. En déduire que, pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Exercice 9. Le but de l'exercice est de montrer que $\mathcal{A}_4$ n'est pas simple.

1. Faire la liste des éléments de $\mathcal{A}_4$, donner leurs ordres.
2. On considère l'ensemble suivant :

$$H := \left\{ \mathrm{Id} \ , \ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \ , \ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \ , \ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}.$$

   Montrer que H est un sous-groupe distingué de $\mathcal{A}_4$ isomorphe au groupe de Klein. Pour montrer qu'il est distingué, on étudiera les ordres des éléments.

Exercice 10. Le but de l'exercice est de montrer que $\mathcal{A}_5$ est simple. Pour cela, on considère $N \lhd \mathcal{A}_5$.

1. Montrer que si (12345) appartient à N, alors (23145) aussi, ainsi que (412).
2. Montrer que si (12)(34) appartient à N, alors (15)(34) aussi, ainsi que (152)
3. Conclure que $\mathcal{A}_5$ est simple.

Exercice 11. Le but de l'exercice est de montrer que $\mathcal{A}_n$ est simple pour tout $n > 5$. Pour cela, on suppose, par récurrence, que $\mathcal{A}_{n-1}$ est simple et, par l'absurde, qu'il existe $N \lhd \mathcal{A}_n$ avec $N \neq \mathcal{A}_n$ et $\sigma \in N \setminus \{\mathrm{Id}\}$.

1. On suppose ici que $\sigma(n) = n$.
   (a) Montrer que $\mathcal{A}_{n-1}$ s'identifie aux éléments de $\mathcal{A}_n$ qui fixent n et que, sous cette identification, $\mathcal{A}_{n-1} \cap N \lhd \mathcal{A}_{n-1}$.
   (b) En déduire que $\mathcal{A}_{n-1} \subset N$.
   (c) En conclure que $N = \mathcal{A}_n$.
   (d) En conclure, plus généralement, que si $\rho \in N$ avec $\rho(n) = n$, alors $\rho = \mathrm{Id}$.
2. On suppose ici que $\sigma(n) = \sigma^{-1}(n) \neq n$.
   (a) Montrer que $\sigma^2 = \mathrm{Id}$.
   (b) Soit $i \neq j \in \{1,\dots,n\} \setminus \big\{n, \sigma(n)\big\}$. On note $\tau := (ij)\big(n\sigma(n)\big)$ et $\sigma_1 := \tau.\sigma.\tau.\sigma$.
      i. Montrer que σ_1 est un élément de N fixant n.
      ii. En déduire que $\sigma = \tau.\sigma.\tau$, puis que $\sigma\big(\{i,j\}\big) = \{i,j\}$.
   (c) En conclure que $\sigma = \big(n\sigma(n)\big) \notin \mathcal{A}_n$.
3. On suppose ici que $\sigma^{-1}(n)$, n et $\sigma(n)$ sont deux à deux distincts.
   (a) Soit $i \neq j \in \{1,\dots,n\} \setminus \big\{\sigma^{-1}(n), n, \sigma(n)\big\}$. On note $\tau := (ij)\big(n\sigma(n)\big)$ et $\sigma_2 := \sigma^{-1}.\tau.\sigma.\tau.\sigma^{-1}$.
      i. Montrer que σ_2 est un élément de N fixant n.
      ii. En déduire que $\tau.\sigma.\tau = \sigma^2$, puis que $\sigma^3 = \mathrm{Id}$.
      iii. En conclure que σ est la composé de 3–cycles disjoints.
   (b) En supposant par l'absurde que σ contient un 3–cycle $\big(k, \sigma(k), \sigma^2(k)\big)$ distinct de $\big(n, \sigma(n), \sigma^2(n)\big)$, et en posant $\sigma_3 = \sigma.\big(n, k, \sigma(n)\big).\sigma.\big(n, \sigma(n), k\big)$, montrer que $k = \sigma_3(k) = \sigma(n)$.
   (c) En conclure que $N = \mathcal{A}_n$.
4. Conclure.

Exercice 12. Le but de l'exercice est de montrer que, pour tout $n \in \mathbb{N}^* \setminus \{6\}$, tous les automorphismes de $\mathfrak{S}_n$ sont *intérieurs*, c'est-à-dire de la forme $(g \mapsto g_0^{-1}.g.g_0)$ pour un certain $g_0 \in \mathfrak{S}_n$.

1. On fixe ici $n \in \mathbb{N}^* \setminus \{6\}$ et $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$.
   (a) Pour tout $\sigma \in \mathfrak{S}_n$, montrer que $Z_{\mathfrak{S}_n}\big(\varphi(\sigma)\big) = \varphi\big(Z_{\mathfrak{S}_n}(\sigma)\big)$, où $Z_{\mathfrak{S}_n}(g)$ dénote le sous-groupe des éléments de $\mathfrak{S}_n$ qui commute avec $g \in \mathfrak{S}_n$.
   (b) Pour tout $\sigma' \in \mathfrak{S}_n$, donner la décomposition en cycles disjoints de $\sigma'.\sigma.\sigma'^{-1}$ en fonction de celle de σ.
   (c) Pour tout $i \in \{1,\dots,n\}$, on note k_i le nombre de i–cycles dans la décomposition en cycles disjoints de σ. Montrer que $|Z_{\mathfrak{S}_n}(\sigma)| = \prod_{i=1}^n k_i! i^{k_i}$.
   (d) En déduire que φ envoie toute transposition sur une transposition.
   (e) En déduire que φ est intérieur.

2. Le but de cette question est de montrer que le résultat tombe en défaut pour $n = 6$.
   (a) Soit $n \geq 5$. On suppose que tous les automorphismes de $\mathfrak{S}_n$ sont intérieurs et on cherche à montrer que tout sous-groupe $H \subset \mathfrak{S}_n$ d'indice n possède un point fixe.
      i. Montrer que l'action par multiplication à gauche de $\mathfrak{S}_n$ sur les classes de H est fidèle.
      ii. En déduire un automorphisme φ_H de $\mathfrak{S}_n$ tel que $H = \varphi_H^{-1}\big(\mathrm{Stab}(1)\big)$.
      iii. En déduire que H est conjugué à $\mathrm{Stab}(1)$.
      iv. Conclure.
   (b) i. Montrer qu'il y a six 5–Sylows dans $\mathfrak{S}_5$.
      ii. Montrer que l'action par conjugaison de $\mathfrak{S}_5$ sur l'ensemble de ses 5–Sylows est fidèle et transitive.
      iii. En déduire l'existence d'un sous-groupe de $\mathfrak{S}_6$ d'indice 6 agissant transitivement sur $\{1, \ldots, 6\}$.
   (c) En déduire qu'il existe un automorphisme de $\mathfrak{S}_6$ qui ne soit pas intérieur.

Exercice 13. Le jeu de taquin est composé de 15 petits carrés numérotés de 1 à 15 disposés sur les cases d'une grille carrée de coté 4. Une des cases de la grille est donc vide et chacun des carrés peut être déplacé horizontalement ou verticalement d'une case lorsqu'il jouxte la case vide (il vient donc se positionner sur la case anciennement vide, et son ancienne case devient vide) :

La position initiale est

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

et le but du jeu est d'arriver à la position

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

.

Montrer que cela est impossible.

Université Aix-Marseille 2019–2020

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

TD3 : GROUPES LINÉAIRES

Dans tout ce qui suit, E est un espace vectoriel de dimension $n \in \mathbb{N}^*$ sur un corps k.

Exercice 1.

1. Dans $\mathrm{GL}_2(\mathbb{R})$, déterminer l'orbite sous l'action par conjugaison de la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Faire de même pour $\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$.
2. Montrer que les matrices $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$, avec $\lambda, \mu \in k^*$ sont conjuguées dans $\mathrm{SL}_2(k)$ ssi $\frac{\lambda}{\mu}$ est un carré dans k. En déduire le nombre de classes de conjugaison de ces matrices lorsque $k = \mathbb{C}$, $k = \mathbb{R}$ et $k = \mathbb{Q}$.

Exercice 2. Montrer que $\mathrm{GL}(E) \cong k^* \rtimes_\varphi \mathrm{SL}(E)$ pour une action φ de k^* sur $\mathrm{GL}(E)$ que l'on précisera.

Exercice 3. On suppose dans cet exercice que $k = \mathbb{R}$ ou $\mathbb{C}$ et on munit $\mathrm{GL}(E)$ et $\mathrm{SL}(E)$ de la topologie induite par celle de k^{n^2} en fixant une base de E et l'utilisant pour identifier $\mathrm{GL}(E)$ à $\mathrm{GL}_n(k)$.

1. Montrer que le produit matriciel est continu.
2. Montrer que le déterminant est continu.
3. Montrer que l'application inverse est continue.
4. Montrer que la topologie ne dépend pas du choix de la base.

Exercice 4. Pour tout ensemble topologique X, on dit que deux éléments $x_1, x_2 \in X$ sont *connectés par arc* s'il existe un chemin $\gamma : [0,1] \to X$ continue tel que $\gamma(0) = x_1$ et $\gamma(1) = x_2$. Cela définit une relation d'équivalence sur X, les classes de la partition associée de X sont appelées *composantes connexes* de X. On dit que X est *connexe par arcs* s'il ne possède qu'une seule composante connexe.

On munit $\mathrm{GL}(E)$ et $\mathrm{SL}(E)$ de la topologie de l'exercice précédent.

1. On suppose dans cette question que $k = \mathbb{R}$.
   (a) Montrer que $\mathrm{SL}(E)$ est connexe par arcs.
   (b) Montrer que $\mathrm{GL}_n(k)$ a deux composantes connexes.
2. On suppose dans cette question que $k = \mathbb{C}$. Montrer que $\mathrm{SL}(E)$ et $\mathrm{GL}(E)$ sont connexes par arcs.

Exercice 5. Soit $u \in \mathrm{GL}(E)$ et $1 \leq r \leq n-1$. Montrer que si u laisse stable tous les sous espaces vectoriels de dimension r alors u est une homothétie.

Exercice 6.

1. Montrer que le conjugué d'une transvection de droite D par $u \in \mathrm{GL}(E)$ est une transvection de droite $u(D)$.
2. Déterminer le centre de $\mathrm{GL}(E)$.
3. Déterminer le centre de $\mathrm{SL}(E)$.

Exercice 7. On suppose dans cet exercice que $n \geq 3$ et que k est de caractéristique différente de 2. On rappelle que sous-groupe dérivé $D(G)$ d'un groupe G est le sous-groupe engendré par les commutateurs de la forme $[g_1, g_2] = g_1^{-1}.g_2^{-1}.g_1.g_2$ avec $g_1, g_2 \in G$.

1. Soit τ une transvection de E. Montrer que τ^2 est également une transvection et en déduire qu'il existe $u \in \mathrm{GL}(E)$ tel que $\tau = [\tau, u]$.
2. Montrer que $D\big(\mathrm{GL}(E)\big) = D\big(\mathrm{SL}(E)\big) = \mathrm{SL}(E)$.

Exercice 8. Le but de l'exercice est de montrer que, si k n'est pas de caractéristique 2, $\mathrm{GL}(E)$ est engendré par les automorphismes diagonalisables (et, de manière équivalente, par les dilatations).

1. Montrer que $u \in \mathrm{GL}(E)$ est une transvection ou une dilatation ssi il existe $a \in E \setminus \{0\}$ et une forme linéaire $\varphi \in E^*$ tels que $u = \mathrm{Id}_E + \varphi.a$ (càd $u(x) = x + \varphi(x).a$ pour tout $x \in E$), u étant alors une transvection ssi $a \in \mathrm{Ker}(\varphi)$.
2. On suppose dans cette question que k n'est pas de caractéristique 2.
   (a) En reprenant les notations de l'exercice précédent, soit $u =: \mathrm{Id}_E + \varphi.a$ une transvection.
      i. Montrer qu'il existe une forme linéaire $\varphi_1 \in E^*$ valant 1 en a.
      ii. Montrer que $\varphi_2 := \frac{1}{2}(\varphi - \varphi_1)$ est une forme linéaire qui ne s'annule pas en a.
      iii. Montrer que $u = u_1 \circ u_2$ avec $u_i := \mathrm{Id}_E + \varphi_i.a$ pour $i = 1, 2$.
   (b) Montrer que $\mathrm{GL}(E)$ est engendré par les dilatations.
   (c) Montrer que $\mathrm{GL}(E)$ est engendré par les automorphismes diagonalisables.

Exercice 9. Le but de l'exercice est de montrer que, si $n \geq 2$, $\mathrm{GL}(E)$ est engendré par les automorphismes de trace nulle.

1. Ecrire la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ comme produit de deux matrices de trace nulle.
2. On suppose dans cette question que $n \geq 3$.
   (a) Montrer que tout automorphisme de E qui permute cycliquement les éléments d'une base de E est de trace nulle.
   (b) Montrer que toute transvection peut s'écrire comme composé de deux automorphismes de trace nulle.
3. Montrer que $\mathrm{SL}(E)$ est engendré par les automorphismes de trace nulle.
4. Montrer que $\mathrm{GL}(E)$ est engendré par les automorphismes de trace nulle.

Exercice 10.

1. On appelle drapeau toute suite $\mathbf{V} := (V_0, v_1, \ldots, v_n)$ de sous-espace vectoriels de E strictement croissante pour l'inclusion.
   (a) i. Montrer que, pour tout drapeau $\mathbf{V}$, on a $V_0 = \{0\}$ et $V_n = E$.
   ii. Montrer que l'application
   $$\delta : \begin{array}{ccc} \big\{\text{base } (e_1, \ldots, e_i) \text{ de } E\big\} & \to & \big\{\text{drapeau de } E\big\} \\ (e_1, \ldots, e_i) & \mapsto & \big(\mathrm{Vect}(e_1, \ldots, e_i)\big)_{i \in \{0, \ldots, n\}} \end{array}$$
   est surjective. On dit qu'une base $\mathcal{B}$ est *adaptée* à un drapeau $\mathbf{V}$ si $\delta(\mathcal{B}) = \mathbf{V}$; et on dit qu'elle est *quasi-adaptée* à $\mathbf{V}$ si une permutation de ses éléments donne une base adaptée à $\mathbf{V}$.
   iii. Montrer que $\mathrm{GL}(E)$ agit transitivement sur l'ensemble des drapeaux et montrer que le stabilisateur d'un drapeau est isomorphe au groupe des matrices triangulaires supérieures inversibles.
   (b) Soit $\mathbf{V}$ et $\mathbf{W}$ deux drapeaux. On définit $s : \{1, \ldots, n\} \to \{1, \ldots, n\}$ par
   $$s(i) := \min\big\{j \in \{1, \ldots, n \mid W_i \subset W_{i-1} + v_j\big\}.$$
   i. Montrer que $s \in \mathfrak{S}_n$ et que toute permutation peut être ainsi réalisée.
   ii. En construisant une famille $(x_1, \ldots, x_n)$ d'éléments de E telle que, pour tout $i \in \{1, \ldots, n\}$,
   $$\begin{cases} W_i = W_{i-1} \oplus k.x_i \\ V_{s(i)} = V_{s(i)-1} \oplus k.x_i \\ x_i \notin W_{i-1} + V_{s(i)-1} \end{cases},$$
   montrer qu'il existe une base simultanément adaptée à $\mathbf{W}$ et quasi-adaptée à $\mathbf{V}$.
   (c) Soit $A \in \mathrm{GL}_n(k)$. On note
   - $\mathcal{B}_1$ la base canonique de k^n,
   - $\mathcal{B}_2$ la base formée par les colonnes de A,

- $\mathcal{B}_1'$ une base adaptée à $\delta(\mathcal{B}_1)$ et quasi-adaptée à $\delta(\mathcal{B}_2)$,
- $\mathcal{B}_2'$ la permutation de $\mathcal{B}_1'$ adaptée à $\delta(\mathcal{B}_2)$.

i. Montrer que la matrice de passage
   - de $\mathcal{B}_2$ vers $\mathcal{B}_2'$ est triangulaire supérieure,
   - de $\mathcal{B}_2'$ vers $\mathcal{B}_1'$ est une matrice de permutation,
   - de $\mathcal{B}_1'$ vers $\mathcal{B}_1$ est triangulaire supérieure et que, quitte à renormaliser, on peut même supposer qu'elle est unipotente (c'est-à-dire avec des 1 sur la diagonale).

ii. En déduire que A s'écrit sous la forme UPV avec U une matrice triangulaire supérieure unipotente, P une matrice de permutation et V une matrice triangulaire supérieure.

(d) Montrer que

$$\mathrm{GL}_n(k) = \bigsqcup_{\sigma \in \mathfrak{S}_n} \mathcal{U} P_\sigma \mathcal{T}$$

où $\mathcal{U}$ est le sous-groupe des matrices triangulaires supérieures unipotentes, $\mathcal{T}$ le sous-groupe des matrices trinagulaires supérieures inversibles, et P_σ la matrice associée à la permutation σ (attention, il s'agit d'une réunion disjointe sur $\mathfrak{S}_n$). C'est ce qu'on appelle la *décomposition de Bruhat*.

2. Redémontrer l'existence de la décomposition de Bruhat par des considérations d'opérations sur les lignes et les colonnes.

Aix–Marseille Université 2019-2020

Mathématiques – Master 1

TDS

1 Polynômes

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

Exercice 2 Montrer que f est irréductible dans $\mathbb{Q}[X]$ en utilisant le critère d'Eisenstein :

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

Exercice 3 On considère les trois matrices I, J, K suivantes.

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Soit $\mathbb{H}$ l'ensemble des matrices de la forme $aId + bI + cJ + dK$ avec a, b, c, d réels.

1. Montrer que $\mathbb{H}$ est un corps. Montrer que c'est un espace vectoriel sur $\mathbb{R}$.
2. Trouver un automorphisme de ce corps.
3. Montrer que $A \to \sqrt{detA}$ est une norme.

Exercice 4 Soit $E = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}\}$

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

Exercice 5 Soit E le $\mathbb{Q}$ espace vectoriel engendré par $1, \sqrt{2}, \sqrt{3}$.

1. Montrer qu'il est de dimension trois.
2. Soit F le $\mathbb{Q}(\sqrt{2})$ espace vectoriel engendré par $1, \sqrt{3}$. Montrer qu'il est de de dimension deux.

3. En déduire que F est un $\mathbb{Q}$ espace vectoriel de dimension quatre. On utilisera le fait que $\mathbb{Q}(\sqrt{2})$ est un corps.

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

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

Exercice 7 Montrer que $[\mathbb{Q}(\sqrt{2}, 2^{1/3}) : \mathbb{Q}] = 6$. En déduire qu'il est égal à $\mathbb{Q}(2^{1/6})$

2 Anneau et corps

Exercice 8 On considère l'ensemble

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

1. Montrer que c'est un anneau intègre.
2. Montrer que $z \mapsto \overline{z} = a - ib$ est un automorphisme d'anneaux.
3. Montrer que $z \mapsto N(z) = z\overline{z}$ est multiplicative.
4. Trouver $\mathbb{Z}[i]^*$.
5. Montrer que l'anneau est euclidien relativement à N. On utilisera la notion d'entier le plus proche d'un réel.

Exercice 9 On considère l'ensemble

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

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

Exercice 10 Pour $n \in \mathbb{N}^*$, soit $\mathcal{P}_n$ l'ensemble des racines n-èmes primitives de l'unité dans $\mathbb{C}$. On pose $\Phi_1(X) = X - 1$ et $\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n} (X - \zeta)$. Φ_n est appelé *le n-ème polynôme cyclotomique* (son degré est $\varphi(n)$ où φ est l'indicateur d'Euler).

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

Exercice 11

1. Montrer que $\mathbb{Q}[\sqrt{7}], \mathbb{Q}[\sqrt{11}]$ sont des corps. Montrer que ce sont des espaces vectoriels sur $\mathbb{Q}$ de dimension 2.
2. Montrer que l'application suivante n'est pas un morphisme de corps

$$\begin{array}{ccc} \mathbb{Q}[\sqrt{7}] & \mapsto & \mathbb{Q}[\sqrt{11}] \\ a + b\sqrt{7} & \mapsto & a + b\sqrt{11} \end{array}$$

3. Montrer que ces corps ne sont pas isomorphes.

Exercice 12 Soit k un corps et P un polynôme sur k de degré n. Soit K un corps contenant k, tel que ce soit un espace vectoriel sur k de dimension m.

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

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

Exercice 13 En utilisant les réductions $\mod 2$ ou $\mod 3$ montrer que les polynômes suivant sont irréductibles dans $\mathbb{Z}[X]$:

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

Exercice 14 Soit α un nombre algébrique.

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

3 Corps finis

Exercice 15 Déterminer à isomorphisme près tous les corps de cardinal 4.

Exercice 16 Soit p un nombre premier. Montrer qu'il y a $\frac{p(p-1)}{2}$ polynômes irréductibles de degré deux dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 17 Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $X^2 - 3X + a = 0$ en fonction de a.

Exercice 18 Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{F}_5$.

Trouver les polynômes irréductibles de degré inférieur ou égal à 4 sur $\mathbb{F}_2$.

Exercice 19 Soit $\mathbb{K}$ un corps de caractéristique p et $f : x \mapsto x^k$.

Trouver des conditions pour que ce soit une bijection.

Exercice 20 Donner une description des éléments du groupe des inversibles de $\mathbb{F}_9$.

Exercice 21 On considère des corps à 16 éléments.

1. Montrer que $\mathbb{Z}_2[X]/(X^4 + X + 1)$ est isomorphe à un tel corps.
2. Montrer que $\mathbb{Z}_2[X]/(X^4 + X^3 + 1)$ est isomorphe à un tel corps.
3. Trouver le groupe des inversibles de chacun de ces corps en fonction de la classe de X.
4. Trouver les isomorphismes entre ces deux corps.

Exercice 22 Le but est de montrer que -1 est un carré de $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p = 1 \mod 4$. Soit F^2 l'ensemble des éléments de $\mathbb{F}_p^*$ qui s'écrivent comme carré d'un élément.

1. Montrer que $x \in F^2 \iff x^{(p-1)/2} = 1$:
   (a) Considérer $x \mapsto x^2$. Montrer que c'est un morphisme et calculer son noyau.

(b) Conclure par un argument de cardinalité.

2. En déduire le résultat.

Exercice 23 Le but est de montrer que Φ_8 est réductible dans tout corps fini.

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

4 Cercles et droites

Exercice 24 Montrer que l'on peut construire un carré d'aire $2a^2$ connaissant un carré d'aire a^2.

Exercice 25 Montrer que l'on peut diviser un angle en deux parties égales à la règle et au compas.

Exercice 26 Montrer que l'on peut diviser un segment en n parties égales à la règle et au compas.

Exercice 27 Etant donné un cercle, montrer que l'on ne peut construire un carré de même aire que le disque.

Exercice 28 Construire un pentagone régulier à la règle et au compas.

5 Théorie de Galois

Exercice 29 Déterminer les corps de décomposition sur $\mathbb{Q}$ de $X^4 + 1, X^4 - 2$.

Exercice 30 Soit $a = (1-\sqrt{2})^{1/3}$. Montrer que a est algébrique sur $\mathbb{Q}$ et exprimer $\frac{1}{a^2+1}$.

Exercice 31 Soit a une racine complexe de $X^2 + 2X + 5$. Exprimer $\frac{a^3+a+2}{a^2-1}$ en fonction de a.

Exercice 32 On considère $\alpha = \sqrt{2} + \sqrt{5}$ et $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

1. Montrer que K est une extension galoisienne de $\mathbb{Q}$.
2. Trouver le cardinal du groupe de Galois et montrer qu'il possède deux éléments d'ordre deux.
3. En déduire le groupe de Galois et trouver les extensions intermédiaires entre $\mathbb{Q}$ et K.

Exercice 33

1. Montrer que toute extension de $\mathbb{Q}$ de degré deux est galoisienne.
2. Soit ω_n une racine n-ème primitive de l'unité. Montrer que $\mathbb{Q}(\omega_n)$ est galoisienne.
3. Montrer que si $K = \mathbb{Q}[\sqrt{5}]$, alors $L = \mathbb{Q}[\sqrt{2+\sqrt{5}}]$ est galoisienne sur K mais pas sur $\mathbb{Q}$.

Exercice 34 Soit $\alpha = 2^{1/3}$ et $K = \mathbb{Q}[j, \alpha]$ le corps de décomposition de $X^3 - 2$.

1. Montrer que K est une extension galoisienne de $\mathbb{Q}$ et déterminer le cardinal du groupe de Galois.
2. Montrer que l'on peut trouver deux éléments f, g du groupe de Galois en définissant.
$$f(\alpha) = \alpha f(j) = j^2, g(\alpha) = j\alpha, g(j) = j$$
3. Montrer que $g^2 = f^{-1}gf$. En déduire le groupe de Galois.
4. Trouver les extensions intermédiaires entre $\mathbb{Q}$ et K.

Exercice 35 Soit $z = e^{2i\pi/5}$.

1. Montrer que $X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{Q}[X]$
2. Calculer le polynôme minimal de z sur $\mathbb{Q}$.
3. En déduire que $\mathbb{Q}(z)$ est une extension galoisienne. Trouver son degré.
4. Montrer que
$$\begin{array}{ccc} \mathbb{Q}(z) & \to & \mathbb{Q}(z) \\ a + bz + cz^2 + dz^3 + ez^4 & \to & a + bz^2 + cz^4 + dz + ez^3 \end{array}$$
est un $\mathbb{Q}$ automorphisme de $\mathbb{Q}(z)$.

5. Calculer le groupe de Galois de $\mathbb{Q}(z)$.
6. En déduire un corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(z)$.

.

Exercice 36 On considère le polynôme cyclotomique Φ_n et ω_n une racine n-ème primitive de l'unité.

Montrer que le corps de décomposition de Φ_n est égal à $\mathbb{Q}(\omega_n)$. En déduire que le groupe de Galois de Φ_n est le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.