Feuille G1 — RAPPEL SUR LES GROUPES

Mode d'emploi. Tout énoncé portant un numéro est un exercice, parfois implicite. Explicitez d'abord ce qui est clair et ce qu'il faut encore montrer. Ne craignez point : les énoncés sont coupés en petites étapes. Une étoile marquera des exercices ☆ longs ou ★ exigeants.

1. QUELQUES QUESTIONS DE RÉVISION

1.1. Donner un groupe fini abélien, fini non abélien, infini abélien, infini non abélien.

1.2. Quand est-ce que $G \to G$, $x \mapsto x^{-1}$ est un homomorphisme de groupe ? et $x \mapsto x^2$?

1.3. Est-ce que l'image d'un sous-groupe est un sous-groupe ? l'image réciproque ?

1.4. Quels sous-groupes peuvent être noyau ? Donner des exemples et des contre-exemples.

1.5. Un sous-groupe d'indice 2 est distingué. Un sous-groupe distingué d'ordre 2 est central.

1.6. Le groupe $\mathbb{Z}$ est monogène. Quels sont ses générateurs ? Quels sont ses sous-groupes ?

1.7. Le groupe $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ est cyclique. Quels sont ses générateurs ? Combien y en a-t-il ?

1.8. Soit $G = \{a, b, c\}$ muni de la loi de composition définie ci-contre. Est-ce un groupe ? Quels sous-ensembles H forment un groupe ? Est-ce que $|H|$ divise $|G|$? La multiplication induit-elle une action de groupe $H \times G \to G$? Déterminer les orbites. Sont-elles toutes de même cardinal ?

·	a	b	c
a	a	b	c
b	b	a	c
c	b	b	a

1.9. Énoncer le théorème de Lagrange, puis en donner une preuve.

2. GROUPES CYCLIQUES

2.1. Énoncer le théorème d'isomorphisme (factorisation canonique d'un homomorphisme).

2.2. En déduire que tout groupe *monogène* est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$.
Est-ce que tout groupe d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$? Et si n est premier ?

2.3. Montrer que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $d\mathbb{Z}/n\mathbb{Z}$ avec $d|n$, $d \geq 1$.
Expliciter son ordre et son indice. (Et $3\mathbb{Z}/10\mathbb{Z}$, est-il un sous-groupe de $\mathbb{Z}/10\mathbb{Z}$?)

2.4. Pour $K = \ker(\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z}/n\mathbb{Z})$ déterminer $d \in \mathbb{Z}$ de sorte que $K = d\mathbb{Z}/n\mathbb{Z}$.

2.5. Expliciter tous les homomorphismes $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

3. ORDRE D'UN PRODUIT VS LE PRODUIT DES ORDRES

Soient $a, b \in G$ deux éléments qui commutent. On pose $m = \mathrm{ord}(a)$ et $n = \mathrm{ord}(b)$.

3.1. Montrer que $\mathrm{ord}(ab) \mid \mathrm{ppcm}(m, n)$. Illustrer que $\mathrm{ord}(ab) < \mathrm{ppcm}(m, n)$ est possible.

3.2. Si $G = A \times B$ avec $a \in A$ et $b \in B$, alors $\mathrm{ord}(ab) = \mathrm{ppcm}(m, n)$.

3.3. Si $\mathrm{pgcd}(m, n) = 1$, alors $\mathrm{ord}(ab) = mn$. *Indication :* Bézout puis Lagrange.

3.4. En déduire qu'il existe toujours $c \in \langle a, b \rangle$ avec $\mathrm{ord}(c) = \mathrm{ppcm}(m, n)$.

3.5. Donner un exemple non commutatif où $\mathrm{ord}(xy)$ ne divise pas mn.
Pour $k \geq 1$ donné, peut-on trouver $\mathrm{ord}(x) = \mathrm{ord}(y) = 2$ et $\mathrm{ord}(xy) = k$?

4. UNE BELLE CARACTÉRISATION DES GROUPES CYCLIQUES

4.1. Soit G un groupe abélien d'ordre n. Les conditions suivantes sont équivalentes :

(a) Le groupe G est cyclique.

(b) Pour tout diviseur $d|n$ il existe un unique sous-groupe d'ordre d dans G.

(c) Pour tout diviseur $d|n$ il existe au plus un sous-groupe d'ordre d dans G.

Indication : L'implication $(a) \Rightarrow (b)$ est facile, et $(b) \Rightarrow (c)$ est triviale. Pour $(c) \Rightarrow (a)$ on pourra regarder un élément $g \in G$ d'ordre maximal et montrer que $G = \langle g \rangle$.

4.2. *Application :* Soit K un corps et $G \subset K^\times$ un sous-groupe multiplicatif *fini*. Alors G est cyclique. En particulier, pour tout p premier le groupe multiplicatif $\mathbb{Z}_p^\times$ est cyclique.

5. Le théorème de Cauchy

5.1. La réciproque du théorème de Lagrange est fausse : si n divise $|G|$ il n'y a pas forcément un sous-groupe d'ordre n. Trouver un groupe d'ordre 12 qui n'a pas de sous-groupe d'ordre 6.

Le théorème suivant nous dit que tout se passe bien pour un facteur *premier* de $|G|$. Il s'agit d'un cas particulier du célèbre théorème de Sylow, dont on fera connaissance plus tard.

Théorème 1. *Pour tout facteur premier p de $|G|$ il existe un élément d'ordre p dans G.*

5.2. On note $S = \{(x_1, x_2, \dots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = 1\}$. Montrer que $|S| = |G|^{p-1}$ en explicitant deux applications $S \to G^{p-1}$ et $G^{p-1} \to S$, inverses l'une à l'autre.

5.3. La rotation $(x_1, x_2, \dots, x_p) \mapsto (x_2, \dots, x_p, x_1)$ définit une bijection $r\colon S \to S$ d'ordre p. Les orbites sous l'action de $\langle r \rangle$ sont de cardinal p ou 1. Dans le dernier cas, l'orbite est de la forme $\{(x, x, \dots, x)\}$ avec $x^p = 1$. Exemple trivial : $(1, 1, \dots, 1)$.

5.4. En déduire l'existence d'un élément d'ordre p dans G. Combien y en a-t-il modulo p ?
S'il y a k sous-groupes d'ordre p, quel est le nombre ν_p d'éléments d'ordre p ?
En déduire deux congruences nécessaires pour ν_p.

5.5. Quelles sont les cinq plus petites valeurs non nulles possibles pour ν_3 ?
Connaissez-vous des groupes qui contiennent un tel nombre d'éléments d'ordre 3 ?

6. L'exposant d'un groupe

6.1. On appelle *exposant* d'un groupe fini G, noté $\exp(G)$, le plus petit entier $m \geq 1$ tel que $x^m = 1$ pour tout $x \in G$. Vérifier que $I = \{n \in \mathbb{Z} \mid g^n = 1 \text{ pour tout } g \in G\}$ est un idéal. Montrer que I est non nul, engendré par $\exp(G)$, et que $\exp(G)$ divise $|G|$.

6.2. Montrer que $\exp(G) = \operatorname{ppcm}\{\operatorname{ord}(x) \mid x \in G\}$. Comparer l'ordre et l'exposant de $\mathbb{Z}_{ab}$ et de $\mathbb{Z}_a \times \mathbb{Z}_b$. Donner un critère nécessaire et suffisant pour que $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$.

6.3. Tout groupe d'exposant 2 est abélien. (NB : ce n'est plus vrai pour un premier $p \geq 3$.)

6.4. Supposons que le groupe G est abélien et d'exposant premier $p \geq 2$. De manière canonique G est un espace vectoriel sur le corps $\mathbb{Z}_p$. Si de plus G est fini, alors $G \cong \mathbb{Z}_p^d$.

7. Groupes d'ordre p, p^2, p^3

7.1. Soit $p \geq 2$ un nombre premier. Montrer que tout groupe d'ordre p est isomorphe à $\mathbb{Z}_p$.

7.2. (a) Si G est d'ordre p^k alors le centre $Z(G)$ est non trivial. *Indication :* Faire agir G sur lui-même par conjugaison, puis regarder la formule des classes modulo p.

(b) Si $\bar{G} = G/Z(G)$ est cyclique alors G est abélien. *Indication :* Soit $g \in G$ un antécédent d'un générateur $\bar{g} \in \bar{G}$. Tout élément de G s'écrit $g^k z$ avec $k \in \mathbb{Z}$ et $z \in Z(G)$.

(c) Un groupe d'ordre p^2 est abélien. Exemples évidents : $\mathbb{Z}_p^2$ et $\mathbb{Z}_{p^2}$. Sont-ils isomorphes ? Existe-t-il d'autres groupes d'ordre p^2, non isomorphes à $\mathbb{Z}_p^2$ ou $\mathbb{Z}_{p^2}$?

7.3. Déterminer l'ordre et l'exposant des groupes $\mathbb{Z}_p^3$ et $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ et $\mathbb{Z}_{p^3}$. Sont-ils isomorphes ?

7.4. Dans $\mathrm{GL}_2 \mathbb{R}$ on considère $I = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Vérifier que $D_4 = \langle I, R \rangle$ est le groupe des isométries d'un carré. Déterminer son ordre en dressant une table de multiplication pour $1, I, R, S$. Déterminer le centre, puis la structure de $D_4/Z(D_4)$.

7.5. Dans $\mathrm{GL}_2 \mathbb{C}$ on considère $I = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $J = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $K = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. Le groupe $Q := \langle I, J \rangle$ est appelé le *groupe des quaternions*. Déterminer son ordre en dressant une table de multiplication pour $1, I, J, K$. Déterminer le centre, puis la structure de $Q/Z(Q)$.

7.6. Montrer qu'il existe au moins 5 groupes non isomorphes d'ordre 8.

7.7. Pour $p \geq 3$ premier soit $G = \left\{ \left(\begin{smallmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_3 \mathbb{Z}_p \right\}$ et $H = \left\{ \left(\begin{smallmatrix} 1+ap & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2 \mathbb{Z}_{p^2} \right\}$.

(a) S'agit-il de sous-groupes ? Déterminer l'ordre et l'exposant. G et H sont-ils isomorphes ?

(b) Déterminer les centres, puis la structure de $G/Z(G)$ et $H/Z(H)$. Sont-ils isomorphes ?

7.8. Montrer qu'il existe au moins 5 groupes non isomorphes d'ordre p^3, avec $p \geq 3$ premier.

Feuille G2 — GROUPES SYMÉTRIQUES

Résumé. Le groupe symétrique est un des exemples phares dans la théorie des groupes et omniprésent dans les applications. Cette feuille en discute quelques propriétés de base.

Notation. On note S_X ou $\mathfrak{S}_X$ ou $\mathrm{Sym}(X)$ le groupe symétrique sur un ensemble X. On note A_X ou $\mathfrak{A}_X$ ou $\mathrm{Alt}(X)$ le groupe alterné, c'est-à-dire le sous-groupe des permutations paires. Dans le cas particulier $X = \{1, 2, \dots, n\}$ il est commode d'écrire S_n et A_n au lieu de S_X et A_X.

1. GROUPES SYMÉTRIQUES

1.1. Pour $A \subset X$ montrer que $S_{X,A} = \{\sigma \in S_X \mid \sigma(A) = A\}$ est un sous-groupe. Vérifier que l'application $r\colon S_{X,A} \to S_A \times S_{X \smallsetminus A}$ donnée par $\sigma \mapsto (\sigma|_A, \sigma|_{X \smallsetminus A})$ est bien définie. Montrer qu'il s'agit d'un isomorphisme. L'application $\iota\colon S_A \to S_{X,A}$ donnée par $\iota(\sigma)(x) = \sigma(x)$ pour $x \in A$, et $\iota(\sigma)(x) = x$ pour $x \in X \smallsetminus A$, est un homomorphisme injectif.

1.2. Expliciter comment S_{n-1} est un sous-groupe de S_n. Quelle est l'orbite de n sous l'action de S_n ? Quel est son stabilisateur ? En déduire que $|S_n| = n!$ par récurrence sur n.

1.3. Deux permutations $\sigma, \tau \in S_X$ à supports disjoints commutent. Mieux : ils engendrent un produit direct $\langle \sigma, \tau \rangle = \langle \sigma \rangle \times \langle \tau \rangle$. En particulier $\mathrm{ord}(\sigma, \tau) = \mathrm{ppcm}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau))$.

1.4. Donner deux permutations σ, τ à supports non disjoints qui engendrent un produit direct $\langle \sigma, \tau \rangle = \langle \sigma \rangle \times \langle \tau \rangle$. Donner deux permutations α, β qui commutent et vérifient $\mathrm{ord}(\alpha\beta) = \mathrm{ppcm}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$ sans que le groupe engendré soit un produit direct.

2. DÉCOMPOSITION EN CYCLES DISJOINTS

2.1. Qu'est-ce qu'un cycle ? des cycles disjoints ? Formuler un énoncé aussi précis que possible sur la décomposition d'une permutation en cycles disjoints.

2.2. Décomposer en cycles disjoints $\mathbb{Z}_{12} \to \mathbb{Z}_{12}$, $x \mapsto 5x + 1$, puis $\mathbb{Z}_{15} \to \mathbb{Z}_{15}$, $x \mapsto 2x$.
Décomposer en cycles disjoints l'action par conjugaison de (1234) sur A_4.

2.3. Déterminer $\mathrm{ord}[(12)(345)(5789)]$. Formuler puis prouver un énoncé sur l'ordre d'une permutation. Quels ordres sont possibles dans S_6 ? dans S_{10} ? Déterminer l'exposant de S_n.

2.4. Est-ce que la puissance σ^k d'un n-cycle σ est forcément un cycle ? Donner un critère nécessaire est suffisant. *Indication :* Établir le rapport avec les générateurs de $(\mathbb{Z}_n, +)$.

3. FAMILLES GÉNÉRATRICES DE S_n ET DE A_n

3.1. Montrer par récurrence que les transpositions $(12), (23), \dots, (n-1, n)$ engendrent S_n.
En déduire que S_n peut être engendré par deux éléments seulement.

3.2. Montrer par récurrence que les 3-cycles $(123), (234), \dots, (n-2, n-1, n)$ engendrent A_n.
Est-ce que A_n peut être engendré par deux éléments ?

Pour vous amuser, regardons le jeu de taquin esquissé ci-contre : dans une grille 4×4 on a enlevé une pièce en haut à gauche. De manière évidente on peut maintenant bouger les autres pièces une par une. Quand la case vide retourne à sa position initiale on a construit une permutation $\sigma \in S_{15}$.

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

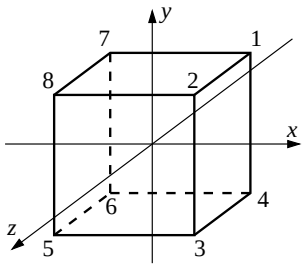
3.3. ☆ Combien de configurations $\sigma \in S_{15}$ sont possibles ?

Indication : Évidemment cette question n'est pas abordable par un comptage naïf. Heureusement elle devient facile en appliquant un peu de théorie des groupes. Les permutations obtenues forment-elles un sous-groupe de S_{15} ? Pour une minoration essayer de réaliser (123) puis un cycle $(123\dots)$ de longueur 15 ; quel sous-groupe obtient-on ? Pour une majoration on pourra se placer dans S_{16} et compter les transpositions nécessaires pour retourner.

Un exemple plus célèbre de ce genre mais beaucoup plus complexe est *Rubik's Cube*. Si vous vous intéressez au calcul formel, je vous conseille vivement de consulter GAP, un logiciel libre extrêmement puissant en groupes finis (cf. `www.gap-system.org`). Vous y trouverez en particulier une analyse de Rubik's Cube comme exemple d'utilisation. ☆ *Projet :* Installez GAP, faites quelques expériences, puis partagez votre savoir-faire dans une des prochaines séances de TD.

4. LE DÉ SUR L'ÉCHIQUIER

Soit O le groupe des isométries d'un cube (rotations et réflexions) et O^+ le sous-groupe des isométries directes (rotations seulement). On note α, β, γ les rotations d'angle $+\frac{\pi}{2}$ autour des axes x, y, z, et σ la symétrie centrale de $\mathbb{R}^3$. (Est-ce une rotation ou une réflexion ?)



4.1. Regarder l'action de O^+ sur les 8 sommets. Pour un sommet donné, quelle est son orbite ? Quel est son stabilisateur ? En déduire l'ordre du groupe O^+. Que dire du groupe O ?

4.2. L'action de O sur les sommets $1, 2, 3, 4, 5, 6, 7, 8$ induit un homomorphisme $O \to S_8$. Est-il injectif ? surjectif ? Décomposer l'action de $\alpha, \beta, \gamma, \sigma$ en cycles disjoints.

4.3. Analyser l'action de O^+ sur les 6 faces $F_1 = \{1, 2, 3, 4\}$, $F_2 = \{5, 6, 7, 8\}$, $F_3 = \{1, 2, 7, 8\}$, $F_4 = \{3, 4, 5, 6\}$, $F_5 = \{2, 3, 5, 8\}$, $F_6 = \{1, 4, 6, 7\}$. Pour une face donnée, quelle est son orbite ? Quel est son stabilisateur ? Que dire dans le cas du groupe O ? L'action induit un homomorphisme $O \to S_6$. Est-il injectif ? surjectif ? Expliciter l'action de $\alpha, \beta, \gamma, \sigma$.

4.4. L'action de O^+ sur les diagonales $D_1 = \{1, 5\}$, $D_2 = \{2, 6\}$, $D_3 = \{3, 7\}$, $D_4 = \{4, 8\}$ induit un homomorphisme $O^+ \to S_4$. Est-il injectif ? surjectif ? Expliciter l'action de α, β, γ. Analysez l'homomorphisme $O \to S_4$. Le groupe $\langle\sigma\rangle$ est-il distingué dans O ? Est-il central ?

4.5. Calculer $\alpha\beta\alpha^{-1}$ et $\alpha^{-1}\beta\alpha$ dans une des représentations précédentes, puis l'interpréter géométriquement. A-t-on $O^+ = \langle\alpha, \beta\rangle$? puis $O = \langle\alpha, \beta, \sigma\rangle$? même $O = \langle\alpha, \beta\sigma\rangle$?

4.6. ☆ On pose un dé sur une case d'un échiquier. Le dé peut être basculé sur une autre face, par une rotation autour d'une de ses arêtes, de sorte qu'il occupe une case voisine. En enchaînant ces mouvements, on peut faire rouler le dé sur l'échiquier.

(a) En retournant à la case initiale, quelles rotations sont réalisables ?

(b) En fixant l'orientation du dé, quelles translations sont réalisables ?

5. D'AUTRES FAMILLES GÉNÉRATRICES DE S_n

5.1. À titre d'avertissement, pour $n \geq 4$ composé, expliciter une transposition τ et un $n-$cycle ρ qui n'engendrent pas S_n. (Pour $n = 4$ penser aux isométries d'un carré.)

5.2. Soient p un nombre premier, τ une transposition et ρ un p-cycle dans S_p.
Alors S_p est engendré par τ et ρ. Où utilise-t-on la primalité de p ?

5.3. Les transpositions $\tau_i = (i, i+1)$ engendrent S_n et vérifient les relations $\tau_i\tau_j\tau_i = \tau_j\tau_i\tau_j$ pour $|i - j| = 1$ et $\tau_i\tau_j = \tau_j\tau_i$ pour $|i - j| \geq 2$. *Nota bene :* La famille $t_1 = \cdots = t_{n-1} = (12)$ vérifie aussi ces relations sans qu'elle engendre S_n, $n \geq 3$. La famille $t_1 = (12)$, $t_2 = (23)$, $t_3 = (12)$ dans S_4 vérifie les relations sans qu'elle engendre S_4.

5.4. Soit $t_1, \ldots, t_{n-1} \in S_n$ une famille *génératrice* de transpositions vérifiant les relations précédentes. Construire $\alpha \in S_n$ de sorte que $\alpha^{-1}t_i\alpha = \tau_i$ pour tout i. *Indication :* Toute transposition est caractérisée par son support ; analyser leur configuration.

5.5. Soit $\phi\colon S_n \to S_n$ un automorphisme. Si ϕ envoie transpositions sur transpositions, alors il existe une permutation σ telle que $\phi(\sigma) = \alpha^{-1}\sigma\alpha$ pour tout $\sigma \in S_n$.

6. Automorphismes intérieurs et extérieurs

6.1. Pour tout $a \in G$ on définit la conjugaison (à gauche) $\gamma_a : G \to G$ par $\gamma_a(x) = axa^{-1}$. Montrer que γ_a est un automorphisme, dit *automorphisme intérieur* de G.

6.2. Montrer que $\gamma : G \to \mathrm{Aut}(G)$ donné par $a \mapsto \gamma_a$ est un homomorphisme de groupe. Son image est le *groupe des automorphismes intérieurs*, noté $\mathrm{Inn}(G)$.

6.3. Le noyau de γ est exactement le centre de G. Conclure que $\mathrm{Inn}(G) \cong G/Z(G)$. Dans le cas des groupes symétriques, montrer que $Z(S_n) = \{\mathrm{id}\}$ pourvu que $n \geq 3$.

6.4. Le groupe $\mathrm{Inn}(G)$ est distingué dans $\mathrm{Aut}(G)$. Le quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ est appelé le groupe des *automorphismes extérieurs* de G.

Feuille G3 — CONJUGAISON DANS LES GROUPES SYMÉTRIQUES

Résumé. Dans un groupe non abélien l'action par conjugaison est un outil important, et aussi une structure intéressante en elle-même. On se propose ici d'expliciter les classes des conjugaison et les centralisateurs dans S_3, S_4, S_5, puis A_4, A_5. On en déduit en particulier la simplicité de A_5.

1. CONJUGAISON DANS S_3 ET S_4 ET S_5

1.1. Énumérer les classes de conjugaison dans S_3 : expliciter un représentant σ pour chacune puis déterminer le centralisateur $C_{S_3}(\sigma)$. Indiquer leur cardinaux $|\sigma^{S_3}|$ et $|C_{S_3}(\sigma)|$. Même exercice pour S_4, puis S_5. (Vérification par $|S_n| = |\sigma^{S_n}| \cdot |C_{S_n}(\sigma)|$ puis $\sum |\sigma^{S_n}| = |S_n|$.)

1.2. Regarder l'action de S_4 sur l'orbite $((12)(34))^{S_4}$. En déduire un homomorphisme de groupes $h\colon S_4 \to S_3$. Calculer $h(12), h(23), h(34)$. Est-il surjectif ? Quel est son noyau ?

2. CONJUGAISON DANS A_4 ET A_5

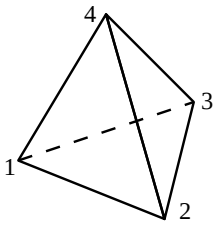
2.1. Après avoir compris la conjugaison dans S_n, passons au groupe alterné A_n. Vérifier d'abord que $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n = \ker(\operatorname{sign}\colon C_{S_n}(\sigma) \to \{\pm 1\})$. Deux cas se présentent :

(a) Si $C_{S_n}(\sigma)$ contient de permutations impaires, alors le centralisateur $C_{A_n}(\sigma) < C_{S_n}(\sigma)$ est d'indice 2, tandis que l'orbite $\sigma^{A_n} = \sigma^{S_n}$ reste la même.

(b) Si $C_{S_n}(\sigma)$ ne contient que des permutations paires, alors $C_{A_n}(\sigma) = C_{S_n}(\sigma)$ reste le même, tandis que l'orbite σ^{S_n} se décompose en deux : σ^{A_n} et $\sigma^{(12)A_n}$.

2.2. Expliciter les classes de conjugaison dans A_4 et A_5 et déterminer leurs cardinaux ; pour chacune entre elles choisir un représentant ; expliciter le centralisateur et son cardinal.

2.3. Soit T le groupe des isométries d'un tétraèdre et T^+ le sous-groupe des isométries directes. L'action sur les sommets induit un homomorphisme $h\colon T \to S_4$. Est-ce un isomorphisme ? Quelle est l'image de T^+ ?
On note $\rho_i^{\pm}$ la rotation d'angle $\pm\frac{2\pi}{3}$ autour de l'axe passant par le sommet i et le barycentre de la face opposée. Décomposer l'action de $\rho_i^{\pm}$ en cycles disjoints. Vérifier que les rotations $\rho_i^{\pm}$ forment *une seule* classe de conjugaison dans T, mais se décomposent en *deux* classes dans T^+, à savoir $\{\rho_i^+\}$ et $\{\rho_i^-\}$. L'interpréter géométriquement.



3. SIMPLICITÉ DE A_5

3.1. Rappeler la définition d'un groupe simple. Discuter les exemples suivants :

(a) Un groupe abélien est simple si et seulement s'il est d'ordre premier.

(b) Expliquer pourquoi S_2 est simple mais S_n ne l'est pas pour $n \geq 3$.

(c) Montrer que A_3 est simple, mais A_4 ne l'est pas.

3.2. Voici une preuve élémentaire que A_5 est simple : Supposons que $H \lhd A_5$. Si H contient x alors il contient tous les conjugués de x. En déduire que $|H| = 1 + a15 + b20 + c12 + d12$ avec $a, b, c, d \in \{0, 1\}$. Conclure que $|H| = 1$ ou $|H| = 60$.

3.3. Déduire de la simplicité que A_5 n'a pas de sous-groupes d'indice 2, 3 ou 4.

3.4. Montrer qu'il n'existe pas d'épimorphisme $S_5 \twoheadrightarrow S_4$, ni $S_5 \twoheadrightarrow S_3$. Et $S_5 \twoheadrightarrow S_2$?

4. PRODUIT DE DEUX SOUS-GROUPES

Pour aller plus loin et analyser des sous-groupes plus complexes, il nous faut des outils. Les notions suivantes nous servirons aussi plus tard quand nous discutons les produits semi-directs.

Notation. Soit G un groupe et $K, H < G$ deux sous-groupes. On pose $HK = \{hk \mid h \in H, k \in K\}$. C'est l'image de l'application $\mu\colon H \times K \to G$ donnée par la multiplication, $\mu(h, k) = hk$.

4.1. Si les ordres $|H|$ et $|K|$ sont premiers entre eux, alors $H \cap K = \{1\}$.
Si $H \cap K = \{1\}$, alors $|HK| = |H| \cdot |K|$. En général on a $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

On s'intéresse au sous-groupe engendré $\langle H, K\rangle$; c'est le plus petit groupe contenant H et K.

4.2. Vérifier que $\langle H, K\rangle$ est la réunion de $HK \subset HKH \subset HKHK \subset \dots$. Bien sûr, dans un groupe fini, cette construction se stabilise, donc $\langle H, K\rangle = (HK)^\ell$ pour un ℓ assez grand.

4.3. Cette construction par produits itérés est peu instructive. En particulier, H et K peuvent être petit, alors que $\langle H, K\rangle$ est grand. Pour en donner un exemple : soient $H = \langle(12)\rangle$ et $K = \langle(12\dots n)\rangle$. Identifier $\langle H, K\rangle$ et déterminer son ordre.

Dans le cas le plus sympathique on a $\langle H, K\rangle = HK$: ici les produits de la forme hk suffisent !

4.4. L'ensemble HK est un sous-groupe ssi $HK = KH$. Dans ce cas $\langle H, K\rangle = HK = KH$. Pour $H = \langle(12)\rangle$, $K = \langle(23)\rangle$ a-t-on $HK = KH$? Est-ce un groupe ? Identifier $\langle H, K\rangle$.

4.5. La condition $HK = KH$ peut être difficile à vérifier. Voici deux critères suffisants :

(a) Si $k^h = k$ pour tout $h \in H$ et $k \in K$, alors $KH = HK$, c'est donc un sous-groupe.

(b) Si $k^h \in K$ pour tout $h \in H$ et $k \in K$, alors $KH = HK$, c'est donc un sous-groupe.

Vérifier que la dernière condition équivaut à $K^h = K$ pour tout $h \in H$, ou encore $K^H = K$.

4.6. Donner un exemple où $KH = HK$ sans que $hk = kh$ pour tout $h \in H$ et $k \in K$.
Donner un exemple dans S_4 où $KH = HK$ sans que $K^H = K$ ni $H^K = H$.

5. Centralisateurs et classes de conjugaison dans S_6

5.1. Le centralisateur de (12) contient $K = \langle(12)\rangle$ et $H = S_{\{3,4,5,6\}}$.
Montrer que $\langle K, H\rangle = K \times H$. Quel est son ordre ?

5.2. Le centralisateur de $(12)(34)$ contient $K = \langle(12), (34)\rangle$ et $H = \langle(13)(24)\rangle$.
Montrer que $\langle K, H\rangle = KH$ et déterminer son ordre. Rajouter $S_{\{5,6\}}$.

5.3. Le centralisateur de $(12)(34)(56)$ contient $K = \langle(12), (34), (56)\rangle$ et $H = \langle(13)(24), (35)(46)\rangle$.
Vérifier que $K \cong \mathbb{Z}_2^3$ et que $H \cong S_3$. Montrer que $\langle K, H\rangle = KH$ et déterminer son ordre.

5.4. Compléter la liste pour les autres classes de conjugaison dans S_n. Pour chaque centralisateur $C(\sigma)$ on exhibera un « grand » sous-groupe, candidat à exhauster $C(\sigma)$ tout entier. En déduire une minoration pour chaque $|C(\sigma)|$, puis une majoration pour $|\sigma^{S_6}|$. En faisant la somme, arrive-t-on à prouver que notre énumération est exhaustive ?

Le cours vous fournit les outils pour le cas général : à $\sigma \in S_X$ on associe son *type* $t_\sigma \colon \mathbb{N}_+ \to \mathbb{N}$ où $t_\sigma(\ell)$ est le nombre des cycles de longueur ℓ sous l'action de $\langle\sigma\rangle$. Deux permutations σ, τ sont conjuguées dans S_X ssi $t_\sigma = t_\tau$. Le centralisateur $C_{S_X}(\sigma)$ est d'ordre $\prod_\ell \ \ell^{t_\sigma(\ell)} \cdot t_\sigma(\ell)!$; sa structure est celle décrite ci-dessus : $C_{S_X}(\sigma) = \prod_\ell K_\ell H_\ell$ avec $K_\ell \cong \mathbb{Z}_\ell^{t(\ell)}$ et $H_\ell \cong S_{t(\ell)}$.

6. Sous-groupes d'ordre p^k dans S_n

6.1. Dans S_9 soit $x = (123)$ et $u = (147)(258)(369)$. Calculer $y = uxu^{-1}$ et $z = u^{-1}xu$.

(a) Déterminer les ordres de u, x, y, z, puis les ordres de $H = \langle u\rangle$ et de $K = \langle x, y, z\rangle$.

(b) A-t-on $K^H = K$? Montrer que $G := KH$ est un groupe, et déterminer son cardinal.

(c) Vérifier que $G = \langle x, u\rangle$. Tout élément non trivial de G est-il d'ordre 3 ?

(d) Déterminer k maximal tel que 3^k divise $|S_9|$. Quelle est la particularité de G ?

6.2. (a) Décomposer en cycles la permutation $v \in S_{27}$, donnée par $v(i) = i + 9$ modulo 27.

(b) Déterminer l'ordre de $K^* = \langle G, G^v, G^{v^2}\rangle$ et $H^* = \langle v\rangle$, puis de $G^* = K^*H^*$.

(c) A-t-on $G^* = \langle x, u, v\rangle$? Quel est l'exposant de G^* ?

(d) Déterminer k^* maximal tel que 3^{k^*} divise $|S_{27}|$. Quelle est la particularité de G^* ?

6.3. Dans S_{52} construire un sous-groupe d'ordre 3^k avec k maximal.

6.4. ★ Si vous voulez, vous pouvez généraliser les exemples précédents :

(a) Pour un nombre premier $p \geq 2$, déterminer k maximal tel que p^k divise $|S_{p^e}|$.

(b) Construire, par récurrence, un sous-groupe G_e d'ordre p^k dans $|S_{p^e}|$.

(c) Formuler un énoncé pour p premier et S_n quelconque. Esquisser une construction.

Feuille G4 — GROUPES LINÉAIRES

Résumé. Les exercices de cette feuille on pour but de se familiariser avec quelques propriétés du groupe $\mathrm{GL}_n \mathbb{K}$ des matrices inversibles, de taille $n \times n$, à coefficients dans un corps (fini) $\mathbb{K}$. En particulier on essaiera d'identifier les plus petits membres de la famille $\mathrm{GL}_n \mathbb{F}_p$.

1. Espaces vectoriels sur $\mathbb{F}_p$

Pour $p \geq 2$ premier on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments.

1.1. Rappeler la définition d'un espace vectoriel E sur $\mathbb{F}_p$. Vérifier que le groupe abélien soujacent $(E, +)$ est d'exposant p, c'est-à-dire tout $x \in E$ vérifie $p \cdot x = 0$.

1.2. Réciproquement, tout groupe abélien $(E, +)$ d'exposant p est un espace vectoriel sur $\mathbb{F}_p$: vérifier que la multiplication $\mathbb{F}_p \times E \to E$, $(\bar{k}, x) \mapsto kx$ est bien définie et fait de E un espace vectoriel sur $\mathbb{F}_p$. En déduire un isomorphisme $E \cong \mathbb{Z}_p^n$ où $n = \dim_{\mathbb{F}_p}(E)$. Tout endomorphisme de $(E, +)$ est linéaire sur $\mathbb{F}_p$; en déduire que $\mathrm{Aut}(E, +) \cong \mathrm{GL}_n \mathbb{F}_p$.

1.3. Soit $\mathbb{K}$ un corps fini. Alors $\mathbb{F} = \langle 1 \rangle$ est un sous-corps d'ordre premier p, isomorphe à $\mathbb{F}_p$. En déduire que $\mathbb{K}$ est un espace vectoriel sur $\mathbb{F}_p$, donc $(\mathbb{K}, +) \cong (\mathbb{F}_p^n, +)$. En particulier tout corps fini est de cardinal p^n, avec p premier et $n \geq 1$. (On verra plus tard que pour p premier et $n \geq 1$ il existe effectivement un corps de cardinal p^n, et un seul à isomorphisme près !)

2. Cardinal des groupes $\mathrm{GL}_n \mathbb{F}_q$ et $\mathrm{SL}_n \mathbb{F}_q$

Dans ce paragraphe soit $\mathbb{F}_q$ un corps fini de cardinal $q = p^d$.

2.1. Le déterminant $\det : \mathrm{GL}_n \mathbb{F}_q \to \mathbb{F}_q^\times$ est un homomorphisme de groupes. Est-il surjectif ? Le noyau $\mathrm{SL}_n \mathbb{F}_q := \ker(\det)$ est un sous-groupe distingué. Quel est son indice ?

2.2. Soit E un espace vectoriel de dimension n sur $\mathbb{F}_q$. Quel est son cardinal ? Soient $v_1, \dots, v_k \in E$ linéairement indépendants. Quel est le cardinal de $\langle v_1, \dots, v_k \rangle < E$? Combien de vecteurs $v_{k+1} \in E$ existent-ils tels que $v_1, \dots, v_k, v_{k+1}$ soient linéairement dépendants ? indépendants ?

2.3. Combien de bases E admet-il ? *Indication :* choisir les éléments $v_1, \dots, v_n$ un par un. Expliciter une bijection entre les éléments de $\mathrm{GL}_n \mathbb{F}_q$ et les bases de $\mathbb{F}_q^n$. En déduire l'ordre du groupe $\mathrm{GL}_n \mathbb{F}_q$ et $\mathrm{SL}_n \mathbb{F}_q$.

2.4. Quelle est la puissance maximale de p divisant $|\mathrm{GL}_n \mathbb{F}_q|$? Montrer que $H = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$ est un sous-groupe de $\mathrm{GL}_n \mathbb{F}_q$. Quel est son cardinal ? Est-ce un p-Sylow ?

3. La coïncidence $\mathrm{GL}_2 \mathbb{F}_2 = \mathrm{SL}_2 \mathbb{F}_2 \cong S_3$

3.1. Vérifier que $\mathrm{GL}_2 \mathbb{F}_2$ et S_3 ont même cardinal. On essaiera de construire un isomorphisme :

(a) Rappeler l'action naturelle du groupe $G = \mathrm{GL}_2 \mathbb{F}_2$ sur l'espace vectoriel $E = \mathbb{F}_2^2$.

(b) Décomposer E en orbites. En déduire une action de G sur $E^* = E \smallsetminus \{0\}$.

(c) En déduire un homomorphisme $h \colon G \to S_{E^*}$. Est-ce un isomorphisme ?

Si vous voulez, énumérez les éléments de $\mathrm{GL}_2 \mathbb{F}_2$ et expliciter leur action sur E^*. En numérotant les éléments de E^*, vous pouvez ainsi expliciter un isomorphisme $G \xrightarrow{\sim} S_3$.

3.2. Plus généralement, on pourrait considérer l'action de $G = \mathrm{GL}_n \mathbb{F}_q$ sur $E = \mathbb{F}_q^n$.

(a) Quelles sont les orbites de E sous cette action ? Peut-on restreindre l'action à E^* ?

(b) Obtient-on donc un homomorphisme $h \colon G \to S_{E^*}$? Est-il injectif ?

(c) Pour quelles valeurs (n, q) l'homomorphisme h peut-il être surjectif ?

4. L'ESPACE PROJECTIF ET LE CENTRE DE $\mathrm{GL}_n\,\mathbb{K}$

Soit $\mathbb{K}$ un corps et E un espace vectoriel sur $\mathbb{K}$. Une *droite* est un sous-espace de dimension 1, donc de la forme $\langle v\rangle = \mathbb{K}v$ avec $v \in E^*$. On note $P(E)$ l'ensemble des droites dans E.

4.1. L'application $p\colon E^* \to P(E)$, $v \mapsto \langle v\rangle$ est une surjection. Les éléments qui paramètrent la droite $\langle v\rangle$ sont exactement ceux dans $\mathbb{K}^*v$: c'est l'orbite sous l'action du groupe $\mathbb{K}^*$.

4.2. Dans le cas de $E = \mathbb{K}^n$ on note la droite $\langle(x_1, \ldots, x_n)\rangle$ par $[x_1 : \ldots : x_n]$. Pour $E = \mathbb{F}_q^n$ déterminer le cardinal de E^* et de $P(E)$. Expliciter les éléments de l'ensemble $P(\mathbb{F}_q^2)$, appelé la *droite projective* sur $\mathbb{F}_q$.

4.3. Expliciter comment l'action de $\mathrm{GL}_n\,\mathbb{K}$ sur $\mathbb{K}^n$ induit une action sur $P = P(\mathbb{K}^n)$.
Une homothétie $\lambda\,\mathrm{id}$, avec $\lambda \in \mathbb{K}^\times$, fixe toutes les droites. Montrer la réciproque.
On a donc un homomorphisme naturel $\mathrm{P}\colon \mathrm{GL}_n\,\mathbb{K} \to S_P$ avec $\ker(\mathrm{P}) = \{\lambda\,\mathrm{id} \mid \lambda \in \mathbb{K}^\times\}$.

4.4. Montrer que $Z(\mathrm{GL}_n\,\mathbb{K}) = \{\lambda\,\mathrm{id} \mid \lambda \in \mathbb{K}^\times\}$. *Indication :* Vérifier d'abord l'inclusion évidente. Pour la réciproque, regarder $\phi \in \mathrm{GL}_n\,\mathbb{K}$ avec $\phi(v) = w \notin \langle v\rangle$. Dans ce cas il existe un $\alpha \in \mathrm{GL}_n\,\mathbb{K}$ avec $v \mapsto v$, $w \mapsto w + v$; calculer $\alpha\phi\alpha^{-1}(v)$; conclure que $\phi \notin Z$.

4.5. En déduire que $Z(\mathrm{SL}_n\,\mathbb{K}) = \{\lambda\,\mathrm{id} \mid \lambda \in \mathbb{K}^\times, \lambda^n = 1\}$.
Montrer que $|Z(\mathrm{SL}_n\,\mathbb{F}_q)| = \mathrm{pgcd}(n, q-1)$.

Ce qui précède motive la définition des *groupes projectifs* $\mathrm{PGL}_n := \mathrm{GL}_n\,/Z(\mathrm{GL}_n)$ et $\mathrm{PSL}_n := \mathrm{SL}_n\,/Z(\mathrm{SL}_n)$.
Leurs relations sont esquissées ci-contre.

$$\begin{array}{ccc} \mathrm{GL}_n\,\mathbb{K} & \xleftarrow{\text{inc}} & \mathrm{SL}_n\,\mathbb{K} \\ {\scriptstyle\text{proj}}\downarrow & & {\scriptstyle\text{proj}}\downarrow \\ \mathrm{PGL}_n\,\mathbb{K} & \xleftarrow{\text{inc}} & \mathrm{PSL}_n\,\mathbb{K} \end{array}$$

4.6. Vérifier que $|\,\mathrm{PGL}_n\,\mathbb{F}_p| = |\,\mathrm{SL}_n\,\mathbb{F}_p|$.
Attention : en général ces groupes sont non isomorphes !

4.7. Vérifier que $\mathrm{GL}_n\,\mathbb{F}_2 = \mathrm{SL}_n\,\mathbb{F}_2 = \mathrm{PSL}_n\,\mathbb{F}_2 = \mathrm{PGL}_n\,\mathbb{F}_2$.

4.8. Pour quelles valeurs (n, p) a-t-on $\mathrm{SL}_n\,\mathbb{F}_p = \mathrm{PSL}_n\,\mathbb{F}_p = \mathrm{PGL}_n\,\mathbb{F}_p$?

4.9. Énoncer le théorème du cours sur la simplicité de $\mathrm{PSL}_n\,\mathbb{F}_p$.

5. LA COÏNCIDENCE $S_4 \cong \mathrm{PGL}_2\,\mathbb{F}_3 \ncong \mathrm{SL}_2\,\mathbb{F}_3$

5.1. Déterminer l'ordre des groupes $\mathrm{GL}_2\,\mathbb{F}_3$, $\mathrm{SL}_2\,\mathbb{F}_3$, $\mathrm{PGL}_2\,\mathbb{F}_3$, $\mathrm{PSL}_2\,\mathbb{F}_3$; comparer avec S_4.

5.2. Montrer que $\mathrm{SL}_2\,\mathbb{F}_3 \ncong S_4$. *Indication :* comparer les centres.

5.3. On essaiera de construire un isomorphisme $\mathrm{PGL}_2\,\mathbb{F}_3 \xrightarrow{\sim} S_4$.

(a) On note P l'ensemble des droites dans $E = \mathbb{F}_3^2$. Les énumérer.

(b) En déduire un homomorphisme $h\colon \mathrm{GL}_2\,\mathbb{F}_3 \to S_4$. Quel est son noyau ? son image ?

(c) Conclure que $\mathrm{PGL}_2\,\mathbb{F}_3 \cong S_4$. A-t-on $\mathrm{PSL}_2\,\mathbb{F}_3 \cong A_4$? Est-ce un groupe simple ?

6. LA COÏNCIDENCE $S_5 \cong \mathrm{PGL}_2\,\mathbb{F}_5 \ncong \mathrm{SL}_2\,\mathbb{F}_5$

6.1. Déterminer l'ordre des groupes $\mathrm{GL}_2\,\mathbb{F}_5$, $\mathrm{SL}_2\,\mathbb{F}_5$, $\mathrm{PGL}_2\,\mathbb{F}_5$, $\mathrm{PSL}_2\,\mathbb{F}_5$; comparer avec S_5.

6.2. Montrer que $\mathrm{SL}_2\,\mathbb{F}_5 \ncong S_5$. *Indication :* comparer les centres.

6.3. (a) Vérifier que les matrices $I = \left(\begin{smallmatrix}0 & 4\\ 1 & 0\end{smallmatrix}\right)$, $J = \left(\begin{smallmatrix}2 & 0\\ 0 & 3\end{smallmatrix}\right)$, $K = \left(\begin{smallmatrix}0 & 2\\ 2 & 0\end{smallmatrix}\right)$ sont dans $\mathrm{SL}_2\,\mathbb{F}_5$, et qu'ils engendrent le sous-groupe $Q = \{\pm 1, \pm I, \pm J, \pm K\}$. Est-ce un 2-Sylow de $\mathrm{SL}_2\,\mathbb{F}_5$?

(b) Montrer que $H := Q/\{\pm 1\}$ est un 2-sous-groupe de Sylow dans $\mathrm{PSL}_2\,\mathbb{F}_5$.

(c) Vérifier que $\rho = \left[\begin{smallmatrix}1 & 1\\ 2 & 3\end{smallmatrix}\right] \in \mathrm{PSL}_2\,\mathbb{F}_5$ est d'ordre 3 et normalise H, c'est-à-dire $H^\rho = H$.

(d) Combien y a-t-il de sous-groupes conjugués H^α, avec $\alpha \in \mathrm{PSL}_2\,\mathbb{F}_5$?

(e) En déduire un homomorphisme $\mathrm{PSL}_2\,\mathbb{F}_5 \to S_5$. Quel est son noyau ? Son image ?

(f) ☆ Essayez d'en construire un isomorphisme $\mathrm{PGL}_2\,\mathbb{F}_5 \xrightarrow{\sim} S_5$.

6.4. L'action projective de $\mathrm{PGL}_2\,\mathbb{F}_5$ fait intervenir « l'anomalie » du groupe S_6 :

(a) On note P l'ensemble des droites dans $E = \mathbb{F}_5^2$. Les énumérer.

(b) En déduire un homomorphisme $h\colon\ \mathrm{PGL}_2\,\mathbb{F}_5 \to S_6$. Est-il injectif ?

(c) Décomposer $h\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ et $h\left[\begin{smallmatrix}0&4\\1&0\end{smallmatrix}\right]$ en cycles disjoints.
L'image de h est-elle conjuguée à S_5 ?

(d) ★ Existe-t-il un automorphisme de S_6 qui envoie l'image de h sur S_5 ?

7. La coïncidence $\mathrm{PSL}_2\,\mathbb{F}_7 \cong \mathrm{PSL}_3\,\mathbb{F}_2$

7.1. Déterminer le cardinal de $\mathrm{PSL}_2\,\mathbb{F}_7$ et de $\mathrm{PSL}_3\,\mathbb{F}_2$.

Afin de construire un ismorphisme, on considère l'action de $G = \mathrm{PSL}_2\,\mathbb{F}_7$ sur l'espace $E = \mathbb{F}_7^2$. Soit $P = P(E)$ l'ensemble des droites, numérotées par $n \mapsto [n:1]$ pour $n = 1, \dots, 7$, puis $8 \mapsto [1:0]$. Ainsi on identifie S_P à S_8. On admet que $\mathrm{PSL}_2\,\mathbb{F}_7$ est engendré par $\tau = \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ et $\sigma = \left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]$.

7.2. Donner la décomposition en cycles de τ et σ. On pose $\alpha := (1,3)(2,6)(4,5)(7,8)$. Donner la décomposition en cycles de $\beta := \alpha^\tau$ et $\gamma := \beta^\tau$. Vérifier également que $\gamma^\tau = \alpha\beta$.

7.3. Donner la décomposition en cycles de α^σ, β^σ, γ^σ et les identifier avec α, β, γ.

7.4. Les éléments α, β, γ commutent-ils ? Quel est l'ordre de $E = \langle \alpha, \beta, \gamma \rangle$? Est-ce un espace vectoriel ? A-t-on $E^\tau = E$? puis $E^\sigma = E$? En déduire que $G = \langle \tau, \sigma \rangle$ agit sur E.

7.5. Déterminer l'ordre de G et de $\mathrm{Aut}(E)$. L'action de G sur V par conjugaison induit un homomorphisme $G \to \mathrm{Aut}(E)$. Est-ce un isomorphisme ? Conclure que $\mathrm{PSL}_2\,\mathbb{F}_7 \cong \mathrm{PSL}_3\,\mathbb{F}_2$.

8. La coïncidence $\mathrm{SL}_2\,\mathbb{F}_4 = \mathrm{PSL}_2\,\mathbb{F}_4 = \mathrm{PGL}_2\,\mathbb{F}_4 \cong A_5$

8.1. Tout d'abord on veut montrer qu'il existe un corps de cardinal 4, et un seul à isomorphisme près. *Attention :* On distinguera soigneusement $\mathbb{F}_4$ et $\mathbb{Z}_4$. Le dernier n'est pas un corps !

(a) Le polynôme $X^2 + X + 1$ n'a pas de racine dans $\mathbb{F}_2$, il est donc irréductible dans $\mathbb{F}_2[X]$. Le quotient $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps de cardinal 4.

(b) Soit $\mathbb{K}$ est un corps de cardinal 4. Alors il contient $\mathbb{F}_2$ comme sous-corps. Soit $x \in \mathbb{K} \smallsetminus \mathbb{F}_2$ et $\phi\colon \mathbb{F}_2[X] \to \mathbb{K}$, $X \mapsto x$. Alors $\ker(\phi) = (X^2 + X + 1)$, donc $\mathbb{F}_4 \cong \mathbb{K}$.

8.2. Déterminer le cardinal de $\mathrm{GL}_2\,\mathbb{F}_4$, $\mathrm{SL}_2\,\mathbb{F}_4$, $\mathrm{PGL}_2\,\mathbb{F}_4$, $\mathrm{PSL}_2\,\mathbb{F}_4$; comparer avec A_5.

8.3. A-t-on $\mathrm{SL}_2\,\mathbb{F}_4 = \mathrm{PSL}_2\,\mathbb{F}_4 = \mathrm{PGL}_2\,\mathbb{F}_4$?

On essaiera de construire un isomorphisme avec A_5 :

8.4. On considère l'action $\mathrm{GL}_2\,\mathbb{F}_4$ sur $E = \mathbb{F}_4^2$. Déterminer le cardinal de $P(E)$. En déduire un homomorphisme $h\colon\ \mathrm{PSL}_2\,\mathbb{F}_4 \to S_5$. Est-il injectif ? Quelle est son image ?

9. L'exemple $\mathrm{PSL}_4\,\mathbb{F}_2 \ncong \mathrm{PSL}_3\,\mathbb{F}_4$

9.1. Déterminer l'ordre des groupes $\mathrm{PSL}_4\,\mathbb{F}_2$ et $\mathrm{PSL}_3\,\mathbb{F}_4$.

9.2. Vérifier que $G = \left\{ \left(\begin{smallmatrix}1&*&*&*\\0&1&*&*\\0&0&1&*\\0&0&0&1\end{smallmatrix}\right) \in \mathrm{PSL}_4\,\mathbb{F}_2 \right\}$ et $H = \left\{ \left(\begin{smallmatrix}1&*&*\\0&1&*\\0&0&1\end{smallmatrix}\right) \in \mathrm{PSL}_3\,\mathbb{F}_4 \right\}$ sont des 2-Sylow.

9.3. Montrer que $Z(G)$ est d'ordre 2 alors que $Z(H)$ est d'ordre 4.

9.4. En faisant appel au théorème de Sylow, montrer que $\mathrm{PSL}_4\,\mathbb{F}_2 \ncong \mathrm{PSL}_3\,\mathbb{F}_4$. *Remarque :* C'est le plus petit exemple de deux groupes simples qui soient de même ordre mais non isomorphes.

Feuille G5 — LE THÉORÈME DE SYLOW

Résumé. Rien qu'à partir de l'ordre $|G|$ le théorème de Sylow permet de déduire des informations précieuses sur la structure d'un groupe G. Cette feuille d'exercices en discute quelques applications.

1. LE THÉORÈME DE SYLOW

Dans la suite on se servira fréquemment du théorème de Sylow. Pour un groupe fini G et un nombre premier p on décompose $|G| = p^k q$ tel que $p \nmid q$. Un *p-sous-groupe de Sylow* de G est un sous-groupe $H < G$ d'ordre p^k. On note m_p le nombre de tels sous-groupes.

1.1. Énoncer le théorème de Sylow. Qu'obtient-on pour un groupe abélien fini ?

1.2. Un p-Sylow est distingué si et seulement si $m_p = 1$.

1.3. Pour un groupe d'ordre $p^a q^b$ quelles sont les valeurs possibles de (m_p, m_q) ?
Projet : Si vous voulez vous pouvez écrire un petit logiciel qui les énumère.

1.4. Tout groupe d'ordre 15 est cyclique. Il en est de même pour l'ordre 35.

1.5. Tout groupe d'ordre 1225 est abélien. Combien y en a-t-il à isomorphisme près ?

1.6. Rappeler l'ordre de $\mathrm{GL}_n \mathbb{F}_p$, puis expliciter un p-Sylow de $\mathrm{GL}_n \mathbb{F}_p$.

1.7. Esquisser comment construire un p-Sylow dans S_n, disons un 2-Sylow dans S_{10}.

2. APPLICATION AUX GROUPES SYMÉTRIQUES

Pour tout groupe fini G il existe un homomorphisme injectif $G \hookrightarrow S_G$ (rappeler la preuve). On peut donc ce demander quel est le plus petit n tel que $G \hookrightarrow S_n$. Certes, $n = |G|$ est toujours possible, mais c'est souvent beaucoup trop grand :

2.1. Regardons le groupe diédral D_4, d'ordre 8. Montrer que $D_4 \hookrightarrow S_4$ en exhibant un sous-groupe $H < S_4$ isomorphe à D_4. Est-ce que ce serait possible dans S_n avec $n < 4$?

2.2. Considérons le groupe des quaternions Q, également d'ordre 8. Rappeler pourquoi $Q \ncong D_4$.

(a) Reprenons notre sous-groupe $H < S_4$ isomorphe à D_4. Est-ce un 2-Sylow de S_4 ? de S_5 ? Existe-t-il un sous-groupe dans S_5 qui soit isomorphe à Q ?

(b) Expliciter un sous-groupe $K < S_6$ isomorphe à $D_4 \times \mathbb{Z}_2$. Est-ce un 2-Sylow de S_6 ? de S_7 ? Existe-t-il un sous-groupe dans S_7 qui soit isomorphe à Q ?

Quel est donc le n minimal tel que S_n contienne un sous-groupe isomorphe à Q ?

3. QUELQUES EXEMPLES DE CLASSIFICATION

En général l'ordre $|G|$ ne détermine pas le groupe G. Néanmoins l'ordre contient beaucoup d'information sur la structure possible. Les exercices suivants en présentent quelques exemples.

3.1. Supposons que $H, K < G$ sont deux sous-groupes tels que $K^H = K$. Dans ce cas on a une action $K \times H \to K$ par conjugaison $(k, h) \mapsto h^{-1}kh$. Elle induit un homomorphisme $\alpha\colon H \to \mathrm{Aut}(K)$. Il est trivial si et seulement si H et K commutent. Dans certains cas, α doit être trivial à cause des cardinaux : Montrer que tout homomorphisme $\mathbb{Z}_5 \to \mathrm{Aut}(\mathbb{Z}_{17})$ est trivial. De même pour $\mathbb{Z}_5 \to \mathrm{Aut}(\mathbb{Z}_3^2)$.

3.2. Déterminer, à isomorphisme près, tous les groupes d'ordre $45 = 3^2 \cdot 5$.

3.3. Déterminer, à isomorphisme près, tous les groupes d'ordre $665 = 5 \cdot 7 \cdot 19$.

3.4. Déterminer, à isomorphisme près, tous les groupes d'ordre $1105 = 5 \cdot 13 \cdot 17$.

3.5. Soit G un groupe d'ordre 30. Pour $p = 2, 3, 5$ on note H_p un p-groupe de Sylow.

(a) On a $m_5 \in \{1, 6\}$ et $m_3 \in \{1, 10\}$. Montrer que G contient $m_5 \cdot 4$ éléments d'ordre 5 et $m_3 \cdot 2$ éléments d'ordre 3. En déduire que $m_5 = 1$ ou $m_3 = 1$.

(b) $K = H_5 H_3$ est un sous-groupe d'ordre 15. Il est cyclique et distingué dans G.

(c) On en déduit que $G = K \rtimes H_2$. Pour l'action $H_2 \to \mathrm{Aut}(K)$ il y a quatre possibilités. Conclure que $G \cong \mathbb{Z}_{30}$ ou $G \cong D_{15}$ ou $G \cong D_5 \times \mathbb{Z}_3$ ou $G \cong \mathbb{Z}_5 \times D_3$.

3.6. Soit G un groupe d'ordre 255. Pour $p = 3, 5, 17$ on note H_p un p-Sylow de G.

(a) Montrer que H_{17} est distingué dans G, donc $K = H_{17}H_5$ est un sous-groupe.

(b) Analyser $K = H_{17} \rtimes H_5$. C'est en fait un produit direct, donc K est cyclique.

(c) Utiliser le fait que $K < N_G(H_5)$ pour montrer que $m_5 = |G : N_G(H_5)| \leq 3$.

(d) En déduire que $m_5 = 1$, donc H_5 aussi est distingué dans G.

(e) Conclure que $G = K \rtimes H_3$. C'est en fait un produit direct, donc G est cyclique.

3.7. Déterminer, à isomorphisme près, tous les groupes d'ordre $595 = 5 \cdot 7 \cdot 17$.

4. Le théorème pqr

Théorème 2. *Soit G un groupe fini dont l'ordre est composé de trois facteurs premiers. Alors G admet un sous-groupe distingué non trivial, c'est-à-dire $K \lhd G$ avec $1 \neq K \neq G$.*

Pour la preuve on suppose que $p > q > r$ sont trois nombres premiers distincts.

4.1. Pour $|G| = p^k$ rappeler que le centre est non trivial. Conclure.

4.2. Pour $|G| = p^k q$ on a $m_q \in \{1, p, p^2, \ldots, p^k\}$ et $m_p = 1$. Conclure.

4.3. Pour $|G| = pq^2$ on a $m_p \in \{1, q^2\}$ et $m_q \in \{1, p\}$.
Montrer par un comptage d'éléments que $m_p = q^2$ implique $m_q = 1$. Conclure.

4.4. Pour $|G| = pqr$ on a $m_p \in \{1, qr\}$ et $m_q \in \{1, p, pr\}$ et $m_r \in \{1, q, p, pq\}$.

(a) Montrer que $m_p(p-1) + m_q(q-1) + m_r(r-1) < pqr$.

(b) En déduire que $m_p = qr$ implique $m_q = 1$. Conclure.

Remarque : On reconnaît ci-dessus le début d'une classification des groupes dont l'ordre est composé de trois facteurs premiers, résultat dû à O. Hölder en 1893. À titre d'exemple nous avons déjà classifié les groupes d'ordre 30, 45, 255, 595, 665 et 1105 en §3.

4.5. Le théorème serait faux à partir de quatre facteurs premiers : donner un contre-exemple.

5. Groupes d'ordre < 60

Les groupes abéliens simples sont $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, \ldots$. Comme groupes non abéliens simples on connaît déjà les groupes alternés $A_5, A_6, A_7, \ldots$ et les groupes linéaires $\mathrm{PSL}_n \mathbb{F}_q$ ($n \geq 3$ ou $q \geq 4$). Parmi ces exemples, le plus petit groupe non abélien simple est $A_5 \cong \mathrm{PSL}_2 \mathbb{F}_4 \cong \mathrm{PSL}_2 \mathbb{F}_5$ d'ordre 60. On se propose ici de montrer que c'est effectivement le plus petit possible :

Théorème 3. *Il n'existe pas de groupe non abélien simple d'ordre < 60.*

5.1. Vérifier que le théorème 2 couvre tous les ordres < 60 sauf 24, 36, 40, 48, 56.

Dans la suite on traitera les cinq cas restants un par un.

5.2. Si $|G| = 40 = 5 \cdot 2^3$, alors $m_5 = 1$, donc G n'est pas simple.

5.3. Si $|G| = 56 = 7 \cdot 2^3$, alors $m_7 \in \{1, 8\}$. Montrer que $m_7 = 8$ implique $m_2 = 1$.

5.4. Pour les ordres 24, 36, 48 l'observation suivante s'avère utile :
Supposons que $P_1, P_2, \ldots, P_m$ avec $m > 1$ sont les p-Sylow de G.
Déduire du théorème de Sylow un homomorphisme non trivial $\phi : G \to S_m$.
Si G est simple, alors ϕ est injectif et $m! \geq |G|$, même $m! \geq 2|G|$.

5.5. Si $|G| = 24 = 3 \cdot 2^3$, alors $m_2 \in \{1, 3\}$. Mais $|G| > 3!$, donc G n'est pas simple.

5.6. Si $|G| = 48 = 3 \cdot 2^4$, alors $m_2 \in \{1, 3\}$. Mais $|G| > 3!$, donc G n'est pas simple.

5.7. Si $|G| = 36 = 3^2 \cdot 2^2$, alors $m_3 \in \{1, 4\}$. Mais $|G| > 4!$, donc G n'est pas simple.

CONTRÔLE CONTINU 2004/1 — GROUPES FINIS

Ni documents ni calculatrices ne sont autorisés.
Les paragraphes sont indépendants entre eux.
Justifiez vos réponses : brièvement mais suffisamment.

1. Le théorème de Sylow

1.1. Rappeler la définition d'un p-Sylow d'un groupe fini, et énoncer le théorème de Sylow.

1.2. En déduire qu'un p-Sylow est distingué si et seulement s'il est unique.

1.3. Déterminer tous les groupes d'ordre 5 et 7, puis d'ordre 35 à isomorphisme près.

1.4. Déterminer tous les groupes d'ordre $595 = 5 \cdot 7 \cdot 17$ à isomorphisme près.

2. Les 2-Sylow de S_5 et de $\mathrm{SL}_2 \mathbb{F}_5$

2.1. Déterminer l'ordre de S_5 et de $\mathrm{SL}_2 \mathbb{F}_5$.

2.2. Rappelons que le groupe diédral D_4 est le groupe des isométries d'un carré.
Expliciter un sous-groupe $H < S_5$ isomorphe à D_4. Est-ce un 2-Sylow de S_5 ?

2.3. Vérifier que les matrices $I = \left(\begin{smallmatrix} 0 & 4 \\ 1 & 0 \end{smallmatrix}\right)$, $J = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, $K = \left(\begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix}\right)$ sont dans $\mathrm{SL}_2 \mathbb{F}_5$ et qu'ils engendrent le sous-groupe $Q = \{\pm 1, \pm I, \pm J, \pm K\}$. Est-ce un 2-Sylow de $\mathrm{SL}_2 \mathbb{F}_5$?

2.4. Les groupes D_4 et Q sont-ils isomorphes ? Dans S_5 existe-t-il un sous-groupe isomorphe à Q ? Dans $\mathrm{SL}_2 \mathbb{F}_5$ existe-t-il un sous-groupe isomorphe à D_4 ? Les groupes S_5 et $\mathrm{SL}_2 \mathbb{F}_5$ sont-ils isomorphes ?

3. Groupes simples

3.1. Rappeler la définition d'un groupe simple. Caractériser les groupes abéliens simples.

3.2. Lesquels des groupes symétriques $S_2, S_3, S_4, S_5, \ldots$ sont simples ?
Lesquels des groupes alternés $A_3, A_4, A_5, \ldots$ sont simples ? Détailler le cas A_4.

3.3. Étant donné $H < G$, construire l'homomorphisme naturel $\alpha \colon G \to \mathrm{Sym}(G/H)$. En déduire, pour H d'indice $n > 1$, qu'il existe un homomorphisme non-trivial $G \to S_n$.

3.4. Pour $n \geq 5$, le groupe A_n admet-il des sous-groupes d'indice $2, 3, 4, \ldots, n$?

4. Le groupe $\mathrm{PSL}_2 \mathbb{F}_7$ ...

On rappelle que le groupe $\mathbb{F}_7^\times$ agit (à gauche) sur $\mathbb{F}_7^2 \smallsetminus \{0\}$ et que la *droite projective* du corps $\mathbb{F}_7$ est définie comme le quotient $P = \mathbb{F}_7^\times \backslash (\mathbb{F}_7^2 \smallsetminus \{0\}) = \mathbb{F}_7 \cup \{\infty\}$. On identifie $\mathrm{Sym}(P)$ à S_8 en notant $n = [\bar{n} : 1]$, pour $n = 1, \ldots, 7$, et $8 = [1 : 0]$. (Ici, par convention, S_8 agit à droite.) L'action à droite de $\mathrm{SL}_2 \mathbb{F}_7$ sur $\mathbb{F}_7^2$ induit une action à droite de $\mathrm{PSL}_2 \mathbb{F}_7$ sur P. Pour $M = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{SL}_2 \mathbb{F}_7$ on représente $\bar{M} = \{\pm M\} \in \mathrm{PSL}_2 \mathbb{F}_7$ par l'homographie $h_M \colon z \mapsto \frac{az+b}{cz+d}$, plus explicitement $h_M \colon [z_1 : z_2] \mapsto [az_1 + bz_2 : cz_1 + dz_2]$. On admet que $\mathrm{PSL}_2 \mathbb{F}_7$ est simple d'ordre 168 et engendré par $\tau \colon z \mapsto z + 1$ et $\sigma \colon z \mapsto -z^{-1}$.

4.1. On pose $\alpha := (1,3)(2,6)(4,5)(7,8)$.

(a) Donner la décomposition en cycles de τ et σ.

(b) Donner la décomposition en cycles de $\beta := \alpha^\tau$ et $\gamma := \beta^\tau$. Vérifier que $\gamma^\tau = \alpha\beta$.

(c) Donner la décomposition en cycles de α^σ, β^σ, γ^σ et les identifier avec α, β, γ.

Le groupe $G = \langle \tau, \sigma \rangle$ est-il inclus dans le normalisateur du groupe $V = \langle \alpha, \beta, \gamma \rangle$ dans S_8 ?

4.2. Les éléments α, β, γ commutent-ils ? Quel est l'ordre de V et que vaut son exposant ?

4.3. L'action de G sur V par conjugaison induit-elle un isomorphisme $G \xrightarrow{\sim} \mathrm{Aut}(V)$?

4.4. Qu'a-t-on démontré ? Énoncer le théorème qui aurait dû être le titre de ce paragraphe.

CORRIGÉ

Les réponses formulées ci-dessous sont un peu plus détaillées que strictement nécessaire ; des raccourcis ou des variantes sont possibles. Les points sont donnés à titre indicatif ; certaines questions sont peut-être encore sous-payées.

1. Le théorème de Sylow

1.1. ▶ Définition : Soit G un groupe d'ordre $p^k q$ où p est premier et $p \nmid q$. Un *p-sous-groupe de Sylow* ou *p-Sylow* de G est un sous-groupe $H < G$ d'ordre p^k. ▶▶ Théorème de Sylow : Pour tout groupe fini G et tout nombre premier p il existe au moins un p-Sylow H de G. Tout p-sous-groupe de G est contenu dans un p-Sylow de G. Tous les p-Sylow de G sont conjugués. Leur nombre $m_p = [G : N_G(H)]$ divise q et vérifie $m_p \equiv 1 \pmod p$.

1.2. ▶ Supposons que H est l'unique p-Sylow de G. La conjugaison par $g \in G$ envoie H sur le sous-groupe H^g, de même ordre. Donc H^g est un p-Sylow de G, et $H^g = H$ par l'hypothèse d'unicité. On conclut que H est distingué dans G. ▶ Réciproquement, supposons que $H \lhd G$ est un p-Sylow de G. Par le théorème de Sylow, pour tout p-Sylow K de G il existe $g \in G$ de sorte que $K = H^g$. On conclut que $K = H$ par l'hypothèse de normalité.

1.3. ▶ Un groupe d'ordre premier p est cyclique (par Lagrange) donc isomorphe à $\mathbb{Z}_p$ (via le théorème d'isomorphisme). ▶ Soit G un groupe d'ordre $35 = 5 \cdot 7$. Il existe alors un 5-Sylow H_5 et un 7-Sylow H_7 dans G. On a $m_5 = 1 + a5 \mid 7$ donc $m_5 = 1$, et $m_7 = 1 + b7 \mid 5$ donc $m_7 = 1$. On obtient ainsi $H_5 \lhd G$ cyclique d'ordre 5 et $H_7 \lhd G$ cyclique d'ordre 7. ▶ Par Lagrange on a $H_5 \cap H_7 = \{1\}$ et $H_5 H_7 = G$. On conclut que $G = H_5 \times H_7 \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$.

1.4. Soit G un groupe d'ordre $595 = 5 \cdot 7 \cdot 17$. Pour $p = 5, 7, 17$ on choisit un p-Sylow H_p et on note m_p le nombre de p-Sylow dans G. ▶ Par le théorème de Sylow on a $m_5 = 1 + k5$ et $m_5 \in \{1, 7, 17, 119\}$. Par conséquent $m_5 = 1$, et H_5 est distingué. ▶ D'autre part on trouve $m_7 \in \{1, 85\}$ et $m_{17} \in \{1, 35\}$, ce qui ne permet pas encore de conclure.

Voici une démarche possible : ▶ Comme H_5 est distingué, le produit $K = H_5 H_7$ est un sous-groupe d'ordre 35, et cyclique d'après l'exercice précédent. ▶ Le normalisateur de H_7 contient K, donc il a au moins 35 éléments. On a donc $m_7 = [G : N_G(H_7)] \in \{1, 17\}$. Par conséquent $m_7 = 1$, et H_7 est distingué. ▶ On en déduit que $K = H_5 H_7$, étant le produit de deux sous-groupes distingués, est lui aussi distingué dans G. Par conséquent $G = K \rtimes H_{17}$. ▶ La conjugaison de H_{17} sur K induit un homomorphisme $H_{17} \to \mathrm{Aut}(K) \cong \mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_7) \cong \mathbb{Z}_5^\times \times \mathbb{Z}_7^\times$. ▶ Un tel homomorphisme est forcément trivial, ce qui veut dire que K et H_{17} commutent. On conclut que $G = K \times H_{17} \cong \mathbb{Z}_{35} \times \mathbb{Z}_{17} \cong \mathbb{Z}_{595}$.

2. Les 2-Sylow de S_5 et de $\mathrm{SL}_2\,\mathbb{F}_5$

2.1. ▶ On trouve $|S_5| = 5! = 120$ et $|\mathrm{SL}_2\,\mathbb{F}_5| = (5^2 - 5^0)(5^2 - 5^1)/(5 - 1) = 120$.

2.2. ▶▶ On pourrait prendre $H = \langle (1234), (13) \rangle$. Ceci se vérifie sur un dessin, ou en constatant que $H = \langle (1234) \rangle \rtimes \langle (13) \rangle$. À noter aussi que $\langle (1234), (12) \rangle = S_4$ n'est pas le groupe cherché. ▶ Comme $|H| = 2^3$ et $|S_5| = 2^3 \cdot 15$ on a effectivement exhiber un 2-Sylow de S_5.

2.3. ▶ Les matrices sont toutes de déterminant 1, donc dans $\mathrm{SL}_2\,\mathbb{F}_5$. ▶ En dressant une table de multiplication comme ci-contre on retrouve les relations bien-connues du groupe des quaternions. ▶ En particulier, l'ensemble Q est stable par multiplication et un sous-groupe de $\mathrm{SL}_2\,\mathbb{F}_5$. ▶ Comme $|Q| = 2^3$ et $|\mathrm{SL}_2\,\mathbb{F}_5| = 2^3 \cdot 15$ on a effectivement exhiber un 2-Sylow de $\mathrm{SL}_2\,\mathbb{F}_5$.

$\cdot$	I	J	K
I	-1	K	$-J$
J	$-K$	-1	I
K	J	$-I$	-1

2.4. ▶ Non, les groupes D_4 et Q ne sont pas isomorphes : D_4 contient 2 éléments d'ordre 4 (et 5 éléments d'ordre 2), tandis que Q contient 6 éléments d'ordre 4 (et 1 élément d'ordre 2). ▶ Non, il n'existe pas de sous-groupe $K < S_5$ isomorphe à Q : un tel K, étant d'ordre 8, serait un 2-Sylow de S_5, donc conjugué à H. On aurait alors $Q \cong K \cong H \cong D_4$, ce qui est absurde. ▶ Pareil, il n'existe pas de sous-groupe $K < \mathrm{SL}_2\,\mathbb{F}_5$ isomorphe à D_4. ▶ On conclut que les groupes S_5 et $\mathrm{SL}_2\,\mathbb{F}_5$ ne sont pas isomorphes. (▶ On aurait pu remarquer aussi que le centre de S_5 est trivial, alors que le centre de $\mathrm{SL}_2\,\mathbb{F}_5$ est $\{1, -1\}$.)

3. GROUPES SIMPLES

3.1. ▶ Définition : Un groupe G est *simple* si $H \lhd G$ implique soit $H = \{1\}$ soit $H = G$. (En particulier on exclut le groupe trivial.) Montrons qu'un groupe abélien est simple si et seulement s'il est d'ordre premier. ▶ Évidemment si G est d'ordre premier, alors il est simple : par Lagrange les seuls sous-groupes sont $\{1\}$ et G. ▶ Réciproquement, supposons que G est abélien simple. Pour tout $x \neq 1$ le sous-groupe $\langle x\rangle$ est non-trivial et distingué, donc $G = \langle x\rangle$. ▶ Si $\mathrm{ord}(x) = \infty$, alors $\{1\} \neq \langle x^2\rangle \neq G$, se qui est impossible. ▶ L'ordre est donc fini : $\mathrm{ord}(x) = pq$ avec un nombre premier $p \geq 2$. L'élément x^q est d'ordre p, donc non-trivial et générateur de G. On conclut que $|G| = p$.

3.2. ▶ Le groupe S_2 est d'ordre 2 donc simple. Pour $n \geq 3$ le groupe S_n contient le sous-groupe $A_n = \ker(\mathrm{sign})$ qui est distingué et différent de $\{1\}$ et S_n, donc S_n n'est pas simple. ▶ Le groupe A_3 est d'ordre 3 donc simple. Les groupes A_n sont simples pour $n \geq 5$ d'après le résultat du cours. ▶ Le groupe A_4, d'ordre 12, n'est pas simple car il contient le groupe de Klein, $V = \langle (12)(34), (13)(24)\rangle$, qui est distingué d'ordre 4.

3.3. ▶ Étant donné $H < G$ on considère $G/H = \{aH \mid a \in G\}$. Le groupe G agit à gauche sur G/H par $g \cdot (aH) = (ga)H$. L'homomorphisme naturel $\alpha\colon G \to \mathrm{Sym}(G/H)$ est donc donné par $\alpha(g)(aH) = (ga)H$. ▶ Si H est d'indice n, on peut numéroter les H-classes à droite par $1, \ldots, n$ et identifier $\mathrm{Sym}(G/H)$ à S_n. Comme G agit transitivement sur les H-classes, l'homomorphisme $G \to S_n$ est non-trivial (pourvu que $n \geq 2$ bien sûr).

3.4. ▶ Un sous-groupe $H < A_n$ d'indice $k \geq 2$ donne lieu à un homomorphisme non-trivial $\alpha\colon A_n \to S_k$, donc $\ker(\alpha) \neq A_n$. ▶ Comme A_n est simple, on a $\ker(\alpha) = \{1\}$, donc α est injectif. ▶ Par conséquent l'ordre $|A_n| = \frac{1}{2}n!$ est plus petit que l'ordre $|S_k| = k!$, ce qui équivaut à $k \geq n$. On conclut que A_n ne peut avoir de sous-groupe d'indice $k = 2, \ldots, n-1$. ▶ Bien sûr il existe un sous-groupe d'indice n, par exemple le stabilisateur du point n, qui est simplement une copie de A_{n-1} dans A_n.

4. LE GROUPE $\mathrm{PSL}_2\,\mathbb{F}_7$ EST ISOMORPHE À $\mathrm{GL}_3\,\mathbb{F}_2$.

4.1. (a) ▶ On trouve $\tau = (1234567)$ et $\sigma = (16)(23)(45)(78)$.

(b) ▶ On calcule d'abord $\beta := \alpha^\tau = (24)(37)(56)(18)$ puis $\gamma := \beta^\tau = (35)(41)(67)(28)$.
▶ Effectivement $\gamma^\tau = (46)(52)(71)(38)$ coïncide avec $\alpha\beta = (17)(25)(38)(46)$.

(c) ▶ On vérifie que $\alpha^\sigma = \alpha$ ainsi que $\beta^\sigma = \gamma$ et $\gamma^\sigma = \beta$.

▶ D'après (b), la conjugaison par τ envoie V sur $V^\tau = \langle \alpha^\tau, \beta^\tau, \gamma^\tau\rangle = \langle \beta, \gamma, \alpha\beta\rangle = V$. D'après (c), la conjugaison par σ envoie V sur $V^\sigma = \langle \alpha^\sigma, \beta^\sigma, \gamma^\sigma\rangle = \langle \alpha, \gamma, \beta\rangle = V$. ▶ On conclut que le groupe $G = \langle \tau, \sigma\rangle$ normalise V.

4.2. ▶ On vérifie, par un calcul direct, que $\alpha^\beta = \alpha$ ainsi que $\alpha^\gamma = \alpha$ et $\beta^\gamma = \beta$. (On peut vérifier la première égalité et déduire les deux autres de la question 4.1b). ▶ Comme $\alpha \neq \beta$ sont deux éléments commutant d'ordre 2, on voit que $\langle \alpha, \beta\rangle = \langle \alpha\rangle \times \langle \beta\rangle$ est d'ordre 4. ▶ Comme $\gamma \notin \langle \alpha, \beta\rangle$ on conclut que $V = \langle \alpha, \beta, \gamma\rangle = \langle \alpha\rangle \times \langle \beta\rangle \times \langle \gamma\rangle$ est un groupe d'ordre 8. ▶ Son exposant vaut 2. (C'est en fait un espace vectoriel sur $\mathbb{F}_2$ ayant pour base α, β, γ.)

4.3. Comme G normalise V, la conjugaison définit une action de G sur V. ▶ L'homomorphisme $\alpha\colon G \to \mathrm{Aut}(V)$ ainsi obtenu est non-trivial d'après la question 4.1, donc $\ker(\alpha) \neq G$. Comme G est simple, on a $\ker(\alpha) = \{1\}$, donc α est injectif. ▶ D'après la question 4.2, V est un espace vectoriel de dimension 3 sur $\mathbb{F}_2$. ▶ On peut alors identifier V à $\mathbb{F}_2^3$, et $\mathrm{Aut}(V)$ à $\mathrm{GL}_3\,\mathbb{F}_2$ d'ordre $7 \cdot 6 \cdot 4 = 168$. ▶ On conclut que α est un isomorphisme.

4.4. ▶ On vient de construire un isomorphisme entre $G = \mathrm{PSL}_2\,\mathbb{F}_7$ et $\mathrm{Aut}(V) \cong \mathrm{GL}_3\,\mathbb{F}_2$, d'où le titre, un peu plus parlant, de ce paragraphe.

Commentaires : Soulignons qu'ici tout est explicite : le choix de la base α, β, γ de V induit un isomorphisme $\mathbb{F}_2^3 \xrightarrow{\sim} V$. Ceci permet d'expliciter notre isomorphisme $\phi\colon \mathrm{PSL}_2\,\mathbb{F}_7 \xrightarrow{\sim} \mathrm{GL}_3\,\mathbb{F}_2$ qui est donné sur les générateurs par $\phi\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$ et $\phi\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. Remarquons aussi que, étant données de telles matrices $\tau', \sigma' \in \mathrm{GL}_3\,\mathbb{F}_2$, il est loin d'être trivial de vérifier que l'application $\tau \mapsto \tau'$ et $\sigma \mapsto \sigma'$ se prolonge en un homomorphisme $\mathrm{PSL}_2\,\mathbb{F}_7 \to \mathrm{GL}_3\,\mathbb{F}_2$. L'approche ci-dessus résout ce problème de manière constructive.

CONTRÔLE CONTINU 2005/1— GROUPES FINIS

1. GROUPES SYMÉTRIQUES ET ALTERNÉS

1.1. Pour $\sigma = (1,2)(3,4)(5,6)(7,8,9)(10,11,12)$, quel est le cardinal de la classe de conjugaison de σ dans S_{13} et du centralisateur de σ dans S_{13} ? Expliciter (sans justification) une famille génératrice du centralisateur.

1.2. Prouver qu'un sous-groupe $H < G$ d'indice 2 d'un groupe G contient le sous-groupe dérivé $G' = [G,G] = \langle\, [a,b] \mid a,b \in G \,\rangle$. En déduire les sous-groupes d'indice 2 de S_{13}.

2. GROUPES SIMPLES

2.1. Rappeler la définition d'un groupe simple.
Caractériser les groupes abéliens simples.

2.2. Lesquels des groupes symétriques $S_2, S_3, S_4, S_5, \ldots$ sont simples ?
Lesquels des groupes alternés $A_3, A_4, A_5, \ldots$ sont simples ?
Lesquels des groupes linéaires $\mathrm{PSL}_n \mathbb{F}_q$ sont simples ?

3. LE THÉORÈME DE SYLOW

3.1. Rappeler la définition d'un p-Sylow d'un groupe fini G. Énoncer le théorème de Sylow.

3.2. En déduire qu'un p-Sylow de G est distingué si et seulement s'il est l'unique p-Sylow de G.

3.3. Déterminer tous les groupes d'ordre 7777 à isomorphisme près.

3.4. Montrer qu'un groupe d'ordre 105 ne peut être simple.

4. LES 2-SYLOW DE $\mathrm{PSL}_3 \mathbb{F}_4$ ET DE A_8

4.1. Soit $\mathbb{F}_4$ un corps de cardinal 4. Déterminer l'ordre de $\mathrm{GL}_3 \mathbb{F}_4$, puis de $\mathrm{SL}_3 \mathbb{F}_4$ et de $\mathrm{PSL}_3 \mathbb{F}_4$. Est-ce que $\mathrm{PSL}_3 \mathbb{F}_4$ et A_8 ont même cardinal ?

Les exercices suivants ont pour but d'étudier la possibilité d'un isomorphisme entre $\mathrm{PSL}_3 \mathbb{F}_4$ et A_8. On rappelle que si x, y sont deux éléments d'un groupe G, le conjugué de x par y est $x^y = y^{-1}xy$.

4.2. On se propose d'expliciter un 2-Sylow de $\mathrm{SL}_3 \mathbb{F}_4$.

(a) Prouver que $T = \left\{ \left(\begin{smallmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid a,b,c \in \mathbb{F}_4 \right\}$ est un sous-groupe de $\mathrm{SL}_3 \mathbb{F}_4$.
Ce sous-groupe T est-il un 2-Sylow de $\mathrm{SL}_3 \mathbb{F}_4$?

(b) Pour $a,b,c \in \mathbb{F}_4$ on pose $\alpha_a = \left(\begin{smallmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ et $\beta_b = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right)$ et $\gamma_c = \left(\begin{smallmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Calculer $\alpha_a\gamma_c$ et $\gamma_c\alpha_a$, puis $\beta_b\gamma_c$ et $\gamma_c\beta_b$, ainsi que le commutateur $[\alpha_a, \beta_b] = \alpha_a^{-1}\beta_b^{-1}\alpha_a\beta_b$.

(c) Établir que tout $t \in T$ admet une écriture unique de la forme $t = \alpha_a\beta_b\gamma_c$ avec $a,b,c \in \mathbb{F}_4$.
Déterminer le centre $Z(T)$ du groupe T et vérifier qu'il est d'ordre 4.

4.3. On se propose d'expliciter un 2-Sylow de A_8. Dans le groupe symétrique S_8 on considère les permutations $a = (1,2)(3,4)$, $b = (5,6)(7,8)$, $c = (3,4)(5,6)$, $f = (1,3)(2,4)$, $g = (5,7)(6,8)$ et $h = (1,5)(2,6)(3,7)(4,8)$.

(a) Prouver que les éléments a, b, c, f, g, h sont dans le groupe alterné A_8.

(b) Prouver que le sous-groupe $E = \langle a,b,c \rangle$ engendré par a,b,c est commutatif et que tous ses éléments non triviaux sont d'ordre 2.

(c) Calculer les conjugués $a^f, b^f, c^f, a^g, b^g, c^g, f^g, g^f, a^h, b^h, c^h, f^h, g^h$. En déduire que E est un sous-groupe distingué de chacun des sous-groupes $F = \langle a,b,c,f \rangle$, $G = \langle a,b,c,f,g \rangle$ et $H = \langle a,b,c,f,g,h \rangle$ de A_8, et que G est distingué dans H.

(d) Déterminer les ordres des groupes E, F, G et H. En déduire que H est un 2-Sylow de A_8.

(e) Montrer que le centre de H est le groupe d'ordre 2 engendré par $ab = (1,2)(3,4)(5,6)(7,8)$.

4.4. Les groupes $\mathrm{PSL}_3\,\mathbb{F}_4$ et A_8 sont-ils isomorphes ?

CORRIGÉ

1. GROUPES SYMÉTRIQUES ET ALTERNÉS

1.1. Le centralisateur de $\sigma = (1,2)(3,4)(5,6)(7,8,9)(10,11,12)$ dans S_{13} est d'ordre $2^3 3! \cdot 3^2 2! = 1728$, la classe de conjugaison a donc $\frac{13!}{2^3 3! \cdot 3^2 2!} = 3603600$ éléments. Les cycles $a = (1,2)$, $b = (3,4)$, $c = (5,6)$, $d = (7,8,9)$, $e = (10,11,12)$ commutent entre eux et avec $\sigma = abcde$: il s'agit de la décomposition de σ en cycles disjoints. On voit aussi que $f = (1,3)(2,4)$ et $g = (3,5)(4,6)$ commutent avec les 3-cycles d, e et permutent les 2-cycles entre eux : $a^f = b$, $b^f = a$, $c^f = c$ ainsi que $a^g = a$, $b^g = c$, $c^g = b$. En particulier $\sigma^f = \sigma^g = \sigma$. De manière analogue, $h = (7,10)(8,11)(9,12)$ commute avec les 2-cycles a, b, c et permute les 3-cycles entre eux : $d^h = e$, $e^h = d$. En particulier $\sigma^h = \sigma$. Le centralisateur de σ contient donc le sous-groupe $\langle a,b,c,d,e,f,g,h\rangle = \langle a,d,f,g,h\rangle$.

Pour information : les éléments a,b,c,d,e,f,g,h engendrent effectivement tout le centralisateur. On peut vérifier que $\langle a,b,c,d,e,f,g,h\rangle = (\langle a,b,c\rangle \rtimes \langle f,g\rangle) \times (\langle d,e\rangle \rtimes \langle h\rangle)$ avec $\langle a,b,c\rangle \cong \mathbb{Z}_2^3$ d'ordre 2^3 et $\langle f,g\rangle \cong S_3$ d'ordre 3!, ainsi que $\langle d,e\rangle \cong \mathbb{Z}_3^2$ d'ordre 3^2 et $\langle h\rangle \cong S_2$ d'ordre 2!. Le sous-groupe engendré par a,b,c,d,e,f,g,h est donc d'ordre $2^3 3! \cdot 3^2 2!$ comme souhaité.

1.2. Un sous-groupe $H < G$ d'indice 2 est distingué ; le quotient G/H est donc un groupe et la projection canonique $p\colon G \to G/H$ un homomorphisme de groupes. Le groupe G/H, étant d'ordre 2, est isomorphe à $\mathbb{Z}_2$. En particulier G/H est abélien, et $H = \ker(p)$ contient $G' = [G,G]$. *Application :* Un sous-groupe H d'indice 2 dans S_{13} contient le groupe commutateur : d'après le cours on a $S'_{13} = A_{13}$, qui est lui-même d'indice 2. On conclut que $H = A_{13}$ est le seul sous-groupe d'indice 2 dans S_{13}. (Cet argument a lieu dans tout groupe symétrique S_n.) *Variante :* si H est d'indice 2 dans S_{13}, alors $p\colon S_{13} \twoheadrightarrow S_{13}/H$ est une surjection sur un groupe d'ordre 2, donc isomorphe à $\{\pm 1\}$. D'autre part la signature est le seul épimorphisme $S_{13} \twoheadrightarrow \{\pm 1\}$. On conclut que $\ker(p) = \ker(\mathrm{sign}) = A_{13}$.

2. GROUPES SIMPLES

2.1. *Définition :* Un groupe G est *simple* si $H \lhd G$ implique soit $H = \{1\}$ soit $H = G$. (En particulier le groupe trivial n'est pas simple.) Montrons qu'un groupe abélien est simple si et seulement s'il est d'ordre premier. Évidemment si G est d'ordre premier, alors il est simple : par Lagrange les seuls sous-groupes sont $\{1\}$ et G. Réciproquement, supposons que G est abélien simple. Soit $x \neq 1$. L'ordre de x est forcément fini : si $\mathrm{ord}(x) = \infty$, alors $\{1\} \subsetneq \langle x^2\rangle \subsetneq \langle x\rangle \subseteq G$, et G ne serait pas simple. On peut même supposer x d'ordre premier. (Si $\mathrm{ord}(x) = pq$ avec un nombre premier $p \geq 2$, alors x^q est d'ordre p.) Le sous-groupe $\langle x\rangle$ est non trivial et distingué, donc $G = \langle x\rangle$ est cyclique d'ordre p.

2.2. Le groupe S_2 est d'ordre 2 donc abélien simple. Pour $n \geq 3$ le groupe S_n n'est pas simple, car $A_n = \ker(\mathrm{sign})$ est un sous-groupe distingué propre. Le groupe A_3 est d'ordre 3 donc abélien simple. Les groupes A_n sont simples pour $n \geq 5$ d'après le résultat du cours. Le groupe A_4, d'ordre 12, n'est pas simple car il contient le groupe de Klein, $V = \langle (12)(34), (13)(24)\rangle$, qui est distingué d'ordre 4. Les groupes $\mathrm{PSL}_n \mathbb{F}_q$ sont simples pour tout $n \geq 2$ et tout $q = p^d$ (avec p premier et $d \geq 1$) avec deux exceptions : Ne sont pas simples $\mathrm{PSL}_2 \mathbb{F}_2 \cong S_3$ d'ordre 6, et $\mathrm{PSL}_2 \mathbb{F}_3 \cong A_4$ d'ordre 12.

3. LE THÉORÈME DE SYLOW

3.1. *Définition :* Soit G un groupe d'ordre $p^k q$ où p est premier et $p \nmid q$. Un *p-sous-groupe de Sylow* ou *p-Sylow* de G est un sous-groupe $H < G$ d'ordre p^k. *Théorème de Sylow :* Pour tout groupe fini G et tout nombre premier p il existe au moins un p-Sylow H de G. Tout p-sous-groupe de G est contenu dans un p-Sylow de G. Tous les p-Sylow de G sont conjugués. Leur nombre $m_p = [G : N_G(H)]$ divise q et vérifie $m_p \equiv 1 \pmod p$.

3.2. Supposons que H est l'unique p-Sylow de G. La conjugaison par $g \in G$ envoie H sur le sous-groupe H^g, de même ordre. Donc H^g est un p-Sylow de G, et $H^g = H$ par l'hypothèse d'unicité. Réciproquement, supposons que $H \lhd G$ est un p-Sylow de G. Par le théorème de Sylow, pour tout p-Sylow K de G il existe $g \in G$ de sorte que $K = H^g$. On conclut que $K = H$ par l'hypothèse de normalité.

3.3. On a la décomposition $7777 = 7 \cdot 11 \cdot 101$. D'après le théorème de Sylow il existe exactement un 7-Sylow A ($\cong \mathbb{Z}_7$), exactement un 11-Sylow B ($\cong \mathbb{Z}_{11}$), et exactement un 101-Sylow C ($\cong \mathbb{Z}_{101}$) dans G, et chacun de ces sous-groupes est distingué. En particulier on a $\langle A,B\rangle = AB$ car $A^B = A$ et $B^A = B$, même $\langle A,B\rangle = A \times B$ car $A \cap B = \{1\}$ et $[A,B] = \{1\}$. (Pour rappel : tout élément de AB s'écrit de manière unique comme ab avec $a \in A$ et $b \in B$. Si de plus $A^B = A$ et $B^A = B$, alors

$a^{b^{-1}}b = ba = ab^a$, donc $a^{b^{-1}} = a$ et $b = b^a$ par unicité.) En répétant le même raisonnement avec $A \times B$ et C on obtient $G = A \times B \times C$, donc $G \cong \mathbb{Z}_{7777}$ par le théorème des restes chinois.

3.4. Soit G un groupe d'ordre $105 = 3 \cdot 5 \cdot 7$. Pour le nombre m_p des p-Sylow on obtient $m_3 \in \{1, 7\}$, $m_5 \in \{1, 21\}$ et $m_7 \in \{1, 15\}$. Si aucun entre eux valait 1, alors on aurait $7 \cdot 2 = 14$ éléments d'ordre 3, puis $21 \cdot 4 = 84$ éléments d'ordre 5, et $15 \cdot 6 = 90$ éléments d'ordre 7, au total plus que 105 éléments dans G, ce qui est absurde. Alors $m_3 = 1$ ou $m_5 = 1$ ou $m_7 = 1$; mais dans ce cas G admet un sous-groupe distingué propre, donc G n'est pas simple. *Pour information :* Il y a seulement deux groupes d'ordre 105 à isomorphisme près, à savoir $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{105}$ et $\mathbb{Z}_5 \times (\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$.

4. Les 2-Sylow de $\mathrm{PSL}_3\,\mathbb{F}_4$ et de A_8

4.1. On a $|\,\mathrm{GL}_3\,\mathbb{F}_4| = (4^3-4^0)(4^3-4^1)(4^3-4^2) = 2^6 \cdot 3^4 \cdot 5 \cdot 7 = 181440$ donc $|\,\mathrm{SL}_3\,\mathbb{F}_4| = 2^6 \cdot 3^3 \cdot 5 \cdot 7 = 60480$ puis $|\,\mathrm{SL}_3\,\mathbb{F}_4| = 2^6 \cdot 3^2 \cdot 5 \cdot 7 = 20160$. Effectivement $|\,\mathrm{SL}_3\,\mathbb{F}_4| = |A_8| = \frac{1}{2}8!$.

4.2. (a) Évidemment T contient l'identité $\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right)$, les produits $\left(\begin{smallmatrix}1&a&c\\0&1&b\\0&0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&a'&c'\\0&1&b'\\0&0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&a+a'&c+c'+ab'\\0&1&b+b'\\0&0&1\end{smallmatrix}\right)$ et (forcément) aussi les inverses $\left(\begin{smallmatrix}1&a&c\\0&1&b\\0&0&1\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}1&-a&-c+ab\\0&1&-b\\0&0&1\end{smallmatrix}\right)$. C'est donc un sous-groupe $\mathrm{GL}_3\,\mathbb{F}_4$, même de $\mathrm{SL}_3\,\mathbb{F}_4$. L'ordre de T étant $4^3 = 2^6$, c'est bien un 2-sous-groupe de Sylow de $\mathrm{SL}_3\,\mathbb{F}_4$.

(b) On trouve $\alpha_a\gamma_c = \gamma_c\alpha_a = \left(\begin{smallmatrix}1&a&c\\0&1&0\\0&0&1\end{smallmatrix}\right)$ et $\beta_b\gamma_c = \gamma_c\beta_b = \left(\begin{smallmatrix}1&0&c\\0&1&b\\0&0&1\end{smallmatrix}\right)$, ainsi que $[\alpha_a, \beta_b] = \left(\begin{smallmatrix}1&0&ab\\0&1&0\\0&0&1\end{smallmatrix}\right)$. Autrement dit γ_c commute avec α_a et β_b, tandis que α_a et β_b commutent ssi $a = 0$ ou $b = 0$.

(c) On a $\alpha_a\beta_b\gamma_c = \left(\begin{smallmatrix}1&a&ab+c\\0&1&b\\0&0&1\end{smallmatrix}\right)$, donc $t = \left(\begin{smallmatrix}1&a&c\\0&1&b\\0&0&1\end{smallmatrix}\right)$ s'écrit comme $t = \alpha_a\beta_b\gamma_{c-ab}$ et cette écriture est unique. Supposons que $z = \alpha_a\beta_b\gamma_c$ est dans le centre de T. En particulier z commute avec α_1, donc $\alpha_a\beta_b\gamma_c = (\alpha_a\beta_b\gamma_c)^{\alpha_1} = \alpha_a\beta_b^{\alpha_1}\gamma_c$. Mais ceci implique que β_b commute avec α_1, donc $b = 0$. De même, z commute avec β_1, donc $\alpha_a\beta_b\gamma_c = (\alpha_a\beta_b\gamma_c)^{\beta_1} = \alpha_a^{\beta_1}\beta_b\gamma_c$, donc $a = 0$. Par conséquent les éléments du centre sont nécessairement de la forme γ_c. Réciproquement tout γ_c est dans le centre, car il commute avec tout élément $\alpha_{a'}\beta_{b'}\gamma_{c'}$. On conclut que le centre $Z(T) = \left\{\left(\begin{smallmatrix}1&0&c\\0&1&0\\0&0&1\end{smallmatrix}\right) \mid c \in \mathbb{F}_4\right\}$ est d'ordre 4. (On remarque plus précisément que $(Z(T), \cdot) \cong (\mathbb{F}_4, +) \cong \mathbb{Z}_2^2$.)

4.3. (a) Les permutations $a = (1,2)(3,4)$, $b = (5,6)(7,8)$, $c = (3,4)(5,6)$, $f = (1,3)(2,4)$, $g = (5,7)(6,8)$ et $h = (1,5)(2,6)(3,7)(4,8)$ sont chacun un produit de deux ou quatre transpositions, donc de signature $+1$. Autrement dit, $a, b, c, f, g, h \in A_8$.

(b) On voit que a et b sont à support disjoint, en particulier ils commutent. On vérifie que $a^c = c$ et $b^c = b$, donc a, b, c commutent entre eux. Tout élément de $E = \langle a, b, c\rangle$ est donc de la forme $e = a^\alpha b^\beta c^\gamma$ avec $\alpha, \beta, \gamma \in \{0, 1\}$, et vérifie $e^2 = a^{2\alpha}b^{2\beta}c^{2\gamma} = \mathrm{id}$.

(c) On trouve $a^f = a$, $b^f = b$, $c^f = ac$, $a^g = a$, $b^g = b$, $c^g = bc$, $f^g = f$, $g^f = g$, $a^h = b$, $b^h = a$, $c^h = abc$, $f^h = g$, $g^h = f$. Ainsi $E = \langle a, b, c\rangle$ est normalisé par chacun des éléments a, b, c, f, g, h c'est-à-dire que $E^a = E^b = E^c = E^f = E^g = E^h = E$. On conclut que E est distingué dans $F = \langle E, f\rangle$, $G = \langle E, f, g\rangle$ et $H = \langle E, f, g, h\rangle$. Pour la même raison on a $G^h = G$, donc $G \lhd H$.

(d) On a $\langle a, b\rangle = \langle a\rangle \times \langle b\rangle$, produit direct d'ordre 4 car a et b sont à support disjoint. Comme $c \notin \{\mathrm{id}, a, b, ab\}$, on a $\langle a, b, c\rangle = \langle a\rangle \times \langle b\rangle \times \langle c\rangle$ d'ordre 8 (isomorphe à $\mathbb{Z}_2^3$). Pour la même raison on voit que $\langle f, g\rangle = \langle f\rangle \times \langle g\rangle$ est d'ordre 4 (isomorphe à $\mathbb{Z}_2^2$). On remarque que l'action de E décompose $\{1,2,3,4,5,6,7,8\}$ en orbites $\{1,2\}, \{3,4\}, \{5,6\}, \{7,8\}$, alors que $\langle f, g\rangle$ a pour orbites $\{1,3\}, \{2,4\}, \{5,7\}, \{6,8\}$. En particulier $E \cap \langle f, g\rangle = \{\mathrm{id}\}$. Par conséquent $F = \langle E, f\rangle = E \rtimes \langle f\rangle$ est d'ordre 16, puis $G = \langle E, f, g\rangle = F \rtimes \langle g\rangle = E \rtimes \langle f, g\rangle$ est d'ordre 32. L'action de G décompose $\{1,2,3,4,5,6,7,8\}$ en orbites $\{1,2,3,4\}, \{5,6,7,8\}$. On voit finalement que $h \notin G$, donc $H = G \rtimes \langle h\rangle$ est d'ordre 64. Comme $|A_8| = 2^6 \cdot 3^2 \cdot 5 \cdot 7$, on conclut que H est effectivement un 2-sous-groupe de Sylow de A_8.

(e) On voit que $ab = (1,2)(3,4)(5,6)(7,8)$ est dans le centre de H, car il commute avec a, b, c, f, g, h d'après les calculs précédents. Réciproquement supposons que $z \in H$ est central. Si $z(1) \in \{5,6,7,8\}$ alors $z^b \neq z$, et si $z(1) \in \{3,4,5,6\}$ alors $z^c \neq z$. Il ne reste que la possibilité $z(1) \in \{1,2\}$. De même on trouve $z(2) \in \{1,2\}$. Deux cas se présentent : si $z(1) = 1$ et $z(2) = 2$, alors $z = z^f$ implique $z(3) = 3$ et $z(4) = 4$, puis $z = z^h$ implique $z(5) = 5$, $z(6) = 6$, $z(7) = 7$, $z(8) = 8$, donc $z = \mathrm{id}$. Sinon, on a forcément $z(1) = 2$ et $z(2) = 1$, et on peut appliquer le raisonnement à zab : comme zab fixe 1 et 2, on conclut que $zab = \mathrm{id}$. Ainsi le centre de H est effectivement réduit à $H = \{\mathrm{id}, ab\}$, comme énoncé.

4.4. S'il existait un isomorphisme $\phi\colon \mathrm{PSL}_3\,\mathbb{F}_4 \xrightarrow{\sim} A_8$, alors $\phi(T)$ serait un 2-Sylow de A_8, donc conjugué à H. En particulier on aurait un isomorphisme $T \cong H$. Mais le centre $Z(T)$ est d'ordre 4 tandis que le centre $Z(H)$ est d'ordre 2, donc $T \ncong H$. On conclut que les groupes simples $\mathrm{PSL}_3\,\mathbb{F}_4$ et A_8, bien que de même ordre, ne sont pas isomorphes.

Feuille A1 — POLYNÔMES SYMÉTRIQUES

Résumé. On considère l'action du groupe symétrique S_n sur l'anneau des polynômes $A[X_1, \dots, X_n]$ par permutation des variables. Les polynômes invariants sont appelés *polynômes symétriques*. Il est un fait très remarquable que les polynômes symétriques forment une algèbre libre, librement engendrée par les polynômes symétriques élémentaires. Cette feuille d'exercices en donne une preuve en développant un algorithme de réécriture.

1. Anneau des invariants et polynômes symétriques

1.1. Soit $\alpha\colon G \times B \to B$ une action d'un groupe G sur une A-algèbre B. Expliciter ce que l'on exige (parfois de manière sous-entendue) d'une telle action pour qu'elle corresponde à un homomorphisme de groupes $\rho\colon G \to \mathrm{Aut}_A(B)$. Montrer que l'ensemble des éléments invariants $B^G = \{b \in B \mid gb = b \text{ pour tout } g \in G\}$ est une sous-algèbre de B.

Remarquons qu'une action bénigne peut produire un anneau des invariants bien compliqué :

1.2. Soit $g = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}_2 \mathbb{Q}$. Le groupe $G = \langle g \rangle$ est d'ordre 2 et agit sur $\mathbb{Q}[X, Y]$ par $g \cdot X = -X$ et $g \cdot Y = -Y$. Montrer que $\mathbb{Q}[X, Y]^G$ est le sous-anneau $\mathbb{Q}[X^2, XY, Y^2]$. Est-il factoriel ? Est-ce une $\mathbb{Q}$-algèbre libre ?

En vue de cet exemple, on apprécie peut-être mieux la beauté des polynômes symétriques :

1.3. Rappeler la définition/construction de l'action naturelle de S_n sur $A[X_1, \dots, X_n]$. Énoncer le théorème sur la structure de l'anneau des invariants $A[X_1, \dots, X_n]^{S_n}$.

1.4. Essayez de réécrire les polynômes suivants en termes de polynômes symétriques élémentaires : $X_1^2 + X_2^2$, $(X_1 - X_2)^2$, $X_1^3 + X_2^3$, $(X_1 - X_2)^2 (X_2 - X_3)^2 (X_1 - X_3)^2$. (Si après réflexion vous n'arrivez pas, lisez la suite pour une méthode générale).

2. Ordre lexicographique des monômes

On ordonne les n-uplets $\alpha \in \mathbb{N}^n$ par ordre lexicographique : deux éléments $\alpha, \beta \in \mathbb{N}^n$ vérifient la relation $\alpha < \beta$ s'il existe un indice $i \in \{1, \dots, n\}$ tel que $\alpha_1 = \beta_1$, …, $\alpha_{i-1} = \beta_{i-1}$, et $\alpha_i < \beta_i$. Les n-uplets $\alpha \in \mathbb{N}^n$ sont en bijection avec les monômes $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, l'ordre sur $\mathbb{N}^n$ induit alors un ordre sur les monômes.

2.1. Voici quelques propriétés remarquables de l'ordre lexicographique :

(a) Tout ensemble non vide $I \subset \mathbb{N}^n$ possède un plus petit élément.

(b) Pour $\alpha, \alpha', \beta \in \mathbb{N}^n$ la relation $\alpha \leq \alpha'$ implique $\alpha + \beta \leq \alpha' + \beta$.

(c) En déduire que $\alpha \leq \alpha'$ et $\beta \leq \beta'$ impliquent $\alpha + \beta \leq \alpha' + \beta'$.

2.2. Pour $\alpha^0 \in \mathbb{N}^n$ il existe en général une infinité d'éléments $\alpha \in \mathbb{N}^n$ vérifiant $\alpha < \alpha^0$. (Quelles sont les exceptions ?) Par contre, montrer qu'il n'y a pas de "descente infinie" $\alpha^0 > \alpha^1 > \alpha^2 > \dots$: toute suite décroissante devient stationnaire.

Pour un polynôme non nul $P = \sum_\alpha p_\alpha X^\alpha$ on définit son degré lexicographique, noté $\deg_{\mathrm{lex}}(P)$, comme le plus grand n-uplet $\mu \in \mathbb{N}^n$ tel que $p_\mu \neq 0$; le terme dominant est $\mathrm{dom}(P) := p_\mu X^\mu$, le coefficient dominant est $\mathrm{cdom}(P) := p_\mu$. Pour le polynôme nul on pose $\mathrm{dom}(0) := 0$, $\mathrm{cdom}(0) := 0$ et $\deg_{\mathrm{lex}}(0) := -\infty$. Voici quelques exemples qui illustrent ces notions :

2.3. Dans le cas d'une variable, vérifier que l'on obtient les notions usuelles.

2.4. Ordonner les monômes de $P = X_2 X_3^2 + X_2^2 X_3 + X_2^2 X_3^2 + X_2 X_3^2 X_1 + X_3 X_2^2 X_1$ par ordre lexicographique. Quel est le terme dominant ? Le polynôme est-il symétrique ? Déterminer le sous-groupe $G < S_3$ qui laisse P invariant.

2.5. Le polynôme $P = \sum_{\sigma \in S_5} \sigma(X_2 X_4^3 X_5^2)$ est-il symétrique ? et $Q = \sum_{\tau \in A_5} \tau(X_2 X_4^3 X_5^2)$? Déterminer le degré lexicographique ainsi que le terme dominant. Quel est le rapport entre les coefficients de P et le stabilisateur du monôme en question ?

3. Algorithme de réécriture pour les polynômes symétriques

Soit A un anneau commutatif unitaire. On se propose de montrer que tout polynôme symétrique $P \in A[X_1, \dots, X_n]$ s'écrit de manière unique en fonction des polynômes symétriques élémentaires $s_1, \dots, s_n$, définis par l'équation

$$(T + X_1)(T + X_2) \cdots (T + X_n) = T^n + s_1 T^{n-1} + s_2 T^{n-2} + \cdots + s_n.$$

En utilisant l'ordre lexicographique, nous pouvons déduire le théorème comme suit :

3.1. Montrer que $\deg_{\mathrm{lex}}(PQ) = \deg_{\mathrm{lex}}(P) + \deg_{\mathrm{lex}}(Q)$ et $\mathrm{dom}(PQ) = \mathrm{dom}(P)\,\mathrm{dom}(Q)$, pourvu que (i) A soit intègre, ou (ii) au moins un des polynômes P et Q soit unitaire. En déduire à nouveau que l'anneau $A[X_1, \dots, X_n]$ est intègre si et seulement si A l'est.

3.2. Déterminer le terme dominant de s_i, puis de $s_1^{\nu_1} s_2^{\nu_2} \dots s_n^{\nu_n}$ pour $\nu \in \mathbb{N}^n$.
Analyser le degré lexicographique d'un polynôme symétrique $P \neq 0$.
Trouver $Q = c s_1^{\nu_1} s_2^{\nu_2} \dots s_n^{\nu_n}$ tel que $\deg_{\mathrm{lex}}(P - Q) < \deg_{\mathrm{lex}}(P)$.

3.3. En déduire un algorithme pour réécrire un polynôme symétrique en fonction des polynômes symétriques élémentaires. Pourquoi cet algorithme s'arrête-t-il ?

3.4. Réécrire les polynômes de l'exercice 1.4. Même question pour $X_1^2X_2^2 + X_1^2X_3^2 + X_2^2X_3^2$, puis $X_1^3X_2 + X_1X_2^3 + X_1^3X_3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$. (Ajouter d'autres exemples.)

3.5. Déterminer le terme dominant d'un polynôme non nul $R = \sum_\alpha r_\alpha s_1^{\alpha_1} s_2^{\alpha_2} \dots s_n^{\alpha_n}$, en montrant que $\mathrm{cdom}(R) = r_\nu$ pour un indice ν à préciser. En déduire que $R = 0$ si et seulement si $r_\alpha = 0$ pour tout α. Conclure que l'écriture en fonction des polynômes $s_1, \dots, s_n$ est unique.

4. Les formules de Newton

4.1. Dans $A[X_1, \dots, X_n]$ on considère les polynômes $p_k = \sum_i X_i^k$ avec $k \geq 1$. Évidemment $p_1 = \sum_i X_i = s_1$. Rappeler les formules de Newton exprimant p_k en fonction des s_k.

4.2. Soient $x_1, x_2, x_3, x_4 \in \mathbb{C}$ les quatre racines du polynôme $3X^4 + 7X^3 + 6X^2 + 8X + 6$. Déterminer la valeur de $x_1^4 + x_2^4 + x_3^4 + x_4^4$ et de $x_1^{-1} + x_2^{-1} + x_3^{-1} + x_4^{-1}$.

4.3. Soient $a, b, c \in \mathbb{C}$ tels que $a + b + c = 1$ et $a^2 + b^2 + c^2 = 2$ et $a^3 + b^3 + c^3 = 3$. Calculer la valeur de $a^4 + b^4 + c^4$. Pour tout $n \in \mathbb{N}$ on a $a^n + b^n + c^n \in \mathbb{Q}$ alors que $a, b, c \notin \mathbb{Q}$.

4.4. Peut-on exprimer tout polynôme symétrique sur A en fonction des polynômes p_k ?

4.5. Pour une matrice $A \in \mathrm{Mat}(n \times n, \mathbb{C})$ on pose $b_k = \mathrm{tr}(A^k)$ et $P_A = \det(T \cdot \mathrm{id} + A) = T^n + c_1 T^{n-1} + \cdots + c_n$. (C'est le polynôme caractéristique après remplacement $T \mapsto -T$.)

(a) Expliquer pourquoi $b_1 = c_1$, puis expliciter le rapport entre b_k et c_k.
Indication : justifier d'abord qu'il suffit de regarder une matrice A triangulaire.

(b) En déduire un algorithme pour calculer le polynôme caractéristique d'une matrice A, de sorte que le coût en nombre d'opérations arithmétiques soit d'ordre n^4.

5. Polynômes antisymétriques et alternés

5.1. Redémontrer que $P \in A[X]$ vérifie $P(a) = 0$ pour $a \in A$ si et seulement s'il existe $Q \in A[X]$ tel que $P = (X - a)Q$. En déduire que $P \in \mathbb{Z}[X, Y]$ vérifiant $P(X, Y) = -P(Y, X)$ s'écrit comme $P = (X - Y)Q$ avec $Q \in \mathbb{Z}[X, Y]$ symétrique.

5.2. On rappelle que le polynôme $\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j)$ dans $\mathbb{Z}[X_1, \dots, X_n]$ est *antisymétrique* dans le sens que $\sigma(\Delta) = \mathrm{sign}(\sigma) \cdot \Delta$ pour toute permutation $\sigma \in S_n$. Montrer que tout polynôme antisymétrique $P \in \mathbb{Z}[X_1, \dots, X_n]$ s'écrit comme $P = Q\Delta$ avec Q symétrique. Exprimer le déterminant de Vandermonde $\det\big(X_i^{j-1}\big)_{1 \leq i,j \leq n}$ en fonction de Δ.

5.3. Un polynôme $P \in A[X_1, \dots, X_n]$ est *alterné* si $\sigma P = P$ pour tout $\sigma \in A_n$. En supposant $2 \in A^\times$, montrer que $P = P_+ + P_-$ avec P_+ symétrique et P_- antisymétrique. Conclure que $A[X_1, \dots, X_n]^{A_n} = A[s_1, \dots, s_n, \Delta]$. Est-ce une algèbre libre ?

5.4. Montrer que $t = \sum_{\sigma \in A_n} \sigma(X_1^{n-1} \cdots X_{n-2}^2 X_{n-1}^1)$ et $t^* = \sum_{\sigma \in A_n} \sigma(X_1^{n-1} \cdots X_{n-2}^2 X_n^1)$ sont deux polynômes alternés. Vérifier que $t + t^*$ est symétrique alors que $\Delta = t - t^*$ est antisymétrique. Montrer que $A[X_1, \dots, X_n]^{A_n} = A[s_1, \dots, s_n, t]$, même si $2 \notin A^\times$.

Feuille A2 — FACTORIALITÉ

1. Anneaux de polynômes et factorialité

1.1. Rappeler la définition d'un anneau euclidien / principal / factoriel. Est-ce que $\mathbb{Q}[X]$ est euclidien ? principal ? factoriel ? et $\mathbb{Z}[X]$? et $\mathbb{Q}[X,Y]$? (On pourra regarder l'idéal $(2,X)$ dans $\mathbb{Z}[X]$, puis l'idéal (X,Y) dans $\mathbb{Q}[X,Y]$.)

1.2. Un anneau factoriel peut contenir un sous-anneau non factoriel ; c'est même possible dans un anneau de polynômes ! L'ensemble $A = \{P \in \mathbb{Q}[X] \mid P'(0) = 0\}$ est-il un sous-anneau de $\mathbb{Q}[X]$? A-t-on $A = \mathbb{Q}[X^2, X^3]$? Cet anneau est-il factoriel ? Montrer que tout élément de A s'écrit comme produit de polynômes irréductibles dans A (par récurrence sur le degré).

1.3. Voici un exemple voisin qui ne parle que de nombres naturels. Pour tout $k \in \mathbb{N}$ l'ensemble $M_k = \{kn + 1 \mid n \in \mathbb{N}\}$ est un sous-monoïde de $(\mathbb{N}, \cdot)$. Définir les notions d'élément inversible / composé / irréductible dans M_k. Déterminer la nature de $1, 4, 7, 10, 13, 16, \ldots$ dans M_3. Est-ce que tout élément de M_3 est produit d'éléments irréductibles ? Une telle décomposition est-elle unique ? Que dire du monoïde M_2 ?

1.4. Dans certains anneaux il existe des éléments qui ne s'écrivent même pas comme produit d'éléments irréductibles. En voici un exemple : On commence par l'anneau des polynômes $A_0 = \mathbb{Q}[X]$ en une variable X. Puis on considère $A_1 = \mathbb{Q}[X^{\frac{1}{2}}]$, qui est simplement l'anneau des polynômes où la variable s'appelle $X^{\frac{1}{2}}$. On regarde A_0 comme sous-anneau de A_1, suivant la convention usuelle $X = X^{\frac{1}{2}} \cdot X^{\frac{1}{2}}$. De même, pour tout $k \geq 0$, on considère $A_k = \mathbb{Q}[X^{\frac{1}{2^k}}]$ comme sous-anneau de $A_{k+1} = \mathbb{Q}[X^{\frac{1}{2^{k+1}}}]$. On obtient ainsi une chaîne infinie d'anneaux $A_0 \subset A_1 \subset A_2 \subset \ldots$. Vérifier que la réunion $A = \bigcup_k A_k$ est un anneau commutatif unitaire, de manière naturelle. (Étant donnés $a, b \in A$ se ramener à un sous-anneau A_k.) On a $A^\times = \mathbb{Q}$, en particulier $X^{\frac{n}{2^k}} \in A$ est non inversible pour tout k. Conclure que X ne s'écrit pas comme produit de facteurs irréductibles dans A.

2. Le lemme de Gauss

2.1. Soit A un anneau intègre. Vérifier que $\deg(PQ) = \deg(P) + \deg(Q)$ pour tout $P, Q \in A[X]$. En déduire que $A[X]$ est intègre et que $A[X]^\times = A^\times$. À titre d'avertissement, montrer que $2X + 1$ est inversible dans $\mathbb{Z}_4[X]$. Effectivement, $\mathbb{Z}_4[X]^\times = \{2PX \pm 1 \mid P \in \mathbb{Z}_4[X]\}$.

2.2. Pour $p \in A$ l'homomorphisme quotient $q\colon A \to A/pA$ se prolonge en un homomorphisme $\tilde{q}\colon A[X] \to (A/pA)[X]$ avec $\tilde{q}(X) = X$. En déduire que $A[X]/pA[X] \cong (A/pA)[X]$. Conclure que p est premier dans A si et seulement s'il est premier dans $A[X]$.

Dans la suite on suppose que A est un anneau factoriel et $K = \mathrm{Frac}(A)$ son corps des fractions.

2.3. Pour $P \in A[X]$ rappeler la décomposition $P = \mathrm{cont}(P)\,\mathrm{prim}(P)$ en contenu $\mathrm{cont}(P) \in A$ et partie primitive $\mathrm{prim}(P) \in A[X]$. Décomposer ainsi $P = X^3Y + X^3 + X^2Y^2 - X^2 + XY^3 - XY$ dans $\mathbb{Q}[Y][X]$ (ici $A = \mathbb{Q}[Y]$) puis dans $\mathbb{Q}[X][Y]$ (ici $A = \mathbb{Q}[X]$).

2.4. Montrer $\mathrm{prim}(PQ) = \mathrm{prim}(P)\,\mathrm{prim}(Q)$ et $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$ à l'aide de l'exercice 2.2. L'illustrer pour $P = 4X^2 - 6X + 10$ et $Q = 3X^3 - 12$ sur $\mathbb{Z}$.

2.5. Pour $P \in K[X]$ expliciter $a \in A \smallsetminus \{0\}$ tel que $aP \in A[X]$. Définir une décomposition $P = \mathrm{cont}(P)\,\mathrm{prim}(P)$ en contenu $\mathrm{cont}(P) \in K$ et partie primitive $\mathrm{prim}(P) \in A[X]$. A-t-on toujours $\mathrm{prim}(PQ) = \mathrm{prim}(P)\,\mathrm{prim}(Q)$ et $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$?

2.6. Énoncer le théorème de Gauss sur la factorialité de $A[X]$, et caractériser les polynômes irréductibles dans $A[X]$. À titre d'avertissement, donner un polynôme dans $\mathbb{Z}[X]$ qui est réductible dans $\mathbb{Z}[X]$ mais irréductible dans $\mathbb{Q}[X]$. La situation réciproque est-elle possible ?

2.7. Soient $P, Q \in A[X]$ deux polynômes primitifs. Dans $K[X]$ l'algorithme d'Euclide permet de calculer un pgcd $R \in K[X]$. Est-ce que $\mathrm{prim}(R)$ est un pgcd de P, Q dans $A[X]$?

2.8. Supposons que l'on sache calculer le pgcd dans A. Expliciter un algorithme pour calculer le pgcd dans $A[X]$. L'appliquer à $P = 24X^3 - 81$ et $Q = 24X^2 - 72X + 54$ dans $\mathbb{Z}[X]$, puis à $P = XY^3 + X^2Y - Y^2 - X$ et $Q = XY^3 - X^3Y - Y^2 + X^2$ dans $\mathbb{Q}[X,Y]$.

3. Extensions quadratiques de $\mathbb{Z}$

3.1. (Rappel) Les entiers de Gauss $\mathbb{Z}[i]$ forment un sous-anneau de $\mathbb{C}$, avec $\mathrm{Aut}(\mathbb{Z}[i]) = \{\mathrm{id}, \mathrm{conj}\}$. L'application $N(z) = z\bar{z}$ est multiplicative et à valeurs dans $\mathbb{N}$. On a $N(z) = 0$ ssi $z = 0$, et $N(z) = 1$ ssi z est inversible dans $\mathbb{Z}[i]$. Tout $q \in \mathbb{C}$ admet une approximation $z \in \mathbb{Z}[i]$ avec $|q - z|^2 \leq \frac{1}{2}$. On en déduit que $\mathbb{Z}[i]$ est euclidien par rapport à N.

3.2. Comme second exemple, regardons l'anneau $\mathbb{Z}[j]$ avec $j = e^{2\pi i/3} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$. Montrer que j est racine de $X^2 + X + 1$. Dessiner $\mathbb{Z}[j]$ dans le plan complexe. Vérifier que $\mathrm{Aut}(\mathbb{Z}[\xi]) = \{\mathrm{id}, \mathrm{conj}\}$. Déterminer le groupe $\mathbb{Z}[j]^\times$. Montrer que tout $q \in \mathbb{C}$ admet une approximation $z \in \mathbb{Z}[j]$ avec $|q - z|^2 \leq \frac{1}{3}$. Conclure que $\mathbb{Z}[j]$ est euclidien par rapport à N.

3.3. Ces deux exemples motivent de regarder plus généralement les *extensions quadratiques* de $\mathbb{Z}$. Soit $P = uX^2 + vX + w$ un polynôme irréductible dans $\mathbb{Z}[X]$, et $\xi, \xi^* \in \mathbb{C}$ ses deux racines.

(a) Montrer que $K = \{a + b\xi \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$.
Vérifier que $(1, \xi)$ est une base de K sur son sous-corps $\mathbb{Q}$.

(b) Montrer que $A = \{a + b\xi \mid a, b \in \mathbb{Z}\}$ est un sous-anneau si et seulement si P est unitaire. Vérifier que $\xi^* \in A$, conclusion spécifique aux extensions quadratiques.

(c) On suppose désormais P unitaire. Vérifier que $(a + b\xi)^* := a + b\xi^*$ définit un automorphisme de l'anneau A. En déduire que $G = \mathrm{Aut}(A)$ est d'ordre 2. *Indication :* Tout automorphisme $\sigma\colon A \to A$ fixe $\mathbb{Z}$. Quelles sont les images possibles de ξ ?
Remarque : Dans le cas où $\xi, \xi^* \in \mathbb{C} \smallsetminus \mathbb{R}$ sont complexes non réelles, vérifier que $\xi \mapsto \xi^*$ est la conjugaison complexe usuelle, donc $\mathrm{Aut}(A) = \{\mathrm{id}, \mathrm{conj}\}$.

(d) Conclure que l'anneau des invariants A^G est exactement $\mathbb{Z}$.

3.4. Certaines propriétés de ces extensions sont d'une nature très générale, non limitée au cas quadratique. Soit A un sous-anneau de $\mathbb{C}$ tel que son groupe d'automorphismes $G = \mathrm{Aut}(A)$ soit fini et le sous-anneau invariant soit $A^G = \mathbb{Z}$. On définit $N\colon A \to \mathbb{Z}$ par $N(a) := \prod_{\sigma \in G} a^\sigma$.

(a) Vérifier que N est effectivement à valeurs dans $\mathbb{Z}$, comme énoncé.

(b) Montrer que N est multiplicative, et que $N(a) = 0$ équivaut à $a = 0$.

(c) Montrer que a est inversible dans A si et seulement si $N(a)$ est inversible dans $\mathbb{Z}$.

(d) Montrer que a est irréductible dans A si $N(a)$ est irréductible dans $\mathbb{Z}$.

(e) Montrer que tout élément de A s'écrit comme produit de facteurs irréductibles.

Le caractère euclidien / principal / factoriel, par contre, doit être étudié cas par cas :

3.5. Pour $\xi = i\sqrt{2}$ dessiner $\mathbb{Z}[\xi]$ dans le plan complexe. Déterminer $\mathbb{Z}[\xi]^\times$. Vérifier que tout $q \in \mathbb{C}$ admet une approximation $z \in \mathbb{Z}[\xi]$ avec $|q - z|^2 \leq \frac{3}{4}$. Conclure que $\mathbb{Z}[i\sqrt{2}]$ est euclidien par rapport à $N(z) = z\bar{z}$.

3.6. Pour $\xi = i\sqrt{3}$ dessiner $\mathbb{Z}[\xi]$ dans le plan complexe. Déterminer $\mathbb{Z}[\xi]^\times$. Vérifier que tout $q \in \mathbb{C}$ admet une approximation $z \in \mathbb{Z}[\xi]$ avec $|q - z|^2 \leq 1$, mais cette borne ne peut être améliorée. Expliquer pourquoi l'approche euclidienne ci-dessus échoue ici.

A priori, l'anneau $\mathbb{Z}[i\sqrt{3}]$ pourrait être euclidien par rapport à un autre stathme. Il n'en est rien — $\mathbb{Z}[i\sqrt{3}]$ n'est même pas factoriel, comme montre l'exercice suivant :

3.7. Énumérer les plus petites valeurs de $N\colon \mathbb{Z}[i\sqrt{3}] \to \mathbb{N}$. En déduire que $z \in \mathbb{Z}[i\sqrt{3}]$ avec $N(z) = 4$ est irréductible dans $\mathbb{Z}[i\sqrt{3}]$. Contempler l'équation $2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$.

3.8. De manière analogue, montrer que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel. De même pour $\mathbb{Z}[i\sqrt{7}]$.

3.9. Soit d un entier négatif congru à 1 modulo 4. On pose $\xi = \frac{1}{2}(1 + \sqrt{d})$. Trouver le polynôme irréductible de ξ sur $\mathbb{Q}$. Expliciter $N(\xi)$ puis $N(a + b\xi)$. Soit D la distance maximale de $q \in \mathbb{C}$ au réseau $\mathbb{Z}[\xi]$. Si $D < 1$, l'anneau $\mathbb{Z}[\xi]$ est-il euclidien ? Expliquer comment trouver $q \in \mathbb{C}$ qui maximise la distance au réseau $\mathbb{Z}[\xi]$. Expliciter D en fonction de d, puis conclure que l'inégalité $D < 1$ équivaut à $d \in \{-3, -7, -11\}$. *Indication :* Si Δ est un triangle de cotés a, b, c, et que A est son aire et R le rayon du cercle circonscrit, alors $abc = 4AR$.

Feuille A3 — EXERCICES DIVERS SUR LES POLYNÔMES

1. QUELQUES QUESTIONS DU COURS ET DE RÉVISION

1.1. Vérifier que $X^2 - 1 \in \mathbb{Z}_8[X]$ admet quatre racines. En quoi est-ce surprenant ? Contempler l'équation $X^2 - 1 = (X-1)(X+1) = (X-3)(X+3)$ sur $\mathbb{Z}_8$.

1.2. Soit A un anneau intègre. Montrer qu'un polynôme $P \in A[X]$ de degré n admet au plus n racines dans A (comptées avec multiplicités ; formuler d'abord un énoncé plus précis).

1.3. Soit A un anneau commutatif unitaire. Si A est intègre et de cardinal fini, alors A est un corps. De manière analogue : soit A un algèbre commutative sur un corps K. Si A est intègre et de dimension finie sur K, alors A est un corps. (On regardera l'application $\gamma_a : x \mapsto ax$.)

1.4. Si M est une matrice $n \times n$ à coefficients dans un anneau commutatif A, telle que l'application associée $A^n \to A^n$ est surjective, alors M est inversible. Peut-on remplacer surjectif par injectif ? et si A était un corps ?

1.5. Si $\phi\colon A \to B$ est un homomorphisme d'anneaux bijectif, d'inverse ψ, alors $\psi\colon B \to A$ est un homomorphisme d'anneaux.

1.6. Soit $\phi\colon A = K[X_0, X_1, \dots, X_n] \to K[Y_0, Y_1, \dots, Y_n]$ l'homomorphisme de K-algèbres défini par $\phi(X_0) = Y_0$ et $\phi(X_k) = Y_0 Y_k$ pour tout $k = 1, \dots, n$. Montrer ϕ est un isomorphisme sur la sous-algèbre B engendrée par les monômes $Y_0^{\nu_0} Y_1^{\nu_1} \cdots Y_n^{\nu_n}$ vérifiant $\nu_0 \geq \nu_1 + \cdots + \nu_n$. Expliciter l'inverse ψ, puis vérifier qu'il est un homomorphisme d'anneaux (d'abord de manière directe, puis en utilisant l'exercice précédent).

1.7. Soit A un anneau intègre, et $P \in A[X] \subset A[X,Y]$ et $Q \in A[Y] \subset A[Y,X] = A[X,Y]$ deux polynômes. Supposons qu'il existe $x \in A$ tel que $P(x) \in A^\times$. Alors les seuls diviseurs communs de P et Q dans $A[X,Y]$ sont les éléments de $A^\times = (A[X,Y])^\times$.

2. POLYNÔMES INTERPOLATEURS

2.1. Énoncer puis démontrer le théorème d'interpolation de Lagrange. Expliciter l'ensemble des polynômes $P \in \mathbb{Q}[X]$ vérifiant $P(0) = 3$, $P(1) = 1$, $P(2) = 5$. Quel en est le plus petit ? Est-il à coefficients entiers ? Mêmes questions pour $P(0) = 1$, $P(1) = 1$, $P(2) = 5$.

2.2. Essayer de factoriser $P = 3X^6 - 11X^5 + 4X^4 + 24X^3 - 28X^2 + 5X + 6$ dans $\mathbb{Z}[X]$ par la méthode d'anneau finiement factoriel développée en cours. (On pourra commencer par évaluer P en $0, 1, 2$.)

2.3. Soit $K_n[X]$ l'ensemble des polynômes de degré $\leq n$. L'application $\Phi\colon K_n[X] \to K^{n+1}$ donnée par $P \mapsto (P(x_0), P(x_1), \dots, P(x_n))$ est K-linéaire. Écrire sa matrice par rapport aux bases canoniques, puis calculer son déterminant. En déduire une preuve alternative d'existence et unicité de l'interpolateur de Lagrange. Quel est l'inconvénient de cette approche ?

2.4. On s'intéresse finalement aux polynômes à coefficients rationnels prenant des valeurs entières sur les entiers. Évidemment tout $P \in \mathbb{Z}[X]$ a cette propriété, mais ce n'est pas tout… Pour $k \in \mathbb{N}$ on définit $C_k \in \mathbb{Q}[X]$ par $C_k = \frac{1}{k!} X(X-1)\cdots(X-k+1)$, donc $C_0 = 1$, $C_1 = X$, $C_2 = \frac{1}{2}X(X-1)$ etc. On pose $C_k = 0$ pour $k < 0$.

(a) Évaluer C_k en $0, 1, \dots, k$. En déduire que tout polynôme $P \in \mathbb{C}[X]$ de degré $\leq n$ s'écrit de manière unique comme $P = \sum_{k=0}^n a_k C_k$ avec $a_k \in \mathbb{C}$.

(b) Pour $P \in \mathbb{C}[X]$ on définit sa *dérivée discrète* par $\Delta P = P(X+1) - P(X)$. Montrer que $\Delta C_k = C_{k-1}$ pour tout k. En déduire que $C_k(\mathbb{Z}) \subset \mathbb{Z}$ pour tout k.

(c) Si $P \in \mathbb{C}[X]$ est de degré $n \geq 1$, alors ΔP est de degré $n-1$. Si $\Delta P = \Delta Q$ et $P(0) = Q(0)$, montrer que $P = Q$.

(d) En déduire que tout polynôme $P \in \mathbb{C}[X]$ de degré $\leq n$ s'écrit comme $P = \sum_{k=0}^n a_k C_k$ avec des coefficients $a_k = (\Delta^k P)(0)$ pour tout $k = 0, \dots, n$.

Conclure qu'un polynôme $P \in \mathbb{C}[X]$ vérifie $P(\mathbb{Z}) \subset \mathbb{Z}$ si et seulement s'il s'écrit comme $P = \sum_{k=0}^n a_k C_k$ avec $a_k \in \mathbb{Z}$.

2.5. Au lieu de prescrire les valeurs $P(x_0), \dots, P(x_n)$, on peut prescrire les valeurs de P *et* de ses dérivées. Pour cela on fixe $n+1$ éléments distincts $x_0, \dots, x_n$ et des multiplicités $\mu_0, \dots, \mu_n \geq 1$, puis on considère $L_{i,k} = \frac{1}{k!}(X - x_i)^k \prod_{j \neq i} \left(\frac{X - x_j}{x_i - x_j}\right)^{\mu_j}$ pour $0 \leq i \leq n$ et $0 \leq k < \mu_i$. Evaluer $L_{i,k}$ et ses dérivées en $x_0, \dots, x_n$. Formuler puis prouver un énoncé analogue à l'interpolation de Lagrange.

3. Le déterminant vu comme polynôme

3.1. Rappeler la formule polynômiale du déterminant. Montrer que $\mathrm{GL}_n \mathbb{R}$ est un ouvert de $\mathbb{R}^{n \times n}$. Est-il dense ? Montrer que $\mathrm{GL}_n \mathbb{R} \to \mathrm{GL}_n \mathbb{R}$, $A \mapsto A^{-1}$ est continue. Est-elle dérivable ?

Dans l'anneau $A_n = \mathbb{Z}[X_{ij} | 1 \leq i, j \leq n]$ soit $\det_n$ le déterminant de la matrice $\begin{pmatrix} X_{11} & \dots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \dots & X_{nn} \end{pmatrix}$.

3.2. Montrer que $\det_2 = X_{11}X_{22} - X_{12}X_{21}$ est irréductible dans A_2.

3.3. On pose $\det_n = \det_{n-1} X_{nn} + P_n$. Est-ce que P_n est homogène ? De quel degré ? Comporte-t-il la variable X_{nn} ? Déterminer le nombre des variables X_{ij} avec $i, j < n$ dans chacun des monômes de P_n. Est-ce que $\det_{n-1}$ divise P_n ?

3.4. Montrer par récurrence que $\det_n$ est irréductible dans A_n.

4. Quelques applications du résultant

4.1. Soient $P, Q \in A[X]$ deux polynômes en une variable X sur un anneau A. Rappeler la définition du résultant $\mathrm{Res}_X(P, Q) \in A$, puis énoncer ses principales propriétés.

4.2. Trouver $\lambda \in \mathbb{R}$ de sorte que $X^3 - \lambda X + 2$ et $X^2 + \lambda X + 2$ aient une racine commune.

4.3. On considère les polynômes $P = X^2Y - XY^2$ et $Q = X^2 + Y^2 - 1$ dans $\mathbb{C}[X, Y]$, et on se propose de trouver toutes les solutions $(x, y) \in \mathbb{C}^2$ du système $P(x, y) = Q(x, y) = 0$.

(a) On pourra calculer le résultant $\mathrm{Res}_Y(P, Q) = X^2(X^2 - 1)(2X^2 - 1)$, en déduire tous les candidats $x \in \mathbb{C}$, puis remonter pour trouver toutes les solutions (x, y).

(b) Pour vérification, en utilisant la structure particulière du système, on pourrait obtenir le résultat par une approche plus directe.

4.4. Pour un exemple plus réaliste, vous pouvez regarder $P = X^3 + Y^3 - 35$ et $Q = X^2 + Y^2 - 13$. *Indication :* Vérifier que $\mathrm{Res}_Y(P, Q) = (X - 2)(X - 3)(2X^2 - 4X - 9)(X^2 + 7X + 18)$, puis en déduire toutes les solutions $(x, y) \in \mathbb{C}^2$ vérifiant $P(x, y) = Q(x, y) = 0$.

5. Quelques applications du discriminant

5.1. Rappeler la définition du discriminant $\mathrm{Disc}(P)$ d'un polynôme $P \in A[X]$. Quel est le rapport avec $\mathrm{Res}(P, P')$? A titre d'illustration, rappeler ou recalculer $\mathrm{Disc}(aX^2 + bX + c) = b^2 - 4ac$ et $\mathrm{Disc}(X^3 + pX + q) = -4p^3 - 27q^2$.

5.2. Calculer $\mathrm{Disc}(X^n - 1)$ et $\mathrm{Disc}(X^n - X)$. Que dire de $\mathrm{Disc}(X^n - X^2)$?

On considère dans la suite le discriminant d'un polynôme unitaire $P \in \mathbb{R}[X]$. On peut supposer que les racines sont toutes distinctes, autrement $\mathrm{Disc}(P) = 0$. Supposons alors que P admet k racines réelles $x_1, \dots, x_k$ et $2l$ racines complexes conjuguées $y_1, \bar{y}_1, \dots, y_l, \bar{y}_l$.

5.3. Montrer que $\mathrm{Disc}(P) < 0$ si l est impair et $\mathrm{Disc}(P) > 0$ si l est pair.

5.4. Retrouver le critère sur le nombre des racines réelles de $aX^2 + bX + c$.

5.5. Expliciter un critère sur le nombre des racines réelles de $X^3 + pX + q$.

5.6. Déterminer k et l pour $X^n - 1$. Retrouver ainsi le signe de $\mathrm{Disc}(X^n - 1)$.

Nous terminons par une application topologique :

5.7. Un polynôme de degré n est *séparable* si ses n racines sont toutes distinctes. Montrer que les polynômes séparables de degré $\leq n$ sur $\mathbb{C}$ forment un ouvert de $\mathbb{C}^{n+1}$. Est-il dense ?

5.8. Montrer que les matrices dans $\mathrm{Mat}_n \mathbb{C} = \mathbb{C}^{n \times n}$ ayant toutes leurs n valeurs propres distinctes forment un ouvert de $\mathbb{C}^{n \times n}$. Est-il dense ?

Feuille A4 — POLYNÔMES IRRÉDUCTIBLES

1. FACTORISATION DE POLYNÔMES DE PETIT DEGRÉ

1.1. Un polynôme $P \in K[X]$ de degré 2 ou 3 sur un corps K est réductible si et seulement s'il admet une racine dans K. Ce critère est-il encore valable pour $\deg P \geq 4$?

1.2. Voici une méthode pour trouver les racines rationnelles de $P = \sum_{i=0}^{i=n} p_i X^i \in \mathbb{Z}[X]$. Vérifier que $b^n P(\frac{a}{b})$ est un entier. Si $\operatorname{pgcd}(a,b) = 1$, montrer que $P(\frac{a}{b}) = 0$ implique $a \mid p_0$ et $b \mid p_n$. En déduire l'ensemble des rationnels candidats à être racine de P.

1.3. Montrer que $\sqrt[n]{a}$ avec $a, n \in \mathbb{N}$ est soit entière soit irrationnelle. Plus généralement : Toute racine rationnelle de $P = X^n + p_{n-1}X^{n-1} + \cdots + p_0 \in \mathbb{Z}[X]$ est entière.

1.4. Les polynômes suivants sont-ils irréductibles dans $\mathbb{Q}[X]$? Les factoriser le cas échéant. $X^3 - X + 1$, $X^3 - X - 1$, $X^3 - 2X^2 + X + 15$, $X^3 + 5X + 3$, $9X^3 + 7X + 3$, $X^3 + 3X^2 + 6X + 5$, $X^3 + 3X^2 + 5X + 6$, $4X^2 + 4X + 1$, $2X^3 + 3X^2 + 3X + 1$.

1.5. Factoriser $2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$ dans $\mathbb{Z}[X]$ en éléments irréductibles.

1.6. Montrer que $X^4 - 10X^3 + 21X^2 - 10X + 11$ est irréductible dans $\mathbb{Z}[X]$.

1.7. Factoriser $X^4 - X^2 + 1$ dans $\mathbb{F}_{11}[X]$ en éléments irréductibles.

1.8. Factoriser $P = X^5 + X + 1$ dans $\mathbb{Z}[X]$. Commencer par remarquer que $P(j) = 0$.

1.9. Montrer que $X^2 + Y^2 - 1$ est irréductible dans $\mathbb{C}[X,Y]$. Est-ce vrai dans $\mathbb{F}_2[X,Y]$?

2. UN CRITÈRE D'IRRÉDUCTIBILITÉ PASSANT PAR DES QUOTIENTS

2.1. Soient A un anneau *intègre* et $P \in A[X]$ un polynôme *unitaire*. Soient I un idéal propre de A et $\phi\colon A[X] \to (A/I)[X]$ l'application quotient induite. Si $\phi(P)$ est irréductible dans $(A/I)[X]$, alors P est irréductible dans $A[X]$.

Soulignons que, dans le critère précédent, les deux hypothèses sont essentielles :

2.2. Le polynôme $P = 2X^2 + X$ est réductible dans $\mathbb{Z}[X]$, alors que son image dans $\mathbb{Z}_2[X]$ est irréductible. Notez que P est de contenu 1 mais non unitaire.

2.3. Vérifier que $X \in \mathbb{Z}_6[X]$ s'écrit comme produit de deux polynômes de degré 1. Pourtant l'image de X est irréductible dans $\mathbb{Z}_2[X]$ *et* dans $\mathbb{Z}_3[X]$.

L'application typique du critère ci-dessus est le cas $A = \mathbb{Z}$ et $I = p\mathbb{Z}$ avec p premier.

2.4. Dresser la liste des polynômes unitaires irréductibles de degré $1, 2, 3$ sur $\mathbb{F}_2$ et $\mathbb{F}_3$.

2.5. Les polynômes suivants sont-ils irréductibles dans $\mathbb{Z}[X]$?
$X^3 + 14X^2 + 19X + 25$, $X^3 + 35X^2 + 18X + 45$, $X^3 + 5X^2 + 7X + 13$.

2.6. Décomposer $X^4 + 1$ dans $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$, $\mathbb{Z}[X]$, $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$.
Remarque : On verra que $X^4 + 1$ est réductible sur $\mathbb{F}_p$ quel que soit le premier p.

3. LE CRITÈRE D'EISENSTEIN

3.1. Énoncer (et redémontrer) le critère d'Eisenstein pour l'irréductibilité d'un polynôme $P \in \mathbb{Z}[X]$.

3.2. Pour $a \geq 2$ premier et $n \geq 2$ on a $\sqrt[n]{a} \notin \mathbb{Q}$. Plus précisément, $[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}] = n$.

3.3. Décomposer $P = 6X^n - 6X^{n-1} + 24X^2 - 12X - 12$ avec $n \geq 3$ en facteurs irréductibles dans $\mathbb{Z}[X]$.

3.4. Décomposer en produit de polynômes irréductibles de $\mathbb{Z}[X]$ les polynômes suivants :
$X^4 - 4X^3 + 6$, $X^3 + nX + 2$, $X^4 + 10X^2 + 1$, $X^4 + 4X^3 + 6X^2 + 2X + 1$, $X^8 - 1$.

4. Automorphismes de $K[X]$ et de $K(X)$

Dans la suite soit K un corps, $K[X]$ l'anneau des polynômes sur K, et $K(X)$ le corps des fractions rationnelles sur K, c'est-à-dire le corps des fractions de $K[X]$.

4.1. Soit $\phi_{a,b}\colon K[X] \to K[X]$ défini par $X \mapsto aX + b$, avec $a \in K^\times$ et $b \in K$. Montrer que $\phi_{a,b}$ est un automorphisme de la K-algèbre $K[X]$; expliciter l'automorphisme inverse.

4.2. Soit $Y \in K[X]$ un polynôme de degré $n \geq 1$. Pour $P \in K[X]$, expliciter $\deg P(Y)$ en fonction de $\deg P$. En déduire que $\mathrm{Aut}_K(K[X]) = \{\phi_{a,b} \mid a \in K^\times, b \in K\}$.

4.3. Pour $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2 K$ on définit $\phi_M\colon K(X) \to K(X)$ par $X \mapsto \frac{aX+b}{cX+d}$. Montrer que ϕ_M est un automorphisme de la K-algèbre $K(X)$; expliciter l'automorphisme inverse.

4.4. Montrer que l'application $\mathrm{GL}_2 K \to \mathrm{Aut}_K(K(X))$ est un homomorphisme de groupes, qui a pour noyau $K^\times \,\mathrm{id}$. Son image est donc isomorphe au groupe $\mathrm{PGL}_2 K = \mathrm{GL}_2 K / K^\times$.

4.5. Énoncer le théorème de Lüroth. En déduire que $\mathrm{Aut}_K(K(X)) \cong \mathrm{PGL}_2 K$.

Ajoutons deux remarques qui sont parfois utiles :

4.6. Un polynôme $P(X)$ est irréductible dans $K[X]$ si et seulement si $P(X+a)$ l'est, avec $a \in K$.

4.7. Quel est le rapport entre les résultants $\mathrm{Res}(P(X), Q(X))$ et $\mathrm{Res}(P(X+a), Q(X+a))$? Même question pour les discriminants $\mathrm{Disc}(P(X))$ et $\mathrm{Disc}(P(X+a))$.

5. Polynômes irréductibles et extensions de corps

5.1. On considère $K_1 = \mathbb{F}_3[X]/(X^2+1)$ et $K_2 = \mathbb{F}_3[Y]/(Y^2+2Y-1)$.

(a) Vérifier que K_i est un corps. Déterminer le degré $[K_i : \mathbb{F}_3]$ et le cardinal $|K_i|$.

(b) Construire explicitement un isomorphisme entre K_1 et K_2.

5.2. Montrer que $\mathbb{Q}[X]/(X^2+1)$ et $\mathbb{Q}[Y]/(Y^2+2Y-1)$ sont deux corps non isomorphes.

6. Extensions de corps et polynômes irréductibles

6.1. Soient $E|K$ une extension de corps et $\alpha \in E$ un élément algébrique sur K, c'est-à-dire il existe un polynôme $P \in K[X]$ dont α est racine. Comme K est un corps on supposera P unitaire. Montrer l'équivalence des conditions suivantes :

(a) P est le polynôme minimal de α sur K.

(b) P est irréductible dans $K[X]$.

(c) On a $[K(\alpha) : K] = \deg P$.

6.2. (a) Déterminer les degrés $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ puis $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

(b) Soit $\alpha = \sqrt{2} + \sqrt{3}$. Expliciter α^{-1} et montrer que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(c) Trouver un polynôme $P \in \mathbb{Q}[X]$ de degré 4 de racine α. Est-il irréductible ?

CONTRÔLE CONTINU 2004/2 — ANNEAUX

Ni documents ni calculatrices ne sont autorisés.
Les paragraphes sont indépendants entre eux.
Justifiez vos réponses : brièvement mais suffisamment.

1. POLYNÔMES IRRÉDUCTIBLES ET FACTORISATION DANS $\mathbb{Z}[X]$

1.1. Énoncer puis redémontrer le critère d'Eisenstein pour l'irréductibilité dans $\mathbb{Z}[X]$.

1.2. Décomposer $P = 6X^n - 6X^{n-1} + 24X^2 - 12X - 12$ avec $n \geq 3$ en facteurs irréductibles dans $\mathbb{Z}[X]$.

2. LE DÉTERMINANT VU COMME POLYNÔME

Dans l'anneau $A_n = \mathbb{Q}[X_{ij} | 1 \leq i, j \leq n]$ soit $\det_n$ le déterminant de la matrice $\begin{pmatrix} X_{11} & \dots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \dots & X_{nn} \end{pmatrix}$.

2.1. Rappeler la formule polynômiale de $\det_n$.

2.2. Montrer que $\det_2 = X_{11}X_{22} - X_{12}X_{21}$ est irréductible dans A_2.

2.3. On pose $\det_n = \det_{n-1} X_{nn} + P_n$. Est-ce que P_n est homogène ? De quel degré ? Comporte-t-il la variable X_{nn} ? Déterminer le nombre des variables X_{ij} avec $i, j < n$ dans chacun des monômes de P_n. Est-ce que $\det_n$ est irréductible dans A_n ?

3. POLYNÔMES SYMÉTRIQUES ET ANTISYMÉTRIQUES

3.1. Énoncer le théorème des polynômes symétriques.

3.2. Réécrire $P = X_1^1X_2^2X_3^3 + X_1^1X_2^3X_3^2 + X_1^2X_2^1X_3^3 + X_1^2X_2^3X_3^1 + X_1^3X_2^1X_3^2 + X_1^3X_2^2X_3^1$ en termes des polynômes symétriques élémentaires.

On rappelle que le polynôme $\Delta = \prod_{i<j}(X_i - X_j)$ dans $\mathbb{Q}[X_1, \dots, X_n]$ est *antisymétrique* dans le sens que $\sigma(\Delta) = \operatorname{sign}(\sigma) \cdot \Delta$ pour toute permutation $\sigma \in S_n$.

3.3. Est-ce que tout polynôme antisymétrique $P \in \mathbb{Q}[X_1, \dots, X_n]$ s'écrit comme $P = Q\Delta$ avec Q symétrique ? Donner une preuve ou un contre-exemple.

3.4. Exprimer le déterminant de Vandermonde $\det \begin{pmatrix} X_1^{n-1} & X_2^{n-1} & \dots & X_n^{n-1} \\ \vdots & \vdots & & \vdots \\ X_1 & X_2 & \dots & X_n \\ 1 & 1 & \dots & 1 \end{pmatrix}$ en fonction de Δ.

4. EXTENSIONS GALOISIENNES DE $\mathbb{Z}$

Soit A un sous-anneau de $\mathbb{C}$. On suppose que son groupe d'automorphismes $G = \operatorname{Aut}(A)$ est fini et que le sous-anneau invariant est $A^G = \mathbb{Z}$. A titre d'exemple penser à $A = \mathbb{Z}[i]$.
On définit la norme $N\colon A \to \mathbb{Z}$ par $N(z) = \prod_{g \in G} g(z)$.

4.1. Expliquer pourquoi N prend ses valeurs dans $\mathbb{Z}$.

4.2. Montrer que N est multiplicative, et que $N(z) = 0$ équivaut à $z = 0$.

4.3. Est-ce que z est inversible dans A si et seulement si $N(z)$ est inversible dans $\mathbb{Z}$?

4.4. Est-ce que z est irréductible dans A si $N(z)$ est irréductible dans $\mathbb{Z}$?

4.5. Est-ce que tout élément de A s'écrit comme produit de facteurs irréductibles ?

4.6. Donner un exemple où A n'est pas factoriel.

CORRIGÉ

1. Polynômes irréductibles et factorisation dans $\mathbb{Z}[X]$

1.1. *Critère d'Eisenstein :* Soit $P = \sum_{i=0}^{i=n} p_i X^i \in \mathbb{Z}[X]$ un polynôme et $p \in \mathbb{Z}$ un nombre premier. Si $p \nmid p_n$, $p \mid p_{n-1}$, …, $p \mid p_0$ mais $p^2 \nmid p_0$, alors P ne se décompose pas comme $P = QR$ avec $\deg(Q), \deg(R) > 0$. (Ceci veut dire que P est irréductible dans $\mathbb{Q}[X]$.) Si de plus P est primitif sur $\mathbb{Z}$, alors il est irréductible dans $\mathbb{Z}[X]$. Pour une preuve, voir le cours.

1.2. On trouve d'abord que $P = 2 \cdot 3 \cdot (X^n - X^{n-1} + 4X^2 - 2X - 2)$. Il admet 1 pour racine, donc $P = 2 \cdot 3 \cdot (X - 1) \cdot (X^{n-1} + 4X + 2)$. Ce dernier facteur est irréductible d'après Eisenstein.

2. Le déterminant vu comme polynôme

2.1. On a $\det_n = \sum_\sigma \operatorname{sign}(\sigma) X_{1,\sigma(1)} \cdots X_{n,\sigma(n)}$, où σ parcourt tout le groupe symétrique S_n.

2.2. On considère $\det_2 = X_{11}X_{22} - X_{12}X_{21}$ comme un polynôme dans $A_2'[X_{22}]$ sur l'anneau $A_2' = \mathbb{Q}[X_{11}, X_{12}, X_{21}]$. On note $\deg\colon A_2'[X_{22}] \to \mathbb{N}$ le degré en la variable X_{22}. On a $\deg(\det_2) = 1$, donc $\det_2 = PQ$ entraîne $\deg(P) = 0$ ou $\deg(Q) = 0$. Supposons $\deg(P) = 0$, c'est-à-dire $P \in A_2'$. Comme P divise $X_{11}X_{22} - X_{12}X_{21}$, il divise les « coefficients » X_{11} et $X_{12}X_{21}$. Ceci n'est possible que pour $P \in \mathbb{Q}^\times$, car $\operatorname{cont}(\det_2) = \operatorname{pgcd}(X_{11}, X_{12}X_{21})$ vaut 1. Il s'agit donc d'un polynôme primitif sur A_2'. On conclut que $\det_2$ est irréductible dans A_2.

2.3. Le polynôme P_n est homogène de degré n. Chacun de ses monômes comporte une variable X_{in} avec $i < n$, une variable X_{nj} avec $j < n$, et $n - 2$ variables X_{ij} avec $i, j < n$.

Montrons par récurrence que $\det_n$ est irréductible dans A_n. Comme avant on considère $\det_n = \det_{n-1} X_{nn} + P_n$ comme un polynôme dans $A_n'[X_{nn}]$ sur l'anneau $A_n' = \mathbb{Q}[X_{ij} | (i,j) \neq (n,n)]$. On note $\deg\colon A_n'[X_{nn}] \to \mathbb{N}$ le degré en la variable X_{nn}. On a $\deg(\det_n) = 1$, donc $\det_n = PQ$ entraîne $\deg(P) = 0$ ou $\deg(Q) = 0$. Supposons $\deg(P) = 0$, c'est-à-dire $P \in A_n'$. Comme P divise $\det_{n-1} X_{nn} + P_n$, il divise le contenu $\operatorname{cont}(\det_n) = \operatorname{pgcd}(\det_{n-1}, P_n)$. On sait par récurrence que $\det_{n-1}$ est irréductible dans A_{n-1}, donc aussi dans A_n. Mais $\det_{n-1}$ ne divise pas P_n d'après notre considération des monômes. Le contenu de $\det_n$ sur A_n' vaut donc $\operatorname{pgcd}(\det_{n-1}, P_n) = 1$. On conclut que $\det_n$ est irréductible dans A_n.

3. Polynômes symétriques et antisymétriques

3.1. On considère un anneau A et l'algèbre des polynômes $A[X_1, \ldots, X_n]$ avec l'action du groupe symétrique S_n par permutation des variables. Un polynôme $P \in A[X_1, \ldots, X_n]$ est appelé *symétrique* s'il est invariant par l'action de S_n. On constate que les polynômes $s_1, \ldots, s_n$ définis par l'équation $(T + X_1) \cdots (T + X_n) = T^n + s_1 T^{n-1} + \cdots + s_n$ sont symétriques par construction. On les appelle *polynômes symétriques élémentaires*.

Théorème : Tout polynôme symétrique dans $A[X_1, \ldots, X_n]$ s'écrit de manière unique comme un polynômes en $s_1, \ldots, s_n$.

Autrement dit, l'homomorphisme d'anneaux $\Phi\colon A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, X_n]$ donné par $Y_i \mapsto s_i$ est un isomorphisme entre l'anneau des polynômes $A[Y_1, \ldots, Y_n]$ est l'anneau des polynômes symétriques $A[X_1, \ldots, X_n]^{S_n}$.

3.2. On trouve $P = s_1 s_2 s_3 - 3s_3^2$. Pour une méthode de calcul voir vos notes de TD.

3.3. Un polynôme antisymétrique $P(X_1, \ldots, X_n)$ change de signe si l'on échange deux variables X_i et X_j, c'est-à-dire $P(\ldots, X_i, \ldots, X_j, \ldots) = -P(\ldots, X_j, \ldots, X_i, \ldots)$. Sur $\mathbb{Q}$ ceci entraîne $P(\ldots, X_j, \ldots, X_j, \ldots) = 0$. Si l'on regarde P comme un polynôme en X_i, il admet alors X_j comme racine. Par conséquent $(X_i - X_j)$ divise P.

On sait que $\mathbb{Q}[X_1, \ldots, X_n]$ est factoriel. Les polynômes $(X_i - X_j)$ avec $i < j$ sont tous irréductibles, donc premiers, et deux à deux non associés. On conclut que $\Delta = \prod_{i<j}(X_i - X_j)$ divise P, il existe donc $Q \in \mathbb{Q}[X_1, \ldots, X_n]$ de sorte que $P = Q\Delta$. Reste à vérifier que Q est symétrique. D'un coté on a $\sigma(Q\Delta) = \sigma(P) = \operatorname{sign}(\sigma) P = \operatorname{sign}(\sigma) \cdot Q\Delta$, de l'autre coté on a $\sigma(Q\Delta) = \sigma(Q)\sigma(\Delta) = \operatorname{sign}(\sigma) \cdot \sigma(Q)\Delta$. On conclut que $\sigma(Q) = Q$.

3.4. Notons V_n le déterminant de Vandermonde. C'est un polynôme antisymétrique en $X_1, \ldots, X_n$. D'après l'exercice précédent, on sait que Δ divise V_n. Le polynôme Δ est homogène de degré $\frac{n(n-1)}{2}$, tout comme le polynôme V_n ; ils sont donc égaux à multiplication d'une constante près. Le terme initial de Δ est $X_1^{n-1} X_2^{n-2} \cdots X_{n-1}$ avec un signe positif, et ce terme apparaît dans le déterminant avec le même signe. On conclut que $V_n = \Delta$.

CONTRÔLE CONTINU 2005/2 — ANNEAUX

Ni documents ni calculatrices ne sont autorisés.
Les paragraphes sont indépendants entre eux.
Justifiez vos réponses : brièvement mais suffisamment.

1. POLYNÔMES IRRÉDUCTIBLES

1.1. Le polynôme $6X^6 - 8X^3 + 4$ est-il irréductible dans $\mathbb{Z}[X]$? Est-il irréductible dans $\mathbb{Q}[X]$?

2. UN ANNEAU NON FACTORIEL

2.1. On considère l'anneau $\mathbb{Z}[i\sqrt{7}] = \{a+bi\sqrt{7} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ avec l'application $N\colon \mathbb{Z}[i\sqrt{7}] \to \mathbb{N}$ donnée par $N(a + bi\sqrt{7}) = a^2 + 7b^2$. On a déjà vu en TD que N est multiplicative, que $N(x) = 0$ équivaut à $x = 0$, et que $N(x) = 1$ équivaut à $x = \pm 1$,

(a) Énumérer toutes les valeurs ≤ 8 prises par l'application N.

(b) Montrer que l'anneau $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.

3. POLYNÔMES SYMÉTRIQUES

3.1. Réécrire $X_1^3 + X_2^3 + X_3^3$ en polynômes symétriques élémentaires.

3.2. Soient $P, Q \in \mathbb{Z}[X_1, \ldots, X_n]$ deux polynômes et soit R un pgcd de P et Q dans $\mathbb{Z}[X_1, \ldots, X_n]$. Si P et Q sont symétriques, montrer que R est symétrique.
Indication : Vous pouvez utiliser le fait que tout polynôme antisymétrique $P_0 \in \mathbb{Z}[X_1, \ldots, X_n]$ s'écrit comme $P_0 = P_1\Delta$ avec $P_1 \in \mathbb{Z}[X_1, \ldots, X_n]$ symétrique et $\Delta = \prod_{1\leq i<j\leq n}(X_i - X_j)$.

3.3. Dans l'anneau $\mathbb{Z}[X_1, \ldots, X_n]$ on considère les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$, notés plus explicitement par $\sigma_{1,n}, \ldots, \sigma_{n,n}$ pour indiquer le nombre n des variables.

(a) Pour $1 \leq k < l \leq n$, déterminer le pgcd de $\sigma_{k,n}$ et $\sigma_{l,n}$ dans $\mathbb{Z}[X_1, \ldots, X_n]$.

(b) Pour $k < n$, exprimer $\sigma_{k,n}$ comme polynôme en X_n et déterminer son contenu.

(c) Décomposer les polynômes $\sigma_{k,n}$ en facteurs irréductibles $\mathbb{Z}[X_1, \ldots, X_n]$.

4. ACTION ET CORPS DES FRACTIONS

Soit G un groupe, A un anneau intègre, et $A \times G \to A$, $(a, g) \mapsto a^g$ une action à droite par automorphismes d'anneaux. On note $A^G := \{a \in A \mid a^g = a \text{ pour tout } g \in G\}$ le sous-anneau des éléments invariants par G.

4.1. Montrer que $\left(\frac{a}{b}\right)^g := \frac{a^g}{b^g}$ est une action bien définie du groupe G sur le corps des fractions $\mathrm{Frac}(A)$. Est-ce que G agit sur $\mathrm{Frac}(A)$ par automorphismes de corps ?

4.2. Montrer que $\mathrm{Frac}(A^G) \subset \mathrm{Frac}(A)^G$. Si G est *fini*, montrer que $\mathrm{Frac}(A^G) = \mathrm{Frac}(A)^G$.

4.3. On se propose de construire un exemple où $\mathrm{Frac}(A^G) \neq \mathrm{Frac}(A)^G$. Soit $A = \mathbb{Q}[X, Y]$ et $g\colon A \to A$ l'unique morphisme d'anneau vérifiant $X^g = 2X$ et $Y^g = 2Y$.

(a) Prouver que g est un automorphisme de l'anneau $\mathbb{Q}[X, Y]$.

Dans le groupe des automorphismes de A, soit $G = \langle g \rangle$ le sous-groupe engendré par g.

(b) Expliciter A^G. *Indication :* Tout polynôme non nul $P \in \mathbb{Q}[X, Y]$ s'écrit de manière unique comme $P = \sum_{i=0}^{n} P_i$ avec $P_i \in \mathbb{Q}[X, Y]$ homogène de degré i et $P_n \neq 0$.

(c) Expliciter $\mathrm{Frac}(A)^G$. *Indication :* Pour $\frac{P}{Q} \in \mathbb{Q}(X, Y)^G$ on pourrait calculer $\lim_{k\to\infty} \left(\frac{P}{Q}\right)^{g^k}$ de deux manières différentes.

4.4. Supposons que l'anneau A est factoriel et que le groupe G est fini. Est-ce que tout élément de $\mathrm{Frac}(A)^G$ admet une écriture sous forme de fraction irréductible de numérateur et dénominateur dans A^G ? *Indication :* Dans l'exemple précédent on pourrait remplacer 2 par -1.

CORRIGÉ

1. POLYNÔMES IRRÉDUCTIBLES

1.1. Le polynôme $P = 6X^6 - 8X^3 + 4$ s'écrit comme $P = 2Q$ avec $Q = 3X^6 - 4X^3 + 2 \in \mathbb{Z}[X]$, donc P est réductible dans $\mathbb{Z}[X]$. Par contre, Q est un polynôme d'Eisenstein par rapport à $p = 2$, il est donc irréductible dans $\mathbb{Q}[X]$. Comme 2 est inversible dans $\mathbb{Q}[X]$, le polynôme $P = 2Q$ est irréductible dans $\mathbb{Q}[X]$.

2. UN ANNEAU NON FACTORIEL

2.1. (a) Les plus petites valeurs prises par $N(a + bi\sqrt{7}) = a^2 + 7b^2$ sont $0, 1, 4, 7, 8, 9, 11, \ldots$.

(b) Dans $\mathbb{Z}[i\sqrt{7}]$ on a $(1 + i\sqrt{7})(1 - i\sqrt{7}) = 2 \cdot 2 \cdot 2$. Montrons que $1 \pm i\sqrt{7}$ et 2 sont irréductibles. Si $2 = xy$ alors $N(x)N(y) = N(2) = 4$, ce qui n'est possible que pour $N(x) = 1$ ou $N(y) = 1$; mais dans ce cas $x = \pm 1$ ou $y = \pm 1$ est inversible. Ceci prouve que 2 est irréductible dans $\mathbb{Z}[i\sqrt{7}]$. De manière analogue, si $1 + i\sqrt{7} = xy$ alors $N(x)N(y) = N(1 + i\sqrt{7}) = 8$, ce qui n'est possible pour $N(x) = 1$ ou $N(y) = 1$. Par conséquent $1 + i\sqrt{7}$ est irréductible dans $\mathbb{Z}[i\sqrt{7}]$. Il en est de même pour $1 - i\sqrt{7}$.

3. POLYNÔMES SYMÉTRIQUES

3.1. D'après les formules de Newton on a $S_1 = X_1 + X_2 + X_3 = \sigma_1$, et $S_2 = X_1^2 + X_2^2 + X_3^2 = \sigma_1 S_1 - 2\sigma_2 = \sigma_1^2 - 2\sigma_2$ puis $S_2 = X_1^3 + X_2^3 + X_3^3 = \sigma_1 S_2 - \sigma_2 S_1 + 3\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

3.2. Soient $P, Q \in \mathbb{Z}[X_1, \ldots, X_n]$ deux polynômes et soit $\tau \in \mathfrak{S}_n$ une permutation. Si R est un pgcd de P et Q, alors R^τ est un pgcd de P^τ et Q^τ. (C'est vrai pour tout automorphisme d'anneau.) Dans le cas où $P^\tau = P$ et $Q^\tau = Q$, on trouve alors que R et R^τ sont deux pgcd de P et Q, donc $R^\tau = \pm R$. On définit $\varepsilon\colon \mathfrak{S}_n \to \{\pm 1\}$ par l'équation $R^\tau = \varepsilon(\tau)R$. Il est clair que ε est un homomorphisme de groupes, donc $\varepsilon = 1$ ou $\varepsilon = \operatorname{sign}$. Dans le cas $\varepsilon = 1$, le polynôme R est symétrique comme souhaité. Il reste à exclure le cas $\varepsilon = \operatorname{sign}$:

Si R est antisymétrique, alors $P = P_0 R$ avec P_0 antisymétrique, donc $P_0 = P_1\Delta$. De même, $Q = Q_0 R$ avec Q_0 antisymétrique, donc $Q_0 = Q_1\Delta$. On conclut que $R\Delta$ est un diviseur commun de P et Q, ce qui contredit notre hypothèse que R est un pgcd.

Avertissement : Il n'est pas vrai en général que le pgcd de deux éléments G-invariants est lui-même G-invariant. Considérons $A = \mathbb{Z}[X, Y]$ avec l'action de $G = \langle g \rangle$ donnée par $X^g = -X$, $Y^g = -Y$. Les polynômes X^2 et XY sont G-invariants, tandis que leurs pgcd X et $-X$ ne le sont pas. En suivant l'argument précédent, on tombe effectivement sur un homomorphisme non trivial $\varepsilon\colon G \to A^\times$. (Cet exemple répond essentiellement à la question 4.4.)

3.3. (a) Le sous-anneau des polynômes symétriques dans $\mathbb{Z}[X_1, \ldots, X_n]$ est une $\mathbb{Z}$-algèbre libre sur $\sigma_{1,n}, \ldots, \sigma_{n,n}$. Par conséquent, le pgcd de $\sigma_{k,n}$ et $\sigma_{l,n}$ dans $\mathbb{Z}[\sigma_{1,n}, \ldots, \sigma_{n,n}]$ vaut 1. Utilisant le résultat précédent, leur pgcd dans $\mathbb{Z}[X_1, \ldots, X_n]$ vaut également 1.

(b) Pour $k < n$ on a $\sigma_{k,n} = \sigma_{k-1,n-1}X_n + \sigma_{k,n-1}$. Par rapport à X_n ce polynôme est donc de contenu $\operatorname{pgcd}(\sigma_{k-1,n-1}, \sigma_{k,n-1}) = 1$.

(c) Pour $k < n$ le polynôme $\sigma_{k,n}$ est de contenu 1 et de degré 1 en X_n ; il est donc irréductible dans $\mathbb{Z}[X_1, \ldots, X_n]$. Par contre $\sigma_{n,n} = X_1 X_2 \cdots X_n$ se décompose en les n facteurs irréductibles évidents : $X_1, X_2, \ldots, X_n$.

4. ACTION ET CORPS DES FRACTIONS

4.1. On a $\frac{a}{b} = \frac{c}{d}$ si et seulement si $ad = bc$. Comme G agit par automorphismes d'anneau on a $a^g d^g = b^g c^g$ donc $\frac{a^g}{b^g} = \frac{c^g}{d^g}$. Ceci montre que l'action est bien définie sur $\operatorname{Frac}(A)$.

On a $0^g = 0$ et $1^g = 1$ dans A, donc aussi dans $\mathrm{Frac}(A)$. On vérifie que

$$\Big(\frac{a}{b} \pm \frac{c}{d}\Big)^g = \Big(\frac{ad \pm cb}{bd}\Big)^g = \frac{a^g d^g \pm c^g b^g}{b^g d^g} = \frac{a^g}{b^g} \pm \frac{c^g}{d^g} = \Big(\frac{a}{b}\Big)^g \pm \Big(\frac{c}{d}\Big)^g,$$

$$\Big(\frac{a}{b} \cdot \frac{c}{d}\Big)^g = \Big(\frac{ac}{bd}\Big)^g = \frac{a^g c^g}{b^g d^g} = \frac{a^g}{b^g} \cdot \frac{c^g}{d^g} = \Big(\frac{a}{b}\Big)^g \cdot \Big(\frac{c}{d}\Big)^g.$$

Il s'agit donc bien d'une action par automorphismes de corps.

Remarque : C'est la seule prolongation possible d'une action $A \times G \to G$ à une action sur $\mathrm{Frac}(A)$ par automorphismes : comme $\frac{a}{b} \cdot b = a$ on a $\big(\frac{a}{b}\big)^g \cdot b^g = a^g$, donc $\big(\frac{a}{b}\big)^g = \frac{a^g}{b^g}$.

4.2. Les éléments de $\mathrm{Frac}(A^G)$ sont les fractions $\frac{a}{b}$ avec $a, b \in A^G$, $b \neq 0$. Évidemment on a $\big(\frac{a}{b}\big)^g = \frac{a^g}{b^g} = \frac{a}{b}$, donc $\frac{a}{b} \in \mathrm{Frac}(A)^G$. Réciproquement soit $\frac{x}{y} \in \mathrm{Frac}(A)^G$, c'est-à-dire $x, y \in A$, $y \neq 0$, tels que $\frac{x^g}{y^g} = \frac{x}{y}$ pour tout $g \in G$. On ne peut pas conclure que $x^g = x$ et $y^g = y$, seulement que $x^g y = x y^g$ pour tout $g \in G$. Si G est fini, par contre, on a $\frac{x}{y} = \frac{a}{b}$ avec $a = x \prod_{g \in G, g \neq 1} y^g$ et $b = y \prod_{g \in G, g \neq 1} y^g$. Par construction b est G-invariant, c'est-à-dire $b \in A^G$. Par conséquent $a = \frac{x}{y} b$ aussi est G-invariant, c'est-à-dire $a \in A^G$. On conclut, pour G fini, que $\mathrm{Frac}(A)^G = \mathrm{Frac}(A^G)$.

4.3. (a) Il existe un unique homomorphisme d'anneau $h \colon \mathbb{Q}[X, Y] \to \mathbb{Q}[X, Y]$ vérifiant $X^h = \frac{1}{2}X$ et $Y^h = \frac{1}{2}Y$. On a $X^{gh} = X$ et $Y^{gh} = Y$, donc $gh = \mathrm{id}$. Inversement, $X^{hg} = X$ et $Y^h g = Y$, donc $hg = \mathrm{id}$.

(b) Soit $P = \sum_{i=0}^n P_i$ avec $P_i \in \mathbb{Q}[X, Y]$ homogène de degré i et $P_n \neq 0$. On a alors $P^g = \sum_{i=0}^n 2^i P_i$. La condition $P = P^g$ équivaut donc à $2^i P_i = P_i$ pour tout i. Ceci n'est possible que pour $n = 0$. Autrement dit, $\mathbb{Q}[X, Y]^G = \mathbb{Q}$.

(c) Il est clair que $\frac{P}{Q} \in \mathbb{Q}(X, Y)$ est G-invariant si P et Q sont deux polynômes homogènes de même degré n : dans ce cas $\frac{P^g}{Q^g} = \frac{2^n P}{2^n Q} = \frac{P}{Q}$.

Pour montrer la réciproque, considérons $\frac{P}{Q} \in \mathbb{Q}(X, Y)^G$. On décompose $P = \sum_{i=0}^n P_i$ et $Q = \sum_{j=0}^m Q_j$ en sommes de polynômes homogènes avec $\deg(P_i) = i$ et $\deg(Q_j) = j$, telles que $P_n \neq 0$ et $Q_m \neq 0$. La condition $\frac{P^g}{Q^g} = \frac{P}{Q}$ veut dire que

$$\Big(\sum_{i=0}^n 2^i P_i\Big)\Big(\sum_{j=0}^m Q_j\Big) = \Big(\sum_{i=0}^n P_i\Big)\Big(\sum_{j=0}^m 2^j Q_j\Big).$$

En comparant les termes dominants, on trouve $2^n P_n Q_m = 2^m P_n Q_m$, ce qui implique déjà $n = m$. Trivialement $\big(\frac{P}{Q}\big)^g = \frac{P}{Q}$ implique que $\lim_{k \to \infty} \big(\frac{P}{Q}\big)^{g^k} = \frac{P}{Q}$. D'un autre coté, $\big(\frac{P}{Q}\big)^{g^k} = \frac{\sum_{i=0}^n 2^{ki} P_i}{\sum_{i=0}^n 2^{ki} Q_i} = \frac{\sum_{i=0}^n 2^{k(i-n)} P_i}{\sum_{i=0}^n 2^{k(i-n)} Q_i}$, donc $\lim_{k \to \infty} \big(\frac{P}{Q}\big)^{g^k} = \frac{P_n}{Q_n}$. Ceci prouve que $\frac{P}{Q} = \frac{P_n}{Q_n}$ est une fraction de deux polynômes homogènes de même degré n.

Avertissement : Il n'est pas vrai que $\frac{P}{Q} \in \mathbb{Q}(X, Y)^G$ est forcément formé de numérateur et dénominateur homogènes de degré n. Par exemple $\frac{X^2+X}{XY+Y}$ est bien G-invariant. D'après l'argument précédent il est équivalent à $\frac{X^2}{XY} = \frac{X}{Y}$; effectivement $\frac{X^2+X}{XY+Y} = \frac{X(X+1)}{Y(X+1)} = \frac{X}{Y}$.

Remarque : Cet exemple montre que, pour un groupe G de cardinal infini, $\mathrm{Frac}(A^G)$ peut différer de $\mathrm{Frac}(A)^G$: dans notre exemple $\frac{X}{Y} \in \mathrm{Frac}(A)^G$, mais $\frac{X}{Y} \notin \mathrm{Frac}(A^G) = \mathbb{Q}$.

4.4. Considérons $A = \mathbb{Q}[X, Y]$ avec $g \colon A \to A$ donné par $X^g = -X$ et $Y^g = -Y$. Évidemment $g^2 = \mathrm{id}$, donc $G = \langle g \rangle$ est d'ordre 2. Les polynômes X^2 et XY sont G-invariants, il en est donc de même pour la fraction $\frac{X^2}{XY} \in \mathbb{Q}(X, Y)$. La fraction réduite $\frac{uX}{uY}$ avec $u \in \mathbb{Q}^\times$ représente le même élément G-invariant, mais numérateur et dénominateur ne sont pas G-invariants.

Feuille C1 — EXTENSIONS ET AUTOMORPHISMES

Résumé. On analysera quelques extensions du corps $\mathbb{Q}$ par des méthodes élémentaires, c'est-à-dire sans la théorie de Galois, pour illustrer les notions de degré et du groupe d'automorphismes.

1. EXTENSIONS ALGÉBRIQUES ET NON ALGÉBRIQUES

1.1. Soient $\alpha = \sqrt{7}$ et $\beta = 1 + \sqrt{7}$. Vérifier que $\mathrm{Irr}_{\mathbb{Q}}(\alpha) \neq \mathrm{Irr}_{\mathbb{Q}}(\beta)$ mais $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

1.2. Soient $\alpha = \sqrt[3]{7}$ et $\beta = j\sqrt[3]{7}$. Vérifier que $\mathrm{Irr}_{\mathbb{Q}}(\alpha) = \mathrm{Irr}_{\mathbb{Q}}(\beta)$ mais $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.
Les deux extensions sont-elles isomorphes ? Comment construire un isomorphisme ?

1.3. Les extensions $\mathbb{Q}(\sqrt{7})$ et $\mathbb{Q}(\sqrt{11})$ sont-elles isomorphes ?

1.4. Montrer que toute extension $E|\mathbb{Q}$ de degré 2 est de la forme $E = \mathbb{Q}(\sqrt{a})$.

1.5. Quelles sont les extensions algébriques de $\mathbb{C}$? de $\mathbb{R}$?
Donner des exemples d'extensions non algébriques de $\mathbb{C}$ et de $\mathbb{R}$.

1.6. Est-ce que toute extension finie est algébrique ? Est-ce que toute extension algébrique est finie ? La clôture algébrique de $\mathbb{Q}$ est-elle de dimension finie sur $\mathbb{Q}$?

1.7. Soient $E \supset L \supset K$ trois corps. Quel est le rapport entre $[E : L]$ et $[L : K]$ et $[E : K]$?
Si les extensions $E|L$ et $L|K$ sont algébriques, est-ce que $E|K$ est algébrique ?

1.8. En admettant que e (ou π) est transcendant sur $\mathbb{Q}$, montrer qu'il est transcendant sur toute extension algébrique de $\mathbb{Q}$. Est-il transcendant ou algébrique sur $\mathbb{R}$?

1.9. ★ Montrer que la clôture algébrique $\bar{\mathbb{Q}}$ dans $\mathbb{C}$ est un ensemble dénombrable. En déduire qu'il existe dans $\mathbb{R}$ des éléments transcendants sur $\mathbb{Q}$. Si l'on choisit un élément $x \in [0, 1]$ au hasard, il est transcendant avec probabilité 1.

2. CORPS DE RUPTURE ET CORPS DE DÉCOMPOSITION

Soit K un corps et $P \in K[X]$ un polynôme de degré $n \geq 1$. On dit qu'une extension E de K est un *corps de rupture de* P si $E = K(x)$ avec $P(x) = 0$. On dit que E est un *corps de décomposition de* P s'il existe $x_1, \ldots, x_n \in E$ tels que $P = a(X - x_1) \cdots (X - x_n)$ et $E = K(x_1, \ldots, x_n)$.

2.1. Pour $X^2 - 2$ sur $\mathbb{Q}$ trouver les corps de ruptures dans $\mathbb{C}$. Sont-ils égaux ?
Expliciter le corps de décomposition E dans $\mathbb{C}$ et préciser une base de E sur $\mathbb{Q}$.

2.2. Pour $(X^2 - 2)(X^2 - 3)$ sur $\mathbb{Q}$ expliciter les corps de rupture dans $\mathbb{C}$. Sont-ils isomorphes ?
Expliciter le corps de décomposition E dans $\mathbb{C}$, trouver $|E : \mathbb{Q}|$ et préciser une base.

2.3. Montrer que $X^3 - 2$ sur $\mathbb{Q}$ admet trois corps de rupture distincts dans $\mathbb{C}$. Sont-ils isomorphes ?
Expliciter le corps de décomposition dans $\mathbb{C}$ et en préciser une $\mathbb{Q}$-base.

2.4. Vérifier que le polynôme $P = X^3 - 3X - 1$ est irréductible sur $\mathbb{Q}$, et qu'il a trois racines réels.
Soit $\alpha \in \mathbb{R}$ une racine. Sur $\mathbb{Q}(\alpha)$ vérifier la factorisation $P = (X - \alpha)(X^2 + \alpha X + \alpha^2 - 3) = (X - \alpha)(X + \frac{\alpha+1}{\alpha})(X + \frac{1}{\alpha+1})$. Conclure que $\mathbb{Q}(\alpha)$ est un corps de décomposition de P.

2.5. Montrer que $E = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps de décomposition de $X^4 + 2$ sur $\mathbb{Q}$.
Montrer que E est aussi le corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$.
Trouver le degré $|E : \mathbb{Q}|$ et expliciter une base de E sur $\mathbb{Q}$.

3. EXTENSIONS ET AUTOMORPHISMES

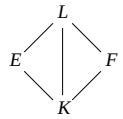
Pour un corps E on note $\mathrm{Aut}(E)$ le groupe des automorphismes de E. Pour tout sous-corps K on peut considérer E comme une extension de K, notée $E|K$. Dans ce cas on note $\mathrm{Aut}_K(E)$ ou $\mathrm{Aut}(E|K)$ le groupe des automorphismes $\phi\colon E \to E$ vérifiant $\phi(k) = k$ pour tout $k \in K$.

3.1. Déterminer $\mathrm{Aut}(\mathbb{C}|\mathbb{R})$ et $\mathrm{Aut}(\mathbb{Q}(i)|\mathbb{Q})$ et $\mathrm{Aut}(\mathbb{Q}(j)|\mathbb{Q})$, puis $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$.

3.2. Déterminer $\mathrm{Aut}(E|\mathbb{Q})$ pour $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, puis $\mathbb{Q}(j, \sqrt[3]{2})$, puis $\mathbb{Q}(i, \sqrt[4]{2})$.

3.3. Déterminer $G = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$. On a $|G| < |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$? Ce n'est pas normal…

4. Composé de deux extensions



4.1. On considère les extensions $E = \mathbb{Q}(i)$ et $F = \mathbb{Q}(\sqrt[3]{2})$ puis $L = \mathbb{Q}(\sqrt[3]{2}, i)$ de $K = \mathbb{Q}$. Déterminer leur degré suivant le schéma à droite. En déduire que $X^3 - 2$ est irréductible sur $\mathbb{Q}(i)$.

4.2. Plus généralement, soient $E|K$ une extension de degré m et $P \in K[X]$ un polynôme irréductible de degré n. Si $\mathrm{pgcd}(m, n) = 1$, alors P est irréductible dans $E[X]$.

4.3. Le polynôme $X^3 + 3$ est-il irréductible dans $\mathbb{Q}(\sqrt{3})[X]$?
Et $X^5 + 3X^3 - 9X + 6$ dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})[X]$?
Puis $X^2 + 2$ dans $\mathbb{Q}(\sqrt{2})[X]$?

5. Automorphismes de $\mathbb{R}$

On se propose ici de contempler $\mathrm{Aut}(\mathbb{R})$. Remarquons d'abord que l'ordre $\leq$ sur le corps $\mathbb{R}$ admet une description purement algébrique : la propriété $x \geq 0$ équivaut à l'existence d'un élément $r \in \mathbb{R}$ tel que $r^2 = x$.

5.1. Soit $\phi : \mathbb{R} \to \mathbb{R}$ un automorphisme. Traiter d'abord la question de savoir si $\mathbb{Q}$ est fixé. Montrer ensuite que tout réel $x \geq 0$ vérifie $\phi(x) \geq 0$, et en déduire que ϕ est un application croissante. Conclure que $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$. Qu'en pensez-vous ?

Avertissement : On a vu que $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\}$ et $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$. On pourrait être tenté de conclure que $\mathrm{Aut}(\mathbb{C}) = \{\mathrm{id}, \mathrm{conj}\}$. Le problème est qu'un automorphisme de $\mathbb{C}$ ne fixe pas forcément le sous-corps $\mathbb{R}$; c'est incroyable mais vrai ! En effet, le groupe $\mathrm{Aut}(\mathbb{C})$ est infini, même non dénombrable. Avouons que c'est un théorème d'existence seulement. Personne n'a jamais vu un automorphisme de $\mathbb{C}$ outre l'identité et la conjugaison.

5.2. Voici une variante du même phénomène, encore plus jolie, qui produit une extension algébrique : Pour tout $n \in \mathbb{N}$, $n \geq 1$, on note $\sqrt[n]{3}$ la racine réelle positive de $X^n - 3$. Vérifier que l'ensemble $K = \bigcup_{n \geq 1} \mathbb{Q}(\sqrt[n]{3})$ est un sous-corps de $\mathbb{R}$. Montrer que $K|\mathbb{Q}$ est une extension algébrique. (Est-elle finie ?) Déterminer les automorphismes de K.

La morale de cette histoire : Pour une extension de corps $K \supset L \supset \mathbb{Q}$, bien que K soit plus grand que L, il se peut que $\mathrm{Aut}(K|\mathbb{Q})$ soit plus petit que $\mathrm{Aut}(L|\mathbb{Q})$. Pour vous réconforter : on verra qu'une extension finie $E|F$ qui est *galoisienne* a toujours le bon goût de vérifier $|\mathrm{Aut}(E|F)| = |E : F|$. Donc tout va bien.

Feuille C2 — CORPS FINIS

Résumé. Cette feuille d'exercices présente la classification des corps finis : (1) Tout corps fini est de cardinal p^n avec p premier et $n \geq 1$. (2) Pour tout tel couple (p, n) il existe un corps de cardinal p^n. (3) Deux corps de cardinal p^n sont isomorphes. *Nota bene :* une bonne partie des questions est une révision du cours et ne sera pas discutée en TD (sauf demande motivée).

1. Exemples de corps finis

Avant toute théorie, regardons deux exemples concrets. D'abord un corps de cardinal 4 :

1.1. Vérifier que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$; c'est en fait le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$. Le quotient $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2+X+1)$ est un corps de cardinal 4. Comme $\mathbb{F}_2$-base on peut choisir $(1, x)$ où x est l'image de X dans $\mathbb{F}_4$. Dans cette base la multiplication est donnée par

$$(\alpha + \beta x)(\alpha' + \beta' x) = (\alpha\alpha' + \beta\beta') + (\alpha\beta' + \beta\alpha' + \beta\beta')x$$

Convainquez-vous qu'il n'est pas évident de partir de telles formules « tombées du ciel » pour ensuite établir qu'il s'agit bien d'un corps. On préférera toujours la construction par quotient, et on verra que tout corps fini se construit ainsi.

1.2. Vérifier que $P = X^3 + X + 1$ est irréductible sur $\mathbb{F}_5$, donc $E = \mathbb{F}_5[X]/(P)$ est un corps de cardinal 125. Expliciter une $\mathbb{F}_5$-base de E et, si vous voulez, la loi de multiplication.
Vérifier que $Q = Y^3 + 2Y^2 - Y + 2$ est aussi irréductible sur $\mathbb{F}_5$. On obtient ainsi un deuxième corps $F = \mathbb{F}_5[Y]/(Q)$ de cardinal 125. Est-il isomorphe à E ? Peut-on expliciter un isomorphisme ? *Indication :* Notons x l'image de X dans E. Vérifier que $x^2 - x$ annule Q.

2. Structures additive et multiplicative d'un corps fini

Dans ce paragraphe on suppose donné un corps fini à q éléments. On le note $\mathbb{F}_q$.

2.1. Montrer qu'il existe un nombre premier p et un sous-corps $K < \mathbb{F}_q$ isomorphe à $\mathbb{F}_p$.
Pour simplifier, on identifie K à $\mathbb{F}_p$, c.-à-d. on considère $\mathbb{F}_p$ comme sous-corps de $\mathbb{F}_q$.

2.2. Regardons la structure additive de $\mathbb{F}_q$: Montrer qu'il existe un entier $n \geq 1$ de sorte que $(\mathbb{F}_q, +)$ soit isomorphe à $(\mathbb{F}_p^n, +)$. En particulier le cardinal vaut $q = p^n$.

2.3. Quant à la structure multiplicative, redémontrer que le groupe $(\mathbb{F}_q^\times, \cdot)$ est cyclique d'ordre $p^n - 1$. En déduire que tout élément $x \in \mathbb{F}_q$ annule le polynôme $X^q - X$.

2.4. Montrer que $\prod_{a \in \mathbb{F}_q}(X - a) = X^q - X$. C'est un fait très remarquable : $X^q - X$ admet q racines distinctes dans $\mathbb{F}_q$; tout élément de $\mathbb{F}_q$ y figure comme racine simple.

2.5. Voici un argument qui ne suppose pas l'existence d'un corps $\mathbb{F}_q$: Calculer le discriminant de $X^q - X$ dans $\mathbb{F}_p[X]$. Conclure que $X^q - X$ est sans facteurs carrés.

3. Polynômes irréductibles sur $\mathbb{F}_p$

3.1. Soit $I_p^n \subset \mathbb{F}_p[X]$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$.
Si $P \in I_p^n$ alors $\mathbb{F}_p[X]/(P)$ est un corps de cardinal p^n, donc P divise $X^{p^n} - X$.

3.2. Montrer que le pgcd de $X^{p^m} - X$ et $X^{p^n} - X$ vaut $X^{p^d} - X$ où $d = \operatorname{pgcd}(m, n)$.
En particulier, $X^{p^m} - X$ divise $X^{p^n} - X$ si et seulement si m divise n.
Indication : Montrer que $m = an + b$ entraîne $X^{p^m} \equiv X^{p^b}$ modulo $X^{p^n} - X$.

3.3. Dans $\mathbb{F}_p[X]$ établir la décomposition primaire $X^{p^n} - X = \prod_{d|n} \prod_{P \in I_p^d} P$. En déduire la formule $p^n = \sum_{d|n} d \cdot |I_p^d|$. Expliciter $|I_p^n|$ pour $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots$.

3.4. Montrer l'estimation $\frac{1}{n}\left(p^n - 2p^{n/2}\right) \leq |I_p^n| \leq \frac{1}{n}p^n$. En particulier, la probabilité qu'un polynôme $P \in \mathbb{F}_p[X]$ de degré n soit irréductible est proche de $\frac{1}{n}$.

3.5. Montrer qu'un polynôme $P \in \mathbb{F}_p[X]$ de degré n est irréductible si et seulement si $X^{p^n} \equiv X$ modulo P et $\operatorname{pgcd}(X^{p^{n/t}} - X, P) = 1$ pour tout diviseur premier $t \mid n$.

4. Existence et unicité des corps finis

4.1. *Existence :* Montrer que pour tout premier $p \geq 2$ et $n \geq 1$, il existe un polynôme unitaire irréductible $P \in \mathbb{F}_p[X]$ de degré n, donc un corps $\mathbb{F}_p[X]/(P)$ de cardinal p^n.

Unicité : Pour tout corps $\mathbb{F}_q$ de cardinal $q = p^n$, montrer qu'il existe $x \in \mathbb{F}_q$ qui a P pour polynôme minimale sur $\mathbb{F}_p$. Construire ainsi un isomorphisme $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_q$.

Existence et unicité peuvent se déduire de manière encore plus élégante :

4.2. *Unicité :* Si $\mathbb{F}_q$ est un corps de cardinal $q = p^n$, alors il est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. Deux corps de décomposition du même polynôme sont isomorphes.

Existence : Il existe un corps K de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. Comme l'ensemble $\{x \in K \mid x^{p^n} = x\}$ est un sous-corps, le cardinal de K est exactement p^n.

5. Exemple : le polynôme $X^4 + 1$ reconsidéré

5.1. Rappeler que le polynôme $P = X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{F}_2$.

On se propose de montrer que P est réductible sur tout corps $\mathbb{F}_p$ avec $p \geq 3$ premier.

5.2. Montrer que 8 divise $p^2 - 1$ et en déduire qu'il existe $\alpha \in \mathbb{F}_{p^2}$ tel que $\alpha^4 = -1$.

5.3. Conclure que P admet une racine dans $\mathbb{F}_{p^2}$, puis que P est réductible sur $\mathbb{F}_p$.

5.4. Décomposer $X^4 + 1$ en polynômes irréductibles de $\mathbb{F}_p[X]$ pour $p = 2, 3, 5, 7, 11$.

6. Automorphismes d'un corps fini

6.1. Soit K un corps de caractéristique p. Montrer que l'application de Frobenius $f\colon K \to K$ donnée par $f(x) = x^p$ est un homomorphisme de corps. En particulier f est injectif.

6.2. Pour un corps fini, l'homomorphisme de Frobenius est forcément un automorphisme. Attention, ceci peut être faux pour un corps infini ! Discuter l'exemple $K = \mathbb{F}_p(X)$.

6.3. Soit désormais $\mathbb{F}_q$ un corps de cardinal $q = p^n$. Vérifier que f est d'ordre n dans $Aut(\mathbb{F}_q)$. Montrer que $\mathrm{Aut}(\mathbb{F}_q)$ est cyclique d'ordre n, engendré par f. *Indication :* Regarder un générateur x de $\mathbb{F}_q^\times$ et son polynôme minimal sur $\mathbb{F}_p$.

6.4. Quel est le sous-corps fixé par $\mathrm{Aut}(\mathbb{F}_q)$? Étant donné $x \in \mathbb{F}_q$ notons $x_1, x_2, \ldots, x_d$ son orbite sous l'action de $\mathrm{Aut}(\mathbb{F}_q)$. (Remarquer que $d|n$.) Que peut-on dire du polynôme $(X - x_1)(X - x_2)\cdots(X - x_d)$? En déduire le nombre d'orbites de longueur d.

7. Clôture algébrique de $\mathbb{F}_p$

Soit p un nombre premier. On se propose ici de construire une clôture algébrique de $\mathbb{F}_p$.

7.1. Soit K un corps à p^r éléments. Montrer que K contient un sous-corps L à p^s éléments si et seulement si s divise r. Dans ce cas $L < K$ est le seul sous-corps à p^s éléments.

Pour tout $n \in \mathbb{N}$ soit désormais E_n un corps à $p^{n!}$ éléments, commençant par $E_1 = \mathbb{F}_p$.
Par le résultat précédent, E_n contient exactement un sous-corps isomorphe à E_{n-1}.
En identifiant les corps correspondants, on peut supposer que $E_1 < E_2 < E_3 < \ldots$.

7.2. Montrer que la réunion $C := \bigcup_n E_n$ est un corps de façon naturelle.
Pour tout $r \geq 1$ le corps C contient exactement un sous-corps à p^r éléments.
Conclure que C est une clôture algébrique de $\mathbb{F}_p$.

Remarque. Pour rendre la notation unique, on peut fixer une fois pour toute une clôture algébrique C de $\mathbb{F}_p$. On peut ensuite définir $\mathbb{F}_{p^r}$ comme étant l'unique sous-corps de C de cardinal p^r. On obtient ainsi l'inclusion $\mathbb{F}_{p^s} < \mathbb{F}_{p^r}$ pour tout $s \mid r$, puis on retrouve $C = \bigcup_r \mathbb{F}_{p^r}$.

7.3. Soit C une clôture algébrique de $\mathbb{F}_p$. Est-ce l'homomorphisme de Frobenius $f\colon x \mapsto x^p$, est un automorphisme de C ? Quel est son ordre ? Est-ce que f engendre $\mathrm{Aut}(C)$? Quelle est la structure de du groupe $\mathrm{Aut}(C)$?

Feuille C3 — RÉCIPROCITÉ QUADRATIQUE

Résumé. Étant donné un nombre premier impair $p \geq 3$, on dit que $a \in \mathbb{Z}$ est un *résidu quadratique* ou *carré modulo* p s'il existe $r \in \mathbb{Z}$ tel que $r^2 \equiv a \pmod p$. Les exercices qui suivent ont pour but d'étudier les résidus quadratiques. On montrera en particulier la célèbre loi de réciprocité quadratique de Gauss, un bijou de la théorie des nombres.

1. SYMBOLE DE LEGENDRE ET CRITÈRE D'EULER

Soit $p \geq 3$ un nombre premier impair. Pour $a \in \mathbb{Z}$ on note $\bar a \in \mathbb{F}_p$ sa réduction modulo p. On définit alors le *symbole de Legendre* de a modulo p par

$$\left(\frac{a}{p}\right) = \left(\frac{\bar a}{p}\right) = \begin{cases} +1 & \text{si } \bar a \in \mathbb{F}_p^\times \text{ est un carré,} \\ -1 & \text{si } \bar a \in \mathbb{F}_p^\times \text{ n'est pas un carré,} \\ 0 & \text{si } \bar a = 0. \end{cases}$$

1.1. Déterminer $\left(\frac{5}{7}\right)$ et $\left(\frac{7}{5}\right)$ puis $\left(\frac{7}{11}\right)$ et $\left(\frac{11}{7}\right)$. Reconaissez-vous déjà un rapport ?

1.2. Le polynôme $X^2 + aX + b \in \mathbb{F}_p[X]$ admet exactement $1 + \left(\frac{a^2-4b}{p}\right)$ racines dans $\mathbb{F}_p$. Combien de racines admet-il dans $\mathbb{F}_{p^2}$?.

1.3. Soit g un générateur de $\mathbb{F}_p^\times$. Montrer que $\bar a$ est un carré dans $\mathbb{F}_p^\times$ si et seulement s'il est une puissance paire de g. En déduire le critère d'Euler : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

1.4. Vérifier que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ et $\left(\frac{1}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, puis $\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) = 0$.

2. LA LOI DE RÉCIPROCITÉ QUADRATIQUE

Théorème 4. *Soient $p, q \geq 3$ deux nombres premiers. Alors on a la formule de réciprocité*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot \varepsilon(p,q) \quad \textit{avec} \quad \varepsilon(p,q) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} +1 & \textit{si } p \equiv 1 \textit{ ou } q \equiv 1 \pmod 4, \\ -1 & \textit{si } p \equiv 3 \textit{ et } q \equiv 3 \pmod 4. \end{cases}$$

Pour le cas exceptionnel $q = 2$ et $p \geq 3$ impair on a la formule complémentaire

$$\left(\frac{2}{p}\right) = \delta(p) \quad \textit{avec} \quad \delta(p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \textit{si } p \equiv \pm 1 \pmod 8, \\ -1 & \textit{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

2.1. Vérifier la réciprocité pour $\left(\frac{5}{7}\right)$ et $\left(\frac{7}{5}\right)$ et $\varepsilon(5,7)$. Même exercice avec $\left(\frac{7}{11}\right)$ et $\left(\frac{11}{7}\right)$ et $\varepsilon(7,11)$. Vérifier la formule complémentaire pour $\left(\frac{2}{3}\right)$ et $\left(\frac{2}{5}\right)$ puis $\left(\frac{2}{7}\right)$ et $\left(\frac{2}{17}\right)$.

On se propose de montrer la loi de réciprocité en passant par les corps finis.

2.2. Montrer que $\mathbb{F}_{p^2}$ contient une racine primitive huitième de l'unité. On la note ζ et on pose $r = \zeta + \zeta^{-1}$. Calculer r^2 puis r^p. En déduire $\left(\frac{2}{p}\right)$ suivant les valeurs de $p \bmod 8$.

2.3. Afin de montrer la formule principale, on suppose que p et q sont deux nombres premiers impaires distincts. Soient $\zeta \in \bar{\mathbb{F}}_p$ une racine primitive q-ième de l'unité et $r = \sum_{k\in\mathbb{F}_q^\times} \left(\frac{k}{q}\right)\zeta^k$.

(a) Montrer que $r^2 = (-1)^{\frac{q-1}{2}} \sum_{m\in\mathbb{F}_q} \zeta^m \sum_{k\in\mathbb{F}_q^\times} \left(\frac{1-mk^{-1}}{q}\right)$.

(b) Montrer que $\sum_{k\in\mathbb{F}_q^\times} \left(\frac{1-mk^{-1}}{q}\right) = \begin{cases} -1 & \text{si } m \neq 0, \\ q-1 & \text{si } m = 0. \end{cases}$

(c) En déduire que $r^2 = (-1)^{\frac{q-1}{2}} q$.

(d) Montrer que $r^p = \left(\frac{p}{q}\right) r$, donc $r^{p-1} = \left(\frac{p}{q}\right)$.

Conclure que $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

2.4. Déterminer si 30 est un carré dans $\mathbb{F}_{65537}$. (On admet que $65537 = 2^{2^4} + 1$ est premier.) Et 20 est-il un carré dans $\mathbb{F}_{65537}$? Est-il aussi facile de trouver une racine, le cas échéant ?

2.5. Justifions finalement ce qui a été tacitement admis : l'existence des racines primitives dans $\bar{\mathbb{F}}_p$, la clôture algébrique de $\mathbb{F}_p$. Expliquer pourquoi le groupe des racines p-ièmes de l'unité dans $\bar{\mathbb{F}}_p$ est trivial. Pour $p \nmid q$, par contre, les racines q-ièmes de l'unité dans $\bar{\mathbb{F}}_p$ forment un groupe cyclique d'ordre q, comme il se doit.

2.6. Dans $\mathbb{C}$ on note $\zeta_n = e^{2\pi i/n}$ comme avant. On a déjà à vu l'aide du discriminant que $\sqrt{q} \in \mathbb{Q}[\zeta_q]$ si $q \equiv 1 \pmod 4$, et $\sqrt{q} \in \mathbb{Q}[\zeta_{4q}]$ si $q \equiv 3 \pmod 4$. Vous pouvez en donner une preuve alternative en explicitant $\sqrt{q}$ à l'aide du symbole de Legendre.

3. Symbole de Jacobi

Le symbole de Legendre $\left(\frac{a}{p}\right)$ n'est défini que pour les nombres premiers $p \geq 3$. On l'étend aux nombres composés par multiplicativité : pour $b \geq 1$ impair on définit le *symbole de Jacobi* par $\left(\frac{a}{b}\right) := \prod_i \left(\frac{a}{p_i}\right)^{e_i}$ où $b = \prod_i p_i^{e_i}$ est la décomposition primaire de b. Autrement dit :

$$\left(\frac{a}{1}\right) = 1 \qquad \text{et} \qquad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

3.1. Montrer que $\left(\frac{a}{b}\right) = 0$ ssi $\operatorname{pgcd}(a,b) > 1$. Justifier les règles de calcul suivantes :

① $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$ et $\left(\frac{1}{b}\right) = 1$

② $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$ si $a \equiv a' \pmod b$

③ $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \cdot \varepsilon(a,b)$ si a et b sont impairs

④ $\left(\frac{2}{b}\right) = \delta(b)$

Indication : Par définition il faut passer par la décomposition primaire de b, et dans ③ il faudra aussi la décomposition de a. Pour ④ montrer d'abord que δ est multiplicatif, et pour ③ que ε est multiplicatif en chaque argument.

3.2. Calculer la valeur de $\left(\frac{71}{83}\right)$ en utilisant les règles ci-dessus.

3.3. Soit $a = 13\,353\,839$ et admettons que $p = 64a + 3$ est premier. Existe-t-il une solution $x, y \in \mathbb{Z}$ à l'équation $x^2 + yp = 4a$? Même question pour l'équation $x^2 + yp = 8a$. (Tout le calcul est faisable à la main.)

4. Nombres de Fermat et critère de Pépin

Fermat constata que la suite $F_n = 2^{2^n} + 1$ commence par cinq nombres premiers : $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Il conjectura ensuite que $F_n = 2^{2^n} + 1$ est premier pour tout n. Cent ans plus tard, Euler trouva la décomposition $F_5 = 4294967297 = 641 \cdot 6700417$. Ceci a provoqué deux questions, toujours largement ouvertes : lesquels des nombres F_n sont premiers, et quant aux autres, quelle est leur décomposition primaire ?

À noter que les nombres de Fermat croissent rapidement : déjà F_5 a 10 chiffres. De plus, F_{n+1} est à peu près le carré de F_n, donc le nombre des chiffres double si l'on augmente n. Il est très difficile de factoriser des entiers à quelques centaines de chiffres, même à nos jours avec les ordinateurs les plus puissants. Par contre, on présentera dans la suite un algorithme efficace pour décider si un nombre de Fermat $F_n = 2^{2^n} + 1$ avec $n \geq 1$ est premier ou non.

4.1. Commençons par un critère suffisant. Soit $N = 2^k + 1$ et supposons que $a \in \mathbb{Z}_N$ vérifie $a^{2^{k-1}} = -1$. Déterminer l'ordre de a dans $\mathbb{Z}_N^\times$. Conclure que N est premier.

4.2. Calculer $\left(\frac{F_n}{3}\right)$ puis $\left(\frac{3}{F_n}\right)$ via réciprocité. En déduire le critère de Pépin : Pour $n \geq 1$ le nombre F_n est premier si et seulement si $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

Sur ordinateur on peut calculer $3^{\frac{F_n-1}{2}} \bmod F_n$ de manière efficace à l'aide d'une méthode dite « puissance dichotomique ». On a ainsi pu montrer, par des calculs sur machine, que F_n est composé pour $5 \leq n \leq 24$, le cas F_{24} n'ayant été résolu qu'en 2003. À noter que l'on sait ainsi prouver que F_{24} est composé, mais on ne connaît aucun de ses facteurs !

Feuille C4 — CORRESPONDANCE DE GALOIS

0.1. Énoncer avec précision la correspondance de Galois.

1. L'ACTION DU GROUPE DE GALOIS SUR LES RACINES

Supposons que P est un polynôme unitaire séparable sur un corps K. Soient $\mathscr{X} = \{x_1, \dots, x_n\}$ ses racines dans un clôture algébrique de K, et soit $E = K(\mathscr{X})$ son corps de décomposition.

1.1. Tout automorphisme $\phi \in \mathrm{Gal}(E|K)$ permute les éléments $x_1, \dots, x_n$ entre eux. On obtient ainsi un homomorphisme $\rho\colon \mathrm{Gal}(E|K) \to \mathrm{Sym}(\mathscr{X})$. Vérifier que ρ est injectif. En numérotant les racines on obtient ainsi un plongement $\mathrm{Gal}(E|K) \hookrightarrow S_n$.

1.2. Si P est irréductible, alors $\mathrm{Gal}(E|K)$ agit transitivement sur $\mathscr{X}$, càd pour tout $x_i, x_j \in \mathscr{X}$ il existe $\phi \in \mathrm{Gal}(E|K)$ de sorte que $\phi(x_i) = x_j$. Dans ce cas n divise l'ordre de $\mathrm{Gal}(E|K)$.

Étant donné P il est en général très difficile de déterminer son groupe $\mathrm{Gal}(P) = \mathrm{Gal}(E|K)$. Certes, $\mathrm{Gal}(P)$ va être isomorphe à un sous-groupe de S_n, mais si n est grand, les possibilités sont énormes. Les paragraphes suivants ne traitent que des exemples les plus faciles.

2. POLYNÔMES SYMÉTRIQUES VUS PAR LA THÉORIE DE GALOIS

Soit $E = \Bbbk(x_1, \dots, x_n)$ le corps des fractions rationnelles dans les indéterminées $x_1, \dots, x_n$ sur un corps $\Bbbk$. Le groupe symétrique S_n agit sur E par permutation des variables, et on note $K = \Bbbk(x_1, \dots, x_n)^{S_n}$ le corps des invariants. C'est le corps des fractions rationnelles dans les polynômes symétriques élémentaires, c'est-à-dire $K = \Bbbk(s_1, \dots, s_n)$.

2.1. Trouver $P \in K[T]$ unitaire de degré n ayant pour racines $\mathscr{X} = \{x_1, \dots, x_n\}$.
Montrer que la restriction $\rho\colon \mathrm{Gal}(E|K) \to \mathrm{Sym}(\mathscr{X})$ est un isomorphisme.

2.2. En utilisant la correspondance de Galois conclure que tout groupe fini se réalise comme groupe de Galois $\mathrm{Gal}(E|L)$ avec $E|L$ convenable.

3. CORRESPONDANCE DE GALOIS POUR LES CORPS FINIS

Soit E un corps à p^{rs} éléments et K le sous-corps à p^s éléments.

3.1. Expliquer pourquoi l'extension $E|K$ est galoisienne de degré r.
Quelles sont les extensions intermédiaires, càd les corps L avec $E > L > K$?

3.2. L'application de Frobenius $f\colon E \to E$, $f(x) = x^p$, est un automorphisme de E.
Vérifier que $f^s \in \mathrm{Gal}(E|K)$, c'est-à-dire f^s est un automorphisme de E fixant K.
Montrer que $\mathrm{ord}(f^s) = r$ et en déduire que $\mathrm{Gal}(E|K) = \langle f^s \rangle$.

3.3. Comparer les extensions intermédiaires de $E|K$ et les sous-groupes de $\mathrm{Gal}(E|K)$, et établir la correspondance de Galois dans ce cas. L'expliciter pour $\mathbb{F}_{4096}$ sur $\mathbb{F}_2$.

4. EXEMPLES DE LA CORRESPONDANCE DE GALOIS SUR $\mathbb{Q}$

On reprend ici quelques extensions $E|\mathbb{Q}$ déjà vues, pour illustrer la correspondance de Galois.

4.1. Commençons par $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, le corps de décomposition de $(X^2 - 2)(X^2 - 3)$.

(a) Déterminer la dimension de E sur $\mathbb{Q}$ et spécifier une $\mathbb{Q}$-base B.
Expliciter $\mathrm{Gal}(E|\mathbb{Q})$ avec son action sur E (en utilisant la base B).

(b) Vérifier que $\mathrm{Gal}(E|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Pour chaque sous-groupe $H < \mathrm{Gal}(E|\mathbb{Q})$ identifier le corps des invariants E^H. Existe-t-il d'autres extensions intermédiaires ?

4.2. À titre d'avertissement, considérons $E = \mathbb{Q}(\sqrt[3]{2})$ et $\mathrm{Aut}(E|\mathbb{Q})$. L'extension $E|\mathbb{Q}$ est-elle galoisienne ? La correspondance de Galois est-elle vérifiée ?

4.3. Rappeler que $E = \mathbb{Q}(j, \sqrt[3]{2})$ est le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. Traiter les questions de l'exercice 4.1 pour l'extension $E|\mathbb{Q}$ et vérifier que $\mathrm{Gal}(E|\mathbb{Q}) \cong S_3$. Déterminer ses 6 sous-groupes et noter ceux qui sont distingués. Expliciter tous les sous-corps de E et noter ceux qui sont normaux sur $\mathbb{Q}$.

4.4. Rappeler que $E = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$. Analyser l'extension $E|\mathbb{Q}$ comme ci-dessus et vérifier que $\mathrm{Gal}(E|\mathbb{Q})$ est isomorphe au groupe diédral D_4. Déterminer ses 10 sous-groupes et noter ceux qui sont distingués. Expliciter toutes les extensions intermédiaires et noter celles qui sont normales sur $\mathbb{Q}$.

5. Discriminant et groupe de Galois

On reprend la notation du §1. Il est commode d'identifier le groupe $\mathrm{Gal}(E|K)$ et son image dans $\mathrm{Sym}(\mathscr{X})$, càd on n'insiste pas sur la distinction entre un automorphisme $\phi \in \mathrm{Gal}(E|K)$ et la permutation $\phi|_{\mathscr{X}} \in \mathrm{Sym}(\mathscr{X})$ donnée par restriction. (Le justifier !) On obtient ainsi $\mathrm{Gal}(E|K) < \mathrm{Sym}(\mathscr{X})$. Dans ce paragraphe on développera un critère pour déterminer si $\mathrm{Gal}(E|K) < \mathrm{Alt}(\mathscr{X})$ ou non.

5.1. On considère l'élément $d = \prod_{i<j}(x_i - x_j)$ dans E. Pour tout $\phi \in \mathrm{Gal}(E|K)$ on a alors $\phi(d) = d \cdot \mathrm{sign}(\phi|_{\mathscr{X}})$, où $\mathrm{sign}(\phi|_{\mathscr{X}})$ est la signature de la permutation $\phi|_{\mathscr{X}}$.

Remarquons que $d^2 = \prod_{i<j}(x_i - x_j)^2 = \mathrm{Disc}(P)$. On ne sait en général pas calculer les racines $x_1, \ldots, x_n$ mais on sait très bien calculer le discriminant de P. Rappeler comment.

5.2. Vérifier que $d^2 \in K$. Si $\mathrm{Gal}(E|K) < \mathrm{Alt}(\mathscr{X})$ alors $d \in K$. Montrer l'implication réciproque sous l'hypothèse que la caractéristique de K est différente de 2.

Ce critère permet de déterminer si $\mathrm{Gal}(E|K)$ est contenu dans $\mathrm{Alt}(\mathscr{X})$ ou non : il suffit de savoir si $\mathrm{Disc}(P)$ admet une racine carrée dans K ou non.

5.3. Montrer que les polynômes $P = X^3 - 3X + 1$ et $Q = X^3 - 4X + 1$ sont irréductibles sur $\mathbb{Q}$ et toutes leurs racines sont réelles. Quels sont les sous-groupes transitifs de S_3 ? Identifier $\mathrm{Gal}(P)$ et $\mathrm{Gal}(Q)$ comme sous-groupes de S_3.

Remarque : Pour un polynôme irréductible de degré 3 seulement deux groupes peuvent apparaître comme groupe de Galois, à savoir A_3 et S_3, et le discriminant permet de les distinguer. Il existe des critères semblables, plus sophistiqués, pour déterminer le groupe $\mathrm{Gal}(P)$ d'un polynôme irréductible $P \in \mathbb{Q}[X]$ de degré 4.

6. Polynômes sur $\mathbb{Q}$ avec groupe S_p

Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p. On note $\mathscr{X} = \{x_1, \ldots, x_p\}$ l'ensemble de ses racines dans $\mathbb{C}$, et $E = \mathbb{Q}(x_1, \ldots, x_p)$ son corps de décomposition.

6.1. Regarder $E > \mathbb{Q}(x_1) > \mathbb{Q}$ et en déduire que p divise $|E : \mathbb{Q}|$. De façon alternative, regarder l'action de $\mathrm{Gal}(E|\mathbb{Q})$ sur $\mathscr{X}$ et en déduire que p divise $|\mathrm{Gal}(E|\mathbb{Q})|$. Pour p premier conclure qu'il existe un automorphisme $\rho \in \mathrm{Gal}(E|\mathbb{Q})$ d'ordre p.

6.2. Supposons que P admet deux racines complexes conjuguées et $p - 2$ racines réelles. Alors il existe $\tau \in \mathrm{Gal}(E|\mathbb{Q})$ agissant comme une transposition sur $\mathscr{X}$.

6.3. Soient $p \geq 3$ un nombre premier, $\tau \in S_p$ une transposition et $\rho \in S_p$ un p-cycle. Alors τ et ρ engendrent le groupe symétrique S_p tout entier.

6.4. Vérifier à nouveau que $\mathrm{Gal}(X^3 - 2) \cong S_3$. Puis montrer que $\mathrm{Gal}(X^5 - 10X + 5) \cong S_5$. Essayer de trouver $P \in \mathbb{Q}[X]$ irréductible de degré 7 tel que $\mathrm{Gal}(P) \cong S_7$.

6.5. Pour $p \geq 5$ premier analyser le polynôme $P = (X-p)(X-2p)\cdots(X-(p-2)p)(X^2+p)-p$. Est-il irréductible ? Combien de ses racines sont réelles ? En déduire son groupe de Galois.

Avertissement. L'hypothèse que p soit premier est nécessaire ! Par exemple le polynôme $X^4 - 2$ admet deux racines réelles $\pm\sqrt[4]{2}$ et deux racines complexes $\pm i\sqrt[4]{2}$. On a vu en exercice 4.4 que $\mathrm{Gal}(X^4 - 2)$ est le groupe diédral D_4 et non le groupe symétrique S_4. Ceci correspond au fait que $\tau = (13)$ et $\rho = (1234)$ n'engendrent pas S_4 mais seulement D_4.

Feuille C5 — CORRESPONDANCE DE GALOIS II

1. GROUPES ABÉLIENS FINIS ET CORRESPONDANCE DE GALOIS

On note $\mathbb{Z}_n$ le groupe additif de l'anneau $\mathbb{Z}/n\mathbb{Z}$, et on note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles. Comme avant on note $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. On construira dans la suite une extension $K|\mathbb{Q}$ avec groupe de Galois isomorphe à $\mathbb{Z}_9$.

1.1. Trouver un générateur g du groupe $\mathbb{Z}_{19}^\times$. Quel est son ordre ? Expliciter ainsi un homomorphisme surjectif $\phi\colon \mathbb{Z}_{19}^\times \twoheadrightarrow \mathbb{Z}_9$ et déterminer son noyau.

1.2. Rappeler pourquoi $\Phi_{19} = X^{18} + X^{17} + \cdots + X + 1$ est irréductible dans $\mathbb{Q}[X]$, et en déduire que $\zeta_{19}, \dots, \zeta_{19}^{18}$ est une base de $E = \mathbb{Q}(\zeta_{19})$ sur $\mathbb{Q}$. Pour tout $k \in \mathbb{Z}_{19}^\times$ construire un automorphisme $\sigma_k\colon E \to E$ avec $\sigma_k(\zeta) = \zeta^k$. Conclure que $\mathrm{Gal}(E|\mathbb{Q}) \cong \mathbb{Z}_{19}^\times$.

1.3. Expliciter une base de $K = E^H$ pour $H = \ker(\phi\colon \mathrm{Gal}(E|\mathbb{Q}) \twoheadrightarrow \mathbb{Z}_9)$. Déterminer $\mathrm{Gal}(E|K)$ et $\mathrm{Gal}(K|\mathbb{Q})$ par la correspondance de Galois.

On se propose de généraliser cet exemple de $\mathbb{Z}_9$ à un groupe abélien fini quelconque. Pour ce faire on admettra le théorème de la progression arithmétique de Lejeune-Dirichlet : Si $a, b \in N$ sont premiers entre eux, alors la progression arithmétique $\{ka+b \mid k \in \mathbb{N}\}$ contient une infinité de nombres premiers.

1.4. Pour tout nombre naturel n, montrer qu'il existe un nombre premier p avec un homomorphisme surjectif $\mathbb{Z}_p^\times \to \mathbb{Z}_n$.

1.5. Plus généralement, pour un groupe abélien fini A, expliquer comment trouver un nombre N avec un homomorphisme surjectif $\mathbb{Z}_N^\times \to A$.

1.6. Rappeler la structure du groupe de Galois de l'extension cyclotomique $E = \mathbb{Q}(\zeta_N)$ sur $\mathbb{Q}$. En déduire que tout groupe abélien fini se réalise comme groupe de Galois $\mathrm{Gal}(K|\mathbb{Q})$.

2. GROUPE DE GALOIS DÉCOMPOSABLE EN PRODUIT DIRECT

2.1. Rappeler qu'un groupe G est le produit direct de deux sous-groupes H et H', noté $G = H \times H'$, si et seulement si H et H' sont distingués, $H \cap H' = \{1\}$ et $HH' = G$.

2.2. Soient $E|K$ une extension galoisienne, F, F' des extensions intermédiaires normales sur K telles que $F \cap F' = K$ et $FF' = E$. Alors on a une décomposition en produit direct $\mathrm{Gal}(E|K) = \mathrm{Gal}(E|F) \times \mathrm{Gal}(E|F')$, puis $\mathrm{Gal}(E|K) \cong \mathrm{Gal}(F|K) \times \mathrm{Gal}(F'|K)$.

2.3. Réciproquement, soient $E|K$ une extension galoisienne et $\mathrm{Gal}(E|K) = H \times H'$. Alors les corps correspondants $F = E^H$ et $F' = E^{H'}$ sont des extensions normales sur K telles que $F \cap F' = K$ et $FF' = E$.

3. EXTENSIONS NON NORMALES ET CLÔTURE GALOISIENNE

3.1. Quels sont les sous-corps « évidents » de $K = \mathbb{Q}[\sqrt[3]{2}, \sqrt[5]{3}]$. (Y en a-t-il d'autres ?)

3.2. Déterminer $\mathrm{Gal}(K|\mathbb{Q})$. La correspondance de Galois est-elle vérifiée ?

3.3. Déterminer la clôture galoisienne E de K sur $\mathbb{Q}$.

3.4. Déterminer le groupe $\mathrm{Gal}(E|\mathbb{Q})$ en utilisant §2.

3.5. Quels sont les sous-groupes de $\mathrm{Gal}(E|\mathbb{Q})$ contenant $\mathrm{Gal}(E|K)$?

3.6. Quels sont les sous-corps de K ? Quelle est la morale de cette histoire ?