UVSQ 2011/2012
Licence de sciences et technologie, santé
LSMA610 (groupes et géométries)

Cours en bref

En TD, s'assurer que sont acquis la définition de $\mathbb{Z}/n\mathbb{Z}$, le théorème de factorisation (exponentielle, notamment) et faire du chinois sur des produits de $\mathbb{Z}/n\mathbb{Z}$ (p-torsion et facteurs invariants).

Table des matières

1 Groupe symétrique **2**
1.1 Permutations d'un ensemble fini 2
1.2 Signature d'une permutation 3
1.3 Groupe alterné 3

2 Polynômes symétriques **5**
2.1 Relations entre racines et coefficients d'un polynôme 5
2.2 Polynômes symétriques 5
2.3 Séries formelles et formules de Newton 7

3 Groupe quotient, théorèmes d'isomorphismes **8**
3.1 Généralités en bref sur les groupes 8
3.2 Classes à gauche et à droite, quotients 8
3.3 Théorèmes d'isomorphismes 9

4 Action d'un groupe sur un ensemble **10**
4.1 Définition, premiers exemples 10
4.1.1 Equation aux classes 10
4.2 Produits semi-directs 11
4.3 Théorèmes de Sylow 11

5 Le groupe orthogonal euclidien (pas en 2012) **12**

6 Appendice : axiomatique des structures abstraites de groupes, anneaux, corps, espaces vectoriels et algèbres **13**
6.1 Groupes 13
6.1.1 Définition, axiomes 13
6.1.2 Sous-groupe, homomorphisme de groupes 13

6.1.3 Exemples fondamentaux 13
6.2 Anneaux 14
6.2.1 Définition, axiomes 14
6.2.2 Sous-anneau, idéal, homomorphisme d'anneaux 14
6.2.3 Exemples fondamentaux 15
6.3 Corps 15
6.3.1 Définition, axiomes 15
6.3.2 Sous-corps, plongements 15
6.3.3 Exemples fondamentaux 15
6.4 Espaces vectoriels 15
6.4.1 Définition, axiomes 15
6.4.2 Sous-espace vectoriel, application linéaire 16
6.4.3 Exemples fondamentaux 16
6.5 Algèbre sur un corps 16
6.5.1 Définition, axiomes 16
6.5.2 Sous-algèbre, homomorphisme d'algèbres 17
6.5.3 Exemples fondamentaux 17

1 Groupe symétrique

1.1 Permutations d'un ensemble fini

Si E est un ensemble, le groupe symétrique de E est le groupe $\mathfrak{S}_E$ des bijections $E \to E$ pour la composition (définition). On note $\sigma\tau = \sigma \circ \tau$ et $\sigma^0 = \mathrm{id}_E$. Si $n \in \mathbb{N}$, on note $\sigma^n = \sigma \circ \cdots \circ \sigma$ (n fois) et $\sigma^{-n} = (\sigma^{-1})^n$.
Si deux ensembles sont équipotents, leurs groupes symétriques sont isomorphes. On note $\mathfrak{S}_n = \mathfrak{S}_{\{1,\ldots,n\}}$.

Exercices. 1- $\mathrm{Card}(\mathfrak{S}_n) = n!$.
2- Si G est un groupe, l'application $f : G \to \mathfrak{S}_G$ définie par $f(g)(h) = gh$ est un homomorphisme injectif de groupes. Ainsi, tout groupe est-il isomorphe à une sous-groupe d'un groupe de permutations.

Définition du support d'une permutation.

Définition d'un p-cycle de $\mathfrak{S}_n$, notation $(a_1, \ldots a_p)$, support d'un p-cycle.
Exercice : si $c = (a_0, \ldots, a_{p-1})$ et $m \in \mathbb{Z}$, alors $c^m(a_k) = a_{\overline{k+m}}$ où $\overline{k+m}$ est le reste de la division euclidienne de $k+m$ par p.

L'ordre d'un p-cycle est p (définir l'ordre d'un élément dans un groupe s'il faut).

Remarque : $\mathfrak{S}_2 \sim \mathbb{Z}/2\mathbb{Z}$; si $n \geq 3$, $\mathfrak{S}_n$ n'est pas abélien ($(12)(23) \neq (23)(12)$).
Deux permutations dont les supports sont disjoints commutent.

Exercice : si s et t sont des permutations dont les supports sont disjoints, l'ordre de st est le ppcm des ordres de s et t.

Définition des classes de conjugaison dans un groupe (s'assurer que classe d'équivalence est connu). Exemple : dans $\mathrm{GL}(V)$, deux endomorphismes sont conjugués si, et seulement s'ils admettent la même matrice dans deux bases *ad hoc*.
Formule de conjugaison des cycles : $s(a_1, \ldots, a_p)s^{-1} = (s(a_1), \ldots, s(a_p))$. Tous les p-cycles sont conjugués dans $\mathfrak{S}_n$.

Deux exemples :
i) $[6, 13, 12, 14, 4, 1, 7, 10, 2, 9, 11, 3, 8, 5] = (1, 6)(2, 13, 8, 10, 9)(3, 12)(4, 14, 5)$;
ii) $(123)(325)(153)(1254) = (154)(23)$.

Toute permutation se décompose en produit de cycles à supports disjoints, unicité à l'ordre près des facteurs.
Dans la preuve, notion d'orbite d'un élément de $\{1, \ldots, n\}$ sous σ. Résultat et preuve à retenir.

Définition d'une transposition. Elles engendrent $\mathfrak{S}_n$ (définition de sous-groupe engendré par intersection ; c'est pareil que minimum pour l'inclusion ; caractérisation par les mots). Raffinement : les $(k, k+1)$ engendrent $\mathfrak{S}_n$.

Exercice. Si $n \geq 4$, les 4-cycles engendrent $\mathfrak{S}_n$ (argument : $(12) = (1324)(1234)^2$).

1.2 Signature d'une permutation

Théorème. *Si $n \geq 2$, il existe un unique homomorphisme de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ non trivial. Si c est un p-cycle, $\varepsilon(c) = (-1)^{p-1}$.*
On appelle ε la signature. Preuve de l'unicité par engendrement des transpositions. Preuve de l'existence par nombre d'inversions.
Si s a m orbites, alors $\varepsilon(s) = (-1)^{n-m}$ (en effet, la somme des longueurs des orbites égale n).

1.3 Groupe alterné

C'est le sous-groupe des permutations paires, noyau de la signature. C'est un sous-groupe distingué d'ordre $n!/2$ (définition de sous-groupe distingué, stabilité par image inverse, les noyaux en sont, on verra plus tard que ce sont les seuls, exemples de $\mathrm{SL}(V)$ dans $\mathrm{GL}(V)$, des rotations dans les isométries, des sous-groupes des groupes abéliens).

Le groupe alterné est engendré par les 3-cycles (pour la preuve : $(12)(23) = (123)$ et $(12)(34) = (12)(23)(23)(34) = (123)(234)$). Si $n \geq 5$, alors les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$. Exercice : classes de conjugaison des 3-cycles dans $\mathfrak{S}_3$ et $\mathfrak{S}_4$.

Cas du groupe de Klein $K = \langle (12)(34), (13)(24) \rangle$ dans $\mathfrak{A}_4$. Chaîne de sous-groupes distingués $\{1\} \triangleleft K \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4$. Cette situation est exceptionnelle.
Définition de groupe simple. Exemple de $\mathbb{Z}/p\mathbb{Z}$, p premier. Simplicité de $\mathfrak{A}_n$ lorsque $n \neq 4$ (on admet le cas $n = 5$ pour l'instant, il sera démontré après la théorie de Sylow ; autre choix possible : montrer le cas $n = 5$ tout de suite avec des moyens plus élémentaires).
[Preuve de la simplicité de $\mathfrak{A}_5$, sans la théorie de Sylow : soit $H \triangleleft \mathfrak{A}_5$. Si H contient un 3-cycle, il les contient tous et donc $H = \mathfrak{A}_5$. Si H contient un élément d'ordre 2, quitte à renuméroter, H contient $(12)(34)$; en conjuguant par (13245), H contient $(34)(25)$, donc le produit $(12)(34)(34)(25) = (125)$ et $H = \mathfrak{A}_5$. Si H contient un élément d'ordre 5, *i.e.* (12345) quitte à renuméroter, on conjugue par (254) ce qui montre que H contient (15324) ; donc H contient $(12345)(15324) = (254)$ et $H = \mathfrak{A}_5$. On a fait le tour des cas possibles.]
[Preuve de la simplicité de $\mathfrak{A}_n$ pour $n \geq 6$: soit $(1) \neq G \triangleleft A_n$. Soit $a \in \{1, \ldots, n\}$ et $\sigma \in G$ tels que $b = \sigma(a) \neq a$. Soit $c \in \{1, \ldots, n\} \setminus \{a, b, \sigma(b)\}$. Soient $\tau = (acb)$ et $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. D'une part $\rho = (\tau\sigma\tau^{-1})\sigma^{-1} \in G$. D'autre part, $\rho = \tau(\sigma\tau^{-1}\sigma^{-1}) = (acb)(\sigma(a)\sigma(b)\sigma(c))$. Soit $E \subseteq \{1, \ldots, n\}$ tel que $\mathrm{Card}\, E = 5$ et $E \supseteq \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ – un tel E existe car $b = \sigma(a)$.
• $\rho \neq 1$; en effet, $\rho = 1$ ssi $(abc) = (\sigma(a)\sigma(b)\sigma(c))$, *i.e.* ssi $(bca) = (b\sigma(b)\sigma(c))$ ce qui n'est pas puisque $\sigma(b) \neq c$.
• [On veut dire proprement que ρ"$\in$"$G \cap \mathfrak{A}_E \triangleleft \mathfrak{A}_E$. Puisque $\mathfrak{A}_E$ est simple, cela impose $G \cap \mathfrak{A}_E = \mathfrak{A}_E$. Donc G contient un 3-cycle. Donc $G = \mathfrak{A}_n$.] On le dit : soit $\pi : \mathfrak{A}_E \to \mathfrak{A}_n$ le prolongement par l'identité hors de E. Alors, $1 \neq (acb)(\sigma(a)\sigma(b)\sigma(c)) \in$

$\pi^{-1}(G) \triangleleft \mathfrak{A}_E$. Par simplicité de $\mathfrak{A}_E$, cela impose $\pi^{-1}(G) = \mathfrak{A}_E$. Donc G contient le 3-cycle $\pi(abc)$. Donc $G = \mathfrak{A}_n$.

Exercice : groupes dérivés (à définir) $D(\mathfrak{A}_n) = D(\mathfrak{S}_n) = \mathfrak{A}_n$ si $n \geq 5$. Calculer $D(\mathfrak{A}_4)$, $D(\mathfrak{A}_3)$, $D(\mathfrak{S}_4)$ et $D(\mathfrak{S}_3)$.
Si $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.
Exercice : si $n \geq 3$, le centre (à définir) de $\mathfrak{S}_n$ est trivial.

2 Polynômes symétriques

2.1 Relations entre racines et coefficients d'un polynôme

A un anneau commutatif. Dans $A[T]$, on a $(T-a_1)(T-a_2) = T^2-(a_1+a_2)T+a_1a_2$, $(T-a_1)(T-a_2)(T-a_3) = \dots$ (l'écrire).
Définition des polynômes symétriques élémentaires de $A[X_1,\dots,X_n]$: $\sigma_0 = 1$,

$$\sigma_k(X_1,\dots,X_n) = \sum_{1\le j_1<\dots<j_k\le n} X_{j_1}\dots X_{j_k}$$

si $1 \le k \le n$ et $\sigma_k = 0$ si $k \ge n+1$. Exemples de σ_1 (somme) et σ_n (produit).
Exercice : quel est le nombre de monômes de σ_k ?
Les énoncés qui suivent sont valables pour $A = \mathbb{Z}$. Il suffirait de les énoncer et de les démontrer dans $\mathbb{Z}$ à cause de l'homomorphisme d'anneaux $\mathbb{Z} \to A$, $n \mapsto n.1$.
Par récurrence sur n,

$$\prod_{k=1}^{n}(T-X_k) = \sum_{k=0}^{n}(-1)^k\sigma_k(X_1,\dots,X_n)T^{n-k} \tag{1}$$

et relations entre racines et coefficients en spécialisant.
Exercice : $\prod_{k=1}^{n}(1+TX_k) = \sum_{k=0}^{n}\sigma_k(X_1,\dots,X_n)T^k$.
Speech sur le problème inverse (équations polynomiales), le degré ≥ 5, la simplicité de $\mathfrak{A}_n$, ...
Exemple : existe-t-il des triplets (x,y,z) de réels tels que $x+y+z = 15$, $xy+xz+yz = -16$ et $xyz = 8$. Un tel triplet existe ssi $T^3-15T^2-16T-8$ a trois racines réelles ; c'est non (graphe du polynôme). Même question sur $\mathbb{C}$, c'est oui (toujours).

2.2 Polynômes symétriques

A un anneau commutatif et n un entier naturel. Si $s \in \mathfrak{S}_n$ et $P \in A[X_1,\dots,X_n]$, on note $s.P$ le polynôme $s.P(X_1,\dots,X_n) = P(X_{s(1)},\dots,X_{s(n)})$. On a $\mathrm{id}.P = P$ et $s.(t.P) = (st).P$ (axiomes d'action ; on verra plus tard).
Définition de polynôme symétrique ($s.P = P$ pour toute permutation s). On note $A[X_1,\dots,X_n]^{\mathfrak{S}_n}$ le sous-anneau des polynômes symétriques (exo : c'est un sous-anneau).
Exemples : les polynômes symétriques élémentaires (qu'ils soient symétriques se voit sur l'identité (1)). Les polynômes de Newton $S_p = \sum_k X_k^p$; par exemple, $S_1 = \sigma_1$ et $S_2 = \sigma_1^2 - 2\sigma_2$.

Exercice : un polynôme P est symétrique si, et seulement s'il est invariant par toute transposition, *i.e.* lorsque $\tau.P = P$ pour toute transposition τ.

Exercice : $\sigma_k(X_1,\dots,X_n)_{|X_n=0} = \sigma_k(X_1,\dots,X_{n-1})$ (spécialisation).
Proposition 1- Division euclidienne par un polynôme unitaire dans $A[X]$.

2- Si $f(X_1, \ldots, X_{n-1}, 0) = 0$, alors X_n divise f.
3- Si $X_1, \ldots, X_k$ divisent f, alors $X_1 \ldots X_k$ divise f.
[Preuve en exo ou dans la littérature.]
Théorème. *Soit A un anneau commutatif. Pour tout $P \in A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$, il existe un unique $Q \in A[X_1, \ldots, X_n]$ tel que $P(X_1, \ldots, X_n) = Q(\sigma_1, \ldots, \sigma_n)$.*
[Preuve. On notera $(\sigma_k)_0 = \sigma_k(X_1, \ldots, X_{n-1}, 0)$ pour tout k.
1- Existence. Par récurrence sur n. Rien à dire si $n = 1$ puisqu'alors, $X_1 = \sigma_1$. Soit $n \geq 2$; on suppose que pour tout $m \leq n-1$, tout polynôme symétrique en $X_1, \ldots, X_m$ est un polynôme en les polynômes symétriques élémentaires de $X_1, \ldots, X_m$. On montre par récurrence sur d que tout polynôme symétrique non nul de degré d en $X_1, \ldots, X_n$ est un polynôme en $(\sigma_1, \ldots, \sigma_n)$. Si $d = 0$, rien à faire. Soit $P \in A[X_1, \ldots, X_n]$, non nul, de degré $d \geq 1$, symétrique. Alors, $P(X_1, \ldots, X_{n-1}, 0)$ est symétrique dans $A[X_1, \ldots, X_{n-1}]$ (exercice). Soit alors $Q_1 \in A[X_1, \ldots, X_{n-1}]$ tel que $P(X_1, \ldots, X_{n-1}, 0) = Q_1((\sigma_1)_0, \ldots, (\sigma_{n-1})_0)$. On pose $P_1(X_1, \ldots, X_n) = P(X_1, \ldots, X_n) - Q_1(\sigma_1, \ldots, \sigma_{n-1})$. On a $\deg P_1 \leq d$ puisque $\deg Q_1((\sigma_1)_0, \ldots, (\sigma_{n-1})_0) = \deg Q_1(\sigma_1, \ldots, \sigma_{n-1})$. Par ailleurs, comme $P_1(X_1, \ldots, X_{n-1}, 0) = 0$, $X_n | P_1$. A cause de la symétrie de P_1, il en résulte que $\sigma_n | P_1$. Soit $P_2 \in A[X_1, \ldots, X_n]$ tel que $P_1 = \sigma_n P_2$. Clairement, P_2 est symétrique et $\deg P_2 \leq d-n$. Par récurrence, soit $Q_2 \in A[X_1, \ldots, X_n]$ tel que $P_2(X_1, \ldots, X_n) = Q_2(\sigma_1, \ldots, \sigma_n)$. Alors, $P(X_1, \ldots, X_n) = Q_1(\sigma_1, \ldots, \sigma_{n-1}) + \sigma_n Q_2(\sigma_1, \ldots, \sigma_n)$.
Unicité. Il suffit de montrer que $\forall P \in A[X_1, \ldots, X_n],\ P(\sigma_1, \ldots, \sigma_n) = 0 \Rightarrow P = 0$. On procède par récurrence sur n. Si $n = 1$, rien à dire. On suppose que $n \geq 2$. Soit $P \in A[X_1, \ldots, X_n]$, non nul, de degré minimal, tel que $P(\sigma_1, \ldots, \sigma_n) = 0$. On ordonne : $P = P_0 + X_n P_1 + \cdots + X_n^d P_d$ où $P_k \in A[X_1, \ldots, X_{n-1}]$. On substitue en $\sigma_1, \ldots, \sigma_n$ et on spécialise en $X_n = 0$. On obtient $0 = P_0((\sigma_1)_0, \ldots, (\sigma_{n-1})_0)$. Par récurrence sur n, cela entrîne que $P_0 = 0$. Ainsi, $P = X_n Q$ où $Q \in A[X_1, \ldots, X_n]$ avec $\deg Q = \deg P - 1$. En particulier, puisque σ_n est unitaire, $Q(\sigma_1, \ldots, \sigma_n) = 0$ ce qui contredit le caractère minimal du degré de P : l'hypothèse $P \neq 0$ ne tient pas.]

Si A est un sous-anneau d'un anneau B, définition d'élément algébrique ou transcendant sur A ; éléments algébriquement (in)dépendants sur A. Exemples de nombres algébriques ou transcendants (sans preuve).
Définitions équivalentes de sous-anneau engendré. Notation $A[b_1, \ldots, b_n]$.
Théorème (reformulation). *Soit A un anneau commutatif.*
1- $A[X_1, \ldots, X_n]^{\mathfrak{S}_n} = A[\sigma_1, \ldots, \sigma_n]$.
2- $\sigma_1, \ldots, \sigma_n$ sont algébriquement indépendants sur A.
Conséquence : $A[X_1, \ldots, X_n]^{\mathfrak{S}_n} = A[\sigma_1, \ldots, \sigma_n] \sim A[X_1, \ldots, X_n]$.
Exemple du polynôme de Vandermonde $V \in \mathbb{Z}[X_1, \ldots, X_n]$ (celui du déterminant avec des indéterminées pour coefficients). Si τ est une transposition, $\tau.V = -V$ (se voit sur la forme déterminant) : V n'est pas symétrique (et calcul de $s.V$ pour n'importe quelle permutation s). En revanche, V^2 l'est ; discriminant ; exemple en dimension deux.

2.3 Séries formelles et formules de Newton

Anneau $A[[T]]$ des séries formelles (suites à valeurs dans A, lois usuelles, notation $T = (0, 1, 0 \dots)$; comme pour les polynômes, sous-anneau des suites presque nulles, occasion de le rappeler pour ceux qui savaient, de le dire pour les autres).
Exemple fondamental : $1 - T$ est inversible dans $A[[T]]$, et $(1 - T)^{-1} = \sum_{k \geq 0} T^k$.
Corollaire : si Q a un terme constant nul, alors $1 - Q$ est inversible et $(1 - Q)^{-1} = \sum_{k \geq 0} Q^k$ (cette dernière somme a du sens).
Exercice : substitution dans une série formelle. Si S est une série formelle dont le terme constant est nul, l'application $A[[T]] \to A[[T]]$, $U = \sum u_k T^k \mapsto U \circ S = \sum u_k S^k$ est bien définie et est un homomorphisme d'anneaux.
Proposition : dans $A[X_1, \dots, X_n]$, pour tout $p \geq 0$, on a

$$\sum_{\substack{(i,j),\ i+j=p \\ i \geq 0,\ j \geq 0}} (-1)^j \sigma_j S_{i+1} = (-1)^p (p+1) \sigma_{p+1}.$$

Permet de calculer les polynômes de Newton en fonction des polynômes symétriques élémentaires. Preuve par la série formelle $F(T) = \prod (1 - TX_k) = \sum (-1)^k \sigma_k T^k$ dont la dérivée logarithmique $S(T)$ vaut $-\sum S_{k+1} T^k$; la formule est obtenu en écrivant que $FS = F'$.
Exercice : calculer $\det_{(\sigma_1, \dots, \sigma_n)}(S_1, \dots, S_n)$ $(= 1)$ et $\det_{(S_1, \dots, S_n)}(\sigma_1, \dots, \sigma_n)$ $(= n!)$; en déduire que si k est un corps de caractéristique nulle, $k[X_1, \dots, X_n]^{\mathfrak{S}_n} = k[S_1, \dots S_n]$.
Les S_k, $1 \leq k \leq n$ sont-ils algébriquement indépendants sur k ? [Réponse est oui.]

3 Groupe quotient, théorèmes d'isomorphismes

3.1 Généralités en bref sur les groupes

Lecture du polycopié "structures abstraites" : notions de groupe, sous-groupe, homomorphisme de groupes ; exemples fondamentaux.
Exercice : $f(1_G) = 1_{G'}$; $f(H)$ et $f^{-1}(H')$ sont des sous-groupes. En particulier, définition du noyau ; c'est un sous-groupe (distingué).
Exemples de référence : groupe linéaire et déterminant, groupe symétrique et signature, exponentielle entre $\mathbb{R}$ et $\mathbb{C}^*$.
Définition du produit direct de groupes à la naïve : produit de deux groupes puis d'un produit quelconque en donnant la loi (pas de considération catégorique). Associativité et commutativité à isomorphisme près. Cas des groupes abéliens finis, théorème chinois, énoncé de décomposition en facteurs invariants (révision) ; exemple de calcul des facteurs invariants de $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ et de $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$; exercice : facteurs invariants de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.
Notion de groupe engendré par une de ses parties. Trois points de vue (minimal pour l'inclusion, intersection, mots).

3.2 Classes à gauche et à droite, quotients

Définition de classes à droite (Hx) ou à gauche (xH, deux relations d'équivalence). Toutes ont le même cardinal, celui du sous-groupe H. Elles forment une partition de G : le cardinal commun de $(G/H)_g$ et de $(G/H)_d$ est noté $[G : H]$ et vérifie $|G| = |H| \times [G : H]$. En particulier si G est un groupe fini et H un sous-groupe, théorème de Lagrange : $|H|$ divise $|G|$.
Exercices. 1- H est un sous-groupe distingué de G ssi $xH = Hx$ pour tout $x \in G$, *i.e. ssi* $(G/H)_g = (G/H)_d$. 2- Si $[G : H] = 2$ alors $H \triangleleft G$.
Envie de mettre sur $(G/H)_g$ la loi $xH.yH = xy.H$. Pas de sens. Exemple détaillé des classes à droite et à gauche dans $\mathfrak{S}_3$ modulo le sous-groupe $\langle(12)\rangle$.
Si (et seulement si) $H \triangleleft G$, la classe de xyH ne depend que de xH et de yH. On pose alors $\overline{x}.\overline{y} = \overline{xy}$ (a du sens) ; cela définit une structure de groupe sur l'ensemble quotient $(G/H)_g = (G/H)_d$. On note ce groupe G/H. L'application $p : G \to G/H$, $x \mapsto \overline{x} = xH$ est un homomorphisme de groupes surjectif dont le noyau est H ; on l'appelle *surjection (ou projection) canonique.*
Propriété universelle du quotient. *Si $f : G \to G'$ est un homomorphisme de groupes et si $H \triangleleft G$ vérifie $H \subseteq \ker f$, alors il existe un unique homomorphisme de groupes $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ p$ où p est la surjection canonique. En outre, $\overline{f}$ est injectif ssi $H = \ker f$; $\overline{f}$ est surjectif ssi f l'est.*
Preuve. Unicité : f détermine $\overline{f}$ car $\overline{f}(\overline{x}) = f(x)$ est nécessaire. Existence : on peut définir $\overline{f}$ ainsi car $H \triangleleft G$. C'est un homomorphisme de groupes. Enfin, $\ker \overline{f} = p(\ker f)$ et $\operatorname{im} \overline{f} = \operatorname{im} f$.

Exemple : théorème chinois. $\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $x \mapsto (x + a\mathbb{Z}, x + b\mathbb{Z})$ se factorise en un homomorphisme injectif $\mathbb{Z}/a \vee b\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Lorsque a et b sont étrangers, c'est un isomorphisme pour des raisons de cardinal (fini).

3.3 Théorèmes d'isomorphismes

Le premier est conséquence directe de la propriété universelle du quotient. Les autres sont donnés en exercice (TD ?).

Premier théorème d'isomorphisme. *Si $f : G \to G'$ est un homomorphisme de groupes, il se factorise en un isomorphisme de groupes* $\boxed{G/\ker f \simeq \operatorname{im} f}$.
Exemple : $\mathrm{GL}(E)/\mathrm{SL}(E) \simeq k^*$, $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{U}_n$ (racines n-ièmes de l'unité), $\mathbb{Q}/\mathbb{Z} \simeq \mathbb{U}$ (toutes les racines de l'unité), $\mathbb{R}/\mathbb{Z} \simeq S^1$ (cercle unité).

Deuxième théorème d'isomorphisme. *$C \subseteq B$ distingués dans A. Alors B/C* est *un sous-groupe distingué de A/C et* $\boxed{(A/C)/(B/C) \sim A/B}$.
Preuve : $p : A \overset{can}{\to} A/C$ est surjective, donc $p(B) = B/C \triangleleft A/C$. Comme $C \subseteq B$, $q : A \overset{can}{\to} A/B$ se factorise en $\overline{q} : A/C \to A/B$, surjectif. Enfin, $\ker \overline{q} = p(B) = B/C$. On conclut avec les premier théorème d'isomorphisme.

Troisième théorème d'isomorphisme. *Si A et B sont deux sous-groupes d'un même groupe G et si A normalise B (i.e. si $aBa^{-1} = B$ pour tout $a \in A$) alors $A \cap B$ est distingué dans A, $AB = \{ab, a \in A, \in B\} = BA$ est un sous-groupe de G, B est un sous-groupe distingué de AB et* $\boxed{AB/B \sim A/A \cap B}$.
Preuve : $A \hookrightarrow AB \overset{can}{\to} AB/B$ est surjectif et a pour noyau $A \cap B$.

4 Action d'un groupe sur un ensemble

4.1 Définition, premiers exemples

Définition *d'action à gauche* d'un groupe G sur un ensemble X comme application $G \times X \to X$ avec ses deux axiomes $1.x = x$ et $g.(g'x) = (gg').x$. Equivalent à la donnée d'un homomorphisme de groupes $G \to \mathfrak{S}_X$.
Variante : action à droite (premier point de vue : $(x.g).g' = x.(gg')$; second point de vue : application $F : G \to \mathfrak{S}_X$ vérifiant $F(gg') = F(g')F(g)$). Quand on a une action à droite F, on obtient une action à gauche en posant $f(g) = F(g^{-1})$.
Exemples : $\mathfrak{S}_E$ opère sur E, sur les parties de E de cardinal fixé, sur les E^n ; si V est un espace vectoriel, $\mathrm{GL}(V)$ opère sur V, sur les droites de V, sur les sous-ev de dimension donnée, sur les drapeaux ; $\mathrm{SL}_2(\mathbb{R})$ opère sur le demi-plan de poincaré *via* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$ (exo) ; les similitudes du plan agissent sur l'ensemble des cercles ; les isométries du plan fixant l'origine agissent sur le cercle trigonométrique ; les isométries du plan qui stabilisent un polygone régulier donné agissent sur ses sommets, sur les milieux de ses arêtes ; les isométries de l'espace qui stabilisent un cube agissent sur ses diagonales. Un groupe agit sur lui-même par conjugaison ou par translation à gauche.
Définition d'*action transitive* ($\forall x, y, \exists g, y = g.x$) ou *fidèle* (seul 1 fixe tous les points). Si f est une action de G, elle se factorise en une action fidèle de $G/\ker(f)$.
Définition d'*orbite* d'un point (notée $G.x$), de *sous-groupe d'isotropie* (noté G_x). Les sous-groupes d'isotropie des points d'une même orbite sont conjugués ($G_{g.x} = gG_xg^{-1}$). Relation d'équivalence $x \sim y \Leftrightarrow \exists g, y = g.x$. Les classes sont les orbites. Elles forment une partition de X.
Une partie Y de X est dite *stable* lorsque $G.Y \subseteq Y$ (en fait, égalité *via* les g^{-1}).
Définition de *stabilisateur* d'une partie (sous-groupe des éléments du groupe qui stabilisent la partie).
Définition de partie *fixe* ($\forall y, g,\ g.y = y$) et de *fixateur* d'une partie (éléments du groupe qui fixent la partie).
Exemple : $u \in \mathrm{GL}(V)$, action naturelle de $\langle u \rangle$ sur V. Une droite stable est une droite de vecteurs propres pour u. Une droite fixe est une droite propre associée à la valeur propre 1.
Si H est un sous-groupe de G, action par conjugaison de G sur lui-même. Stabilisateur de H s'appelle *normalisateur* ; fixateur de H s'appelle *centralisateur*. *Centre* d'un groupe.

4.1.1 Equation aux classes

Si x est dans X, l'application $g \mapsto g.x$ est constante sur les classes à gauche modulo G_x. Elle induit une bijection de l'ensemble $(G/G_x)_g$ sur l'orbite $G.x$. On en déduit que $\boxed{\mathrm{Card}(G.x) = [G : G_x]}$ ou encore $|G| = |G_x| \times \mathrm{Card}(G.x)$.

Dans le cas où X est un ensemble fini, l'équation aux classes traduit la partition de X en orbites sous l'action de G en termes de cardinaux : $\boxed{\mathrm{Card}(X) = \sum_{x\in\mathcal{R}}[G : G_x]}$ où $\mathcal{R}$ est un système de représentants des orbites.
Exemple des p-groupes : si X^G désigne les invariants sous G et si G est un p-groupe, alors $\mathrm{Card}(X) \equiv \mathrm{Card}(X^G)\ [p]$. Exemple de l'action de G sur lui-même par conjugaison : le centre d'un p-groupe est non trivial (et exo : un p-groupe est nilpotent (donc résoluble), récurrence sur l'exposant de l'ordre).
Exemple : action du groupe positif du cube sur les centres des faces. Transitive, 6 centres, isotropie d'ordre 4 : le groupe positif du cube est d'ordre 24.

4.2 Produits semi-directs

Suite exacte de groupes, suite exacte scindée (existence d'une section ou existence d'un sous-groupe qui fait de la surjection un isomorphisme par restriction).
Une suite exacte $1 \to N \to G \to Q \to 1$ est scindée si, et seulement s'il existe un sous-groupe H de G tel que $H \cap N = 1$ et $G = HN$.
Définition du produit semi-direct de N et Q relatif à une action de Q sur N par automorphismes, *i.e.* un homomorphisme de groupes $\varphi : Q \to \mathrm{Aut}(N)$ (c'est la loi de groupes sur le produit cartésien définie par $(n, q)(n', q') = (n\varphi(q)(n'), qq')$, le neutre est $(1, 1)$, l'inverse de (n, q) est $(\varphi(q^{-1})(n^{-1}), q^{-1})$).
G est isomorphe à un produit semi-direct de Q et N si, et seulement s'il existe une suite exacte scindée $1 \to N \to G \to Q \to 1$. En passant, formule du produit direct interne $nhn'h' = nhn'h^{-1}hh'$.
Caractérisation du produit direct parmi les semi-directs (N et H commutent).
Exemples dans $\mathfrak{S}_n$, groupe diédral, groupe linéaire, groupe affine, isométries (dont celles des polyèdres réguliers ; groupe du cube, groupe du tétraèdre).

4.3 Théorèmes de Sylow

Définition d'un p-Sylow (p sous-groupe dont l'indice n'est pas divisible par p).
Exemple : les matrices trigonales sup avec des 1 sur la diagonale forment un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.
Premier théorème de Sylow *Tout groupe fini contient un p-Sylow.*
Preuve : voir G comme un sous-groupe de $\mathfrak{S}_n$ où n est l'ordre de G, puis comme un sous-groupe de $\mathrm{GL}(n, \mathbb{F}_p)$. Comme on a un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$, on conclut avec le lemme suivant.
Lemme *Soient G un groupe fini, H un sous-groupe, S un p-Sylow de G. Il existe $a \in G$ tel que $H \cap (aSa^{-1})$ soit un p-Sylow de H.*
Preuve. On fait agir H sur $(G/S)_g$ par translation à gauche et on écrit l'équation aux classes $[G : S] = \sum_{a\in\mathcal{R}}[H : H_{aS}]$. Comme p ne divise pas $[G : S]$, soit a tel que p ne divise pas $[H : H_{aS}]$: un tel a convient car $H_{aS} = H \cap (aSa^{-1})$ est un p-Sylow de H (c'est un p-groupe car c'est un sous-groupe du p-Sylow aSa^{-1}).

Deuxième théorème de Sylow *Tout p-sous-groupe est contenu dans un p-Sylow ; les p-Sylow sont conjugués.*
Preuve : avec le lemme, deux fois.
Remarque : un p-Sylow est distingué ss'il est le seul p-Sylow.
Troisième théorème de Sylow *Le nombre de p-Sylow divise l'ordre du groupe et est $\equiv 1$ $[p]$.*
Preuve. 1- Faire agir G par conjugaison sur l'ensemble $\mathcal{S}$ de ses p-Sylow. Une seule orbite. 2- Faire agir un p-Sylow S par conjugaison sur $\mathcal{S}$. Comme S est un p-groupe, $\#\mathcal{S} \equiv \#\mathcal{S}^S$ $[p]$. On montre que $\mathcal{S}^S = \{S\}$: si $T \in \mathcal{S}^S$, soit $N = \mathrm{Stab}_G(T)$; alors $T \triangleleft N$, donc T est l'unique p-Sylow de N. D'où $S = T$ puisque S est aussi un p-Sylow de N.
Exemples : un groupe d'ordre 91 n'est jamais simple (voir les 7-Sylow). Les 3-Sylow et les 2-Sylow de $\mathfrak{S}_4$.
Exercice : compter et décrire les Sylow de $\mathfrak{S}_3$, $\mathfrak{A}_4$, $\mathfrak{A}_5$, $\mathfrak{S}_5$.
Dette : démontrer la simplicité de $\mathfrak{A}_5$.

5 Le groupe orthogonal euclidien (pas en 2012)

6 Appendice : axiomatique des structures abstraites de groupes, anneaux, corps, espaces vectoriels et algèbres

6.1 Groupes

6.1.1 Définition, axiomes

Un **groupe** est un ensemble G muni d'une *loi de composition interne* notée ici $\times$ (*i.e.* une application $G \times G \to G$, $(x, y) \mapsto x \times y$) vérifiant les trois axiomes suivants :
1- la loi $\times$ est *associative (i.e.* $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, et z de G ; on note $x \times y \times z$ ce produit) ;
2- G possède un *élément neutre* e pour $\times$ (*i.e.* $x \times e = e \times x = x$ pour tout $x \in G$; on note souvent 1 l'élément neutre) ;
3- tout élément de G possède un *symétrique* pour $\times$ (*i.e.* pour tout $x \in G$, il existe $y \in G$ tel que $x \times y = y \times x = e$; on note souvent $y = x^{-1}$).

Si en outre $\times$ est *commutative* (*i.e.* $x \times y = y \times x$ pour tous x et y de G), le groupe est dit *commutatif* ou *abélien*.

On omet souvent le symbole $\times$ de la loi en notant $xy = x \times y$. On note parfois $+$ la loi des groupes commutatifs ; dans ces conditions, l'élément neutre est noté 0 et le symétrique de tout $x \in G$ est noté $-x$.

6.1.2 Sous-groupe, homomorphisme de groupes

Un **sous-groupe** d'un groupe G est une partie de G qui soit un groupe pour la loi de G.

Proposition *Une partie non vide H d'un groupe G est un sous-groupe de G si, et seulement si :*
1- H est stable pour la loi de G (i.e. $x \times y \in H$ pour tous x et y de H) ;
2- le symétrique (pour la loi de G) de tout élément de H est dans H.

Un **homomorphisme de groupes** est une application f d'un groupe G dans un groupe G' qui préserve les lois de G et de G', c'est-à-dire telle que $f(xy) = f(x)f(y)$ pour tous x et y de G.

6.1.3 Exemples fondamentaux

L'addition usuelle dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{Z}$, et dans leurs puissances.

La multiplication usuelle dans $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ ou $\mathbb{C}^*$, dans l'ensemble des nombres complexes de module un, dans l'ensemble des racines n-ièmes de l'unité ($n \geq 1$) et dans l'ensemble de toutes les racines de l'unité.

La composition dans $\mathfrak{S}_A$ (groupe symétrique de l'ensemble A) ; dans $\mathrm{GL}(E)$ (groupe linéaire de l'espace vectoriel E) et dans ses sous-groupes $\mathrm{SL}(E)$, $\mathrm{O}(E)$, $\mathrm{SO}(E)$, $\mathrm{U}(E)$, $\mathrm{SU}(E)$; dans l'ensemble des similitudes (resp. des similitudes directes) vectorielles planes ; dans $\mathrm{GA}(E)$ (groupe affine de l'espace affine E) et dans ses sous-groupes des translations, des homothéties-translations, des isométries, des rotations, des similitudes *etc.*

Le produit matriciel dans $\mathrm{GL}_n(A)$ (matrices carrées $n \times n$ inversibles à coefficients dans l'anneau A), $\mathrm{SL}_n(A)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{U}_n(\mathbb{C})$, $\mathrm{SU}_n(\mathbb{C})$; dans l'ensemble des matrices triangulaires supérieures (resp. inférieures) inversibles, dans l'ensemble des matrices diagonales inversibles, *etc.*

6.2 Anneaux

6.2.1 Définition, axiomes

Un **anneau** (unitaire) est un ensemble A muni de deux lois de composition interne notées ici $+$ (addition) et $\times$ (multiplication) vérifiant les axiomes suivants :
1- $(A, +)$ est un groupe abélien ; on note souvent son élément neutre 0 et $-a$ le symétrique de $a \in A$ pour $+$ (on parle de l'*opposé* de a) ;
2- la loi $\times$ est associative et admet un élément neutre souvent noté 1 ;
3- la multiplication est *distributive* par rapport à l'addition (*i.e.* $a \times (b + c) = (a \times b) + (a \times c)$ et $(a + b) \times c = (a \times c) + (b \times c)$ pour tous a, b et c de A).

Si en outre la multiplication est commutative, l'anneau est dit *commutatif*.

Les règles de calcul dans un anneau commutatif sont celles de $\mathbb{Z}$; en particu- lier, la formule du binôme de Newton est vraie dans un anneau commutatif (ou dans un anneau général entre deux éléments qui commutent). Dans les systèmes de parenthésages, on donne la priorité à la multiplication ; ainsi, $a \times b + c = (a \times b) + c$.

6.2.2 Sous-anneau, idéal, homomorphisme d'anneaux

Un **sous-anneau** d'un anneau A est une partie de A qui soit un anneau pour les lois de A. Une partie B d'un anneau $(A, +, \times)$ est un sous-anneau de A si, et seulement si $(B, +)$ est un sous-groupe de $(A, +)$ contenant 1, et B est stable pour la multiplication de A.
Un **idéal** d'un anneau commutatif A est une partie I de A telle $(I, +)$ soit un sous-groupe de $(A, +)$ et $ia \in I$ pour tous $i \in I$ et $a \in A$.
Une application f d'un anneau A dans un anneau B est un **homomorphisme d'anneaux** si, et seulement si elle préserve les unités et les lois de A et B, c'est-à-dire si, et seulement si $f(1) = 1$, $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tous x et y de A.

6.2.3 Exemples fondamentaux

Pour leurs lois usuelles, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 2$, les corps de nombres $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, l'ensemble des nombres décimaux.

Les anneaux de polynômes à coefficients dans un anneau A.

L'anneau des endomorphismes d'un espace vectoriel (la multiplication est la composition), l'anneau des matrices carrées à coefficients dans un anneau (la multiplication est le produit matriciel).

L'ensemble des applications d'un ensemble E dans un anneau A (pour les lois usuelles $(f+g)(x) = f(x) + g(x)$ et $(fg)(x) = f(x)g(x)$).

6.3 Corps

6.3.1 Définition, axiomes

Un **corps** est un anneau A dans lequel tout élément non nul x admet un symétrique pour la multiplication (on parle alors de l'*inverse* de x, souvent noté x^{-1}). Cela revient à demander que $A \setminus \{0\}$ soit un groupe pour la multiplication.

6.3.2 Sous-corps, plongements

Un **sous-corps** d'un corps L est une partie K de L qui soit un corps pour les lois de L. Cela revient à demander que $(K, +)$ soit un sous-groupe de $(L, +)$ et que $(K \setminus \{0\}, \times)$ soit un sous-groupe de $(L \setminus \{0\}, \times)$.
Un homomorphisme d'anneaux $k \to A$ où k est un corps est toujours injectif. On parle de **plongement** de k dans A ou d'**extension** de k.

6.3.3 Exemples fondamentaux

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ pour leurs lois usuelles. Le corps des nombres algébriques.

$\mathbb{Z}/p\mathbb{Z}$ si p est un nombre premier, les corps finis $\mathbb{F}_{p^a}$.

$k[X]/(P)$ si k est un corps et si P est un polynôme irréductible de $k[X]$; plus généralement, le quotient d'un anneau par un idéal maximal.

L'ensemble des fractions rationnelles sur un corps (une ou plusieurs indéterminées).

L'ensemble des fonctions méromorphes sur un ouvert de $\mathbb{C}$.

Le corps des quaternions (non commutatif).

6.4 Espaces vectoriels

6.4.1 Définition, axiomes

Un **espace vectoriel** sur le corps k est un ensemble E muni d'une loi de composition interne (*addition*) notée ici $+$ et d'une loi externe sur k notée . (*i.e.* une application

$k \times E \to E$, $(a, x) \mapsto a.x$, *multiplication par les scalaires*) vérifiant :
1- $(E, +)$ est une groupe abélien ;
2- pour tous $(a, b) \in k^2$ et $(x, y) \in E^2$,
• $1.x = x$;
• $(a + b).x = a.x + b.x$;
• $a.(x + y) = a.x + a.y$;
• $a.(b.x) = (ab).x$.

6.4.2 Sous-espace vectoriel, application linéaire

Un **sous-espace vectoriel** d'un espace vectoriel E est une partie de E qui soit un espace vectoriel pour les lois de E. Une partie F d'un espace vectoriel E est un sous-espace vectoriel de E si, et seulement si F est non vide et stable pour les lois de E, *i.e.* $x + y \in F$ et $a.x \in F$ pour tous $(x, y) \in F^2$ et $a \in k$.
Une application f d'un espace vectoriel E sur k dans un espace vectoriel F sur k est une **application linéaire** (ou homomorphisme d'espaces vectoriels) si, et seulement si elle préserve les lois de E et F, c'est-à-dire si, et seulement si $f(x+y) = f(x)+f(y)$ et $f(a.x) = a.f(x)$ pour tous $(x, y) \in E^2$ et $a \in k$.

6.4.3 Exemples fondamentaux

k^n où $n \in \mathbb{N}^*$, pour les lois $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ et $a.(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$; prototype d'espace vectoriel de dimension finie égale à n.

L'ensemble des applications linéaires d'une espace vectoriel dans un autre (pour les lois $(f+g)(x) = f(x)+g(x)$ et $(a.f)(x) = a.f(x)$) ; en particulier, l'espace des formes linéaires (dual).

L'ensemble des suites à coefficient dans k (dimension dénombrable), pour les lois $(x_n)_n + (y_n)_n = (x_n + y_n)_n$ et $a.((x_n)_n) = (ax_n)_n$.

L'ensemble des applications d'un ensemble dans le corps k pour les lois usuelles.

Si A est un anneau, extension d'un corps k, alors A est un espace vectoriel sur k (d'où les cardinaux des corps finis).

6.5 Algèbre sur un corps

6.5.1 Définition, axiomes

Une **algèbre** (unifère) sur le corps k est un ensemble A muni de deux lois de composition interne notées $+$ (*addition)* et $\times$ (*multiplication*) et d'une loi externe sur k notée . (*multiplication par les scalaires*) vérifiant :
1- $(A, +, \times)$ est un anneau ;
2- $(A, +, .)$ est un espace vectoriel sur k ;

3- $(a.x) \times y = x \times (a.y) = a.(x \times y)$ pour tous $(x, y) \in A$ et $a \in k$; on note ce produit $a.x \times y$.
L'axiome **3-** revient à demander que l'application $A \times A \to A$, $(x, y) \mapsto x \times y$ soit bilinéaire pour la structure d'espace vectoriel de A.

6.5.2 Sous-algèbre, homomorphisme d'algèbres

Une partie d'une algèbre en est une **sous-algèbre** lorsqu'elle en est à la fois un sous-anneau et un sous-espace vectoriel. Les sous-algèbres sont les sous-anneaux stables pour la loi externe.
Une application d'une k-algèbre dans une autre est un **homomorphisme de k-algèbres** si, et seulement si elle est à la fois une application linéaire et un homomorphisme d'anneaux.

6.5.3 Exemples fondamentaux

L'ensemble des endomorphismes d'un espace vectoriel (la multiplication est la composition).

L'ensemble des matrices carrées à coefficients dans un corps (la multiplication est le produit matriciel).

Les algèbres de polynômes à coefficients dans un corps.

L'ensemble des applications d'un ensemble E dans une k-algèbre et ses sous-algèbres selon les structures (algébriques, topologiques, géométriques, *etc*) de E et de k.

UVSQ 2005/2006 25 novembre 2005
Licence de sciences et technologies
LSMA112 (algèbre 3)

Examen partiel

(trois heures)

Questions de cours (6 points)

1- Donner la définition d'éléments algébriquement indépendants sur un sous-anneau. Enoncer le théorème de structure des polynômes symétriques (existence et unicité).

2- Soient $s = (152)(5314)(94)(617482)$ et $t = (163)(8193)(67)(521743)$ deux permutations de $\mathfrak{S}_9$. Calculer leurs signatures. Ces permutations sont-elles conjuguées ?

Problème 1 (6 points)

Soit n un entier naturel ≥ 2. On note M la matrice carrée $n \times n$ à coefficients dans l'anneau de polynômes $\mathbb{Z}[X_1, \ldots, X_n]$ définie par $M_{ij} = X_i^{j-1}$ pour tous i et j dans $\{1, \ldots, n\}$. Autrement dit,

$$M = \begin{pmatrix} 1 & X_1 & \ldots & X_1^{n-1} \\ 1 & X_2 & \ldots & X_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & X_n & \ldots & X_n^{n-1} \end{pmatrix}.$$

1- Calculer la matrice ${}^tMM$ en fonction des sommes de Newton $S_k = \sum_{j=1}^n X_j^k$, $k \geq 1$ (${}^tM$ désigne la transposée de la matrice M).

2- On rappelle que le polynôme de Vandermonde est le déterminant de M et que le polynôme discriminant est le carré du polynôme de Vandermonde. Calculer le discriminant de trois indéterminées X_1, X_2, X_3 en fonction de leurs sommes de Newton.

3- Soient p et q deux nombres rationnels, et x_1, x_2, x_3 les racine complexes du polynôme $X^3 + pX + q$. Calculer, en fonction de p et q, la valeur du discriminant en x_1, x_2, x_3. Ce dernier nombre est-il toujours rationnel ?

[*On rappelle la formule liant les polynômes de Newton S_k aux polynômes symétriques élémentaires σ_k : pour tout $p \geq 0$,*

$$\sum_{\{(i,j),\ i\geq 0,\ 0\leq j\leq n,\ i+j=p\}} (-1)^j \sigma_j S_{i+1} = (-1)^p (p+1)\sigma_{p+1}.]$$

Problème 2 (8 points)

1- Centralisateur

1.1- Si G est un groupe et $x \in G$, on appelle *centralisateur* de x le sous-ensemble $Z(x)$ des éléments de G qui commutent avec x :

$$Z(x) = \{y \in G,\ xy = yx\}.$$

Montrer que les centralisateurs d'un groupe G sont des sous-groupes, et que pour tout $(x, y) \in G^2$,

$$Z(yxy^{-1}) = yZ(x)y^{-1}.$$

1.2- Dans le groupe $\mathfrak{S}_5$, montrer que toute permutation σ du centralisateur de la transposition (12) vérifie $\sigma(\{1, 2\}) = \{1, 2\}$ et $\sigma(\{3, 4, 5\}) = \{3, 4, 5\}$. En déduire que $Z((12))$ contient 12 éléments et en donner la liste.

1.3- Dans le groupe $\mathfrak{S}_5$, montrer que $Z((12)(34))$ contient 8 éléments et en donner la liste.

1.4- Dans $\mathfrak{S}_5$, montrer que le centralisateur d'une transposition contient 12 éléments, et que le centralisateur d'un produit de deux transpositions à supports disjoints en contient 8.

2- Automorphismes de $\mathfrak{S}_5$

On appelle *automorphisme* d'un groupe G tout homomorphisme de groupe bijectif $G \to G$. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G pour la composition des applications. On rappelle qu'un élément x d'un groupe est dit *d'ordre deux* lorsque $x \neq 1$ et $x^2 = 1$.

2.1- Montrer que si $\sigma \in \mathfrak{S}_5$, l'application $f_\sigma : \mathfrak{S}_5 \to \mathfrak{S}_5$ définie par $f_\sigma(\tau) = \sigma\tau\sigma^{-1}$ pour tout $\tau \in \mathfrak{S}_5$ est un automorphisme de $\mathfrak{S}_5$. Un tel automorphisme est dit *intérieur*. Montrer que l'application $\mathfrak{S}_5 \to \mathrm{Aut}(\mathfrak{S}_5)$, $\sigma \mapsto f_\sigma$ est un homomorphisme injectif de groupes.

2.2- Montrer que tout automorphisme φ d'un groupe G envoie un élément d'ordre deux sur un élément d'ordre deux et que pour tout $x \in G$, on a $\varphi(Z(x)) = Z(\varphi(x))$.

2.3- Décrire tous les éléments d'ordre deux de $\mathfrak{S}_5$. Montrer que l'image d'une transposition par un automorphisme de $\mathfrak{S}_5$ est une transposition (on pourra utiliser **1-**).

2.4- Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_5)$. Montrer que l'intersection des supports de $\varphi((12))$ et de $\varphi((13))$ est réduite à un singleton. En déduire que φ est nécessairement intérieur.

UVSQ 2005/2006 25 novembre 2005
Licence de sciences et technologies
LSMA112 (algèbre 3)

Corrigé succinct du partiel

Questions de cours

2- En termes de produits de cycles à supports disjoints, $s = (1792648)(35)$ et $t = (13529)(4867)$. Ces cycles n'ont pas les mêmes longueurs : s et t ne sont pas conjuguées.

Problème 1

1- A l'aide de la formule du produit de matrices, on trouve que le coefficient de la i-ième ligne et de la j-ième colonne de ${}^tMM$ est la somme de Newton S_{i+j-2}, à savoir

$$ {}^tMM = \begin{pmatrix} n & S_1 & \dots & S_{n-1} \\ S_1 & S_2 & \dots & S_n \\ \vdots & \vdots & & \vdots \\ S_{n-1} & S_n & \dots & S_{2n-2} \end{pmatrix}. $$

2- On note V le polynôme de Vandermonde en X_1, X_2, X_3. Comme $\det({}^tM) = \det(M)$ (c'est vrai pour n'importe quelle matrice carrée), $V^2 = \det({}^tM)\det(M) = \det({}^tMM) = 3S_2S_4 - S_1^2S_4 - 3S_3^2 + 2S_1S_2S_3 - S_2^3$ (calcul élémentaire du déterminant d'une matrice 3×3).

3- Comme V^2 est un polynôme symétrique, $V^2(x_1, x_2, x_3)$ s'exprime en fonction des polynômes symétriques élémentaires en (x_1, x_2, x_3), c'est-à-dire en fonction des coefficients p et q du polynôme dont ils sont les racines (relations entre racines et coefficients d'un polynôme). Puisque $S_1(x_1, x_2, x_3) = 0$ (le coefficient de X^2 dans $X^3 + pX + q$ est nul), on a déjà la simplification suivante : $V^2(x_1, x_2, x_3)$ est la valeur en (x_1, x_2, x_3) du polynôme $3S_2S_4 - 3S_3^2 - S_2^3$. A l'aide des formules de Newton qui impliquent que $S_2 = \sigma_1^2 - 2\sigma_2$, $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, $S_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2$ et des relations entre racines et coefficients qui imposent $\sigma_2(x_1x_2x_3) = p$ et $\sigma_3(x_1x_2x_3) = -q$, on obtient que $V^2 = -4p^3 - 27q^2$. Comme p et q sont rationnels, V^2 l'est aussi.

Problème 2

1.1- Soit $x \in G$. Que $1 \in Z(x)$ est évident ; si $z, z' \in Z(x)$, on a successivement $xzz' = zxz' = zz'x$: $Z(x)$ est stable pour le produit ; en multipliant par z^{-1} à gauche et à droite l'égalité $xz = zx$, on obtient $z^{-1}x = xz^{-1}$: $Z(x)$ est stable pour le passage à l'inverse. Ainsi $Z(x)$ est-il un sous-groupe de G.

Soient $x, y \in G$. Si $z \in Z(yxy^{-1})$, alors $zyxy^{-1} = yxy^{-1}z$, ce qui s'écrit aussi $y^{-1}zyx = xy^{-1}zy$ en multipliant à droite par y et à gauche par y^{-1} ; cette dernière égalité montre que $y^{-1}zy \in Z(x)$, qui équivaut à $z \in yZ(x)y^{-1}$. On a montré que $Z(yxy^{-1}) \subseteq yZ(x)y^{-1}$. Inversement, si $z \in Z(x)$, on a successivement $(yzy^{-1})(yxy^{-1}) = yzxy^{-1} = yxzy^{-1} = (yxy^{-1})(yzy^{-1})$; cela montre que $yZ(x)y^{-1} \subseteq Z(yxy^{-1})$. Au bout du compte, $Z(yxy^{-1}) = yZ(x)y^{-1}$.

1.2- Si $\sigma \in Z((12))$, alors $\sigma(12)\sigma^{-1} = (12)$ Par ailleurs, $\sigma(12)\sigma^{-1} = (\sigma(1)\sigma(2))$ par la formule de conjugaison des cycles ; ainsi σ stabilise-t-il $\{1, 2\}$ et son complémentaire $\{3, 4, 5\}$.

Comme le produit d'une permutation de $\{1, 2\}$ par une permutation de $\{3, 4, 5\}$ commute avec (12), on obtient les 12 possibilités suivantes (deux choix pour les images de 1 et 2, six choix pour les images de 3, 4 et 5) : $Z((12)) = \{\mathrm{id}, (34), (35), (45), (345), (354), (12), (12)(34), (12)(35), (12)(45), (12)(345), (12)(354)\}$.

1.3- Soit $\sigma \in Z((12)(34))$; alors $\sigma(12)(34)\sigma^{-1} = (12)(34)$. Par ailleurs, $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$ par la formule de conjugaison des cycles. Alors, $\sigma(\{1,2\}) \in \{\{1,2\}, \{3,4\}\}$ et $\sigma(\{3,4\}) \in \{\{1,2\},\{3,4\}\}$. On obtient ainsi les 8 éléments suivants (considérer successivement toutes les images possibles de 1, 2, 3 et 4) : $\sigma \in Z((12)(34)) = \{\mathrm{id}, (34), (12), (12)(34), (1324), (13)(24), (1423), (14)(23)\}$. [Remarques : on pouvait s'attendre en effet à trouver les éléments du groupe de Klein de $\mathfrak{S}_4$ puisqu'il est abélien ; la notion d'action de groupe rendra les résultats des questions **1.2-** et **1.3-** presque automatiques).

1.4- Toute transposition de $\mathfrak{S}_5$ est conjuguée à (12). D'après **1.1-**, les centralisateurs des transpositions sont donc conjugués à un groupe d'ordre 12 : ils sont eux-mêmes d'ordre 12. De la même manière, puisque les produits de deux transpositions à supports disjoints sont tous conjugués à (12)(34), leurs centralisateurs sont d'ordre 8.

2.1- f_σ est bijective puisque $f_{\sigma^{-1}}$ est une réciproque. Par ailleurs, pour tous $t, t' \in \mathfrak{S}_5$, on a successivement $f_\sigma(tt') = \sigma tt'\sigma^{-1} = (\sigma t\sigma^{-1})(\sigma t'\sigma^{-1}) = f_\sigma(t)f_\sigma(t')$: cela montre que f_σ est un homomorphisme de groupes. Ainsi, $f_\sigma \in \mathrm{Aut}(\mathfrak{S}_5)$.

Soit $f : \mathfrak{S}_5 \to \mathrm{Aut}(\mathfrak{S}_5)$, $\sigma \mapsto f_\sigma$. Pour tous $\sigma, \sigma' \in \mathfrak{S}_5$ et pour tout $\tau \in \mathfrak{S}_5$, on a successivement $f_{\sigma\sigma'}(\tau) = (\sigma\sigma')\tau(\sigma\sigma')^{-1} = \sigma(\sigma'\tau\sigma'^{-1})\sigma^{-1} = f_\sigma(f_{\sigma'}(\tau)) = (f_\sigma \circ f_{\sigma'})(\tau)$. Cela montre que $f_{\sigma\sigma'} = f_\sigma \circ f_{\sigma'}$ pour tous $\sigma, \sigma' \in \mathfrak{S}_5$, c'est-à-dire que f est un homomorphisme de groupes.

Si σ est dans le noyau de f, alors σ est dans le centre de $\mathfrak{S}_5$ qui est trivial ; donc f est injectif.

2.2- Soient $x \in G$ et $\varphi \in \mathrm{Aut}(G)$.

On suppose que x est d'ordre 2. Comme $x \neq 1$ et φ est injectif, $\varphi(x) \neq 1$. Par ailleurs, $(\varphi(x))^2 = \varphi(x^2) = \varphi(1) = 1$. Cela montre que $\varphi(x)$ est d'ordre 2.

Si $z \in \varphi(Z(x))$, soit $y \in Z(x)$ tel que $z = \varphi(y)$. Alors, $z\varphi(x) = \varphi(yx) = \varphi(xy) = \varphi(x)z$, d'où $z \in Z(\varphi(x))$. Ainsi, $\varphi(Z(x)) \subseteq Z(\varphi(x))$.

Inversement, si $z \in Z(\varphi(x))$, soit $y = \varphi^{-1}(z)$. Alors, $\varphi(xy) = \varphi(x)z = z\varphi(x) = \varphi(yx)$ ce qui implique, puisque φ est injectif, que $xy = yx$: $y \in Z(x)$, soit encore $z = \varphi(y) \in \varphi(Z(x))$. Ainsi, $Z(\varphi(x)) \subseteq \varphi(Z(x))$. Au bout du compte, $\varphi(Z(x)) = Z(\varphi(x))$.

2.3- A l'aide de la décomposition des permutations en produits de cycles à supports disjoints, on voit immédiatemment que les éléments d'ordre 2 de $\mathfrak{S}_5$ sont les transpositions et les produits de deux transpositions à supports disjoints.

Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_5)$ et τ une transposition. D'après **2.2-**, $\varphi(\tau)$ est d'ordre deux, donc est une transposition ou un produit de deux transpositions à supports disjoints. D'après **1.4-**, le centralisateur de τ est d'ordre 12. Alors, d'après **2.2-**, le centralisateur de $\varphi(\tau)$ est également d'ordre 12. Ainsi $\varphi(\tau)$ ne peut-il pas être un produit de deux transpositions à supports disjoints (son centralisateur serait d'ordre 8 d'après **1.4-**). Donc c'est une transposition.

2.4- $\varphi((12))$ est une transposition (ab) et $\varphi((13))$ est une transposition (cd). On ne peut pas avoir $\{a,b\} = \{c,d\}$ ni $\{a,b\} \cap \{c,d\} = \emptyset$ car alors, (ab) et (cd) commuteraient ce qui n'est pas puisque (12) et (13) ne commutent pas (puisque φ est injectif, deux permutations s et t commutent si, et seulement si $\varphi(s)$ et $\varphi(t)$ commutent). Donc le cardinal de $\{a,b\} \cap \{c,d\}$ égale 1.

On note $a_1 \in \{1,\ldots,5\}$ l'élément commun entre les supports de $\varphi((12))$ et de $\varphi((13))$. Pour chaque $p \in \{2,\ldots,5\}$, soit alors $a_p \in \{2,\ldots,5\}$ tel que $\varphi((1p)) = (a_1 a_p)$ (pour a_4 et a_5, même raisonnement que pour a_2 et a_3 ; comme φ est injectif, les a_k sont tous distincts). On note $\alpha \in \mathfrak{S}_5$ la permutation définie par $\alpha(p) = a_p$ pour tout $p \in \{1,\ldots,5\}$. Alors, $\varphi((1p)) = \alpha(1p)\alpha^{-1} = f_\alpha((1p))$ pour tout $p \in \{1,\ldots,5\}$: les automorphismes φ et f_α coïncident sur les transpositions de la forme $(1p)$. A cause des formules du type $(13)(12)(13) = (23)$, cela montre que φ et f_α coïncident sur les transpositions de la forme $(k, k+1)$; comme ces dernières engendrent $\mathfrak{S}_5$, on obtient $\varphi = f_\alpha$: φ est intérieur.

UVSQ 2005/2006 31 janvier 2006
Licence de sciences et technologies
LSMA112 (algèbre 3)

Examen

(deux heures)

Questions de cours

1- Donner un exemple d'action transitive d'un groupe sur un ensemble.

2- Enoncer le premier théorème d'isomorphisme pour les groupes.

3- Soit V un espace vectoriel de dimension finie sur $\mathbb{R}$. Montrer que $\mathrm{SL}(V)$ est un sous-groupe distingué de $\mathrm{GL}(V)$ et que le quotient $\mathrm{GL}(V)/\mathrm{SL}(V)$ est isomorphe au groupe multiplicatif $\mathbb{R}^*$.

Problème 1

On note $\mathbb{F}_3$ le corps $\mathbb{Z}/3\mathbb{Z}$ et $\mathrm{SL}(2,\mathbb{F}_3)$ le groupe des matrices 2×2 à coefficients dans $\mathbb{F}_3$ dont le déterminant vaut 1.

1- Montrer que l'ordre de $\mathrm{SL}(2,\mathbb{F}_3)$ est 24. Quels sont les ordres des 2-sous-groupes de Sylow et des 3-sous-groupes de Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$?

2- Montrer que $T = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{F}_3\}$ est un sous-groupe de $\mathrm{SL}(2,\mathbb{F}_3)$. Est-il distingué dans $\mathrm{SL}(2,\mathbb{F}_3)$?

3- Calculer le nombre de 3-sous-groupes de Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$.

Problème 2

Soit G un groupe *infini*. On suppose que G contient un sous-groupe H différent de G dont l'indice dans G est *fini*.

1- On note $n = [G : H]$. Montrer que l'action de G par translation à gauche sur les classes à gauche modulo H, définie par $x.yH = xyH$ pour tous x et y dans H, induit un homomorphisme de groupes

$$\varphi : G \to \mathfrak{S}_n.$$

2- Montrer que φ n'est pas injectif.

3- Montrer que

$$\ker(\varphi) = \bigcap_{x\in G} xHx^{-1}$$

et en déduire que $\ker(\varphi) \neq G$.

4- Montrer que G n'est pas simple.

UVSQ 2005/2006 5 septembre 2006
Licence de sciences et technologies
LSMA112 (algèbre 3)

Examen, seconde session

(deux heures)

Problème 1 (7 points)

Soit n un entier naturel, $n \geq 5$.

1- Si $p \in \{1, \ldots, n\}$, quelle est la signature d'un p-cycle du groupe symétrique $\mathfrak{S}_n$?

2- Calculer le produit des deux 5-cycles (12345) et (12543).

3- Montrer que tout 3-cycle de $\mathfrak{S}_n$ est produit de deux 5-cycles.

4- Le groupe alterné $\mathfrak{A}_n$ est-il engendré par ses 5-cycles ?

Problème 2 (13 points)

Soit n un entier naturel non nul. On note B l'ensemble des matrices triangulaires supérieures du groupe linéaire $\mathrm{GL}(n, \mathbb{C})$:

$$B = \big\{(m_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}(n, \mathbb{C}),\ \forall (i,j),\ i > j \Longrightarrow m_{i,j} = 0\big\},$$

T l'ensemble des matrices diagonales de $\mathrm{GL}(n, \mathbb{C})$ et U l'ensemble des matrices de B dont tous les éléments diagonaux égalent 1. On admettra, sans chercher à le démontrer, que B, U et T sont des sous-groupes de $\mathrm{GL}(n, \mathbb{C})$.

Partie I

1- Soient $M = (m_{i,j})_{1 \leq i,j \leq n}$, $N = (n_{i,j})_{1 \leq i,j \leq n}$ et $P = (p_{i,j})_{1 \leq i,j \leq n}$ dans B, tels que $MN = P$. Montrer que $p_{i,i} = m_{i,i} n_{i,i}$ pour tout $i \in \{1 \ldots, n\}$.

2- Montrer que l'application $f : B \to T$ définie, pour tout $M = (m_{i,j})_{1 \leq i,j \leq n}$, par

$$f(M) = \begin{pmatrix} m_{1,1} & 0 & \ldots & 0 \\ 0 & m_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & m_{n,n} \end{pmatrix}$$

est un homomorphisme surjectif de groupes.

3- Montrer que U est un sous-groupe distingué de B et que B/U est isomorphe à T.

4- Le groupe T est-il isomorphe au groupe produit $(\mathbb{C}^*)^n$?

Partie II

On appelle *drapeau complet* de $\mathbb{C}^n$ tout n-uplet $E = (E_1, E_2, \ldots, E_n)$ de sous-espaces vectoriels de $\mathbb{C}^n$ tels que $\dim E_j = j$ pour tout $j \in \{1 \ldots n\}$ et tels que

$$E_1 \subset E_2 \subset \cdots \subset E_n = \mathbb{C}^n.$$

1- Pour tout $g \in \mathrm{GL}(n, \mathbb{C})$ et pour tout drapeau complet $E = (E_1, E_2, \ldots, E_n)$, on note $g.E$ le n-uplet de sous-espaces vectoriels

$$g.E = \big(g(E_1), g(E_2), \ldots, g(E_n)\big).$$

Montrer que $g.E$ ainsi défini est un drapeau complet et que l'application $(g, E) \mapsto g.E$ est une action du groupe $\mathrm{GL}(n, \mathbb{C})$ sur l'ensemble des drapeaux complets. Cette action est-elle transitive ?

2- On appelle *drapeau standard* le drapeau $S = (S_1, \ldots, S_n)$ où S_j est le sous-espace de $\mathbb{C}^n$ engendré par les j premiers vecteurs de la base canonique. Identifier le groupe d'isotropie du drapeau standard.

3- Expliciter une bijection entre l'ensemble des classes à gauche $\big(\mathrm{GL}(n, \mathbb{C})/B\big)_g$ et l'ensemble des drapeaux complets de $\mathbb{C}^n$.

UVSQ 2006/2007 16 mars 2007
Licence de sciences et technologies
LSMA212 (groupes et géométries)

Examen partiel

Question de cours (3 points)

Pour quelles valeurs de l'entier non nul n le groupe alterné $\mathfrak{A}_n$ est-il simple ? Donner la liste des éléments du groupe de Klein, sous-groupe distingué d'ordre 4 du groupe alterné $\mathfrak{A}_4$.

Problème 1 (6 points)

Dans l'anneau de polynômes $\mathbb{Z}[X, Y, Z]$, pour tout $k \in \{1, 2, 3\}$, on note σ_k le polynôme symétrique élémentaire de degré k et S_k le polynôme de Newton de degré k.

1- Question de cours : exprimer, sans démonstration, S_2 en fonction de σ_1 et σ_2.

2- On note P le polynôme symétrique $P(X, Y, Z) = X^2Y^2 + Y^2Z^2 + Z^2X^2$ (on ne demande pas de montrer que P est symétrique). Exprimer ${\sigma_2}^2$ en fonction de P et des σ_k, $1 \leq k \leq 3$. En déduire un polynôme $Q \in \mathbb{Z}[X, Y, Z]$ tel que $P = Q(\sigma_1, \sigma_2, \sigma_3)$.

3- Soit $R(X, Y, Z) = (X^2 - Y^2 - Z^2)(Y^2 - Z^2 - X^2)(Z^2 - X^2 - Y^2)$. Montrer que R est symétrique et l'écrire en fonction de σ_1, σ_2 et σ_3.

Problème 2 (11 points)

Dans le groupe symétrique $\mathfrak{S}_8$, on note

$$a = [3, 4, 2, 1, 7, 8, 6, 5],\ b = [5, 6, 8, 7, 2, 1, 3, 4],\ c = (12)(34)(56)(78),$$

et H le sous-groupe engendré par a et b.

1- Question de cours : donner deux définitions équivalentes du sous-groupe engendré par une partie A d'un groupe G (on ne demande pas de montrer que les deux définitions que l'on donnera sont équivalentes).

2- Décomposer a et b en produits de cycles à supports disjoints et calculer leurs signatures.

3- Calculer a^2 et b^2 en fonction de c et montrer que c est dans le centre de H (on rappelle que le centre d'un groupe est l'ensemble de ses éléments qui commutent avec tous les éléments du groupe).

4- Calculer les ordres de a, b et c et montrer que $ba = a^3b = cab$ (l'ordre d'un élément x

dans un groupe noté multiplicativement est le plus petit entier strictement positif n tel que $x^n = 1$).

5- Montrer que $H = \{a^p b^q,\ (p,q) \in \mathbb{Z}^2\}$ (on pourra vérifier auparavant que l'ensemble $\{a^p b^q,\ (p,q) \in \mathbb{Z}^2\}$ est un sous-groupe de H).

6- Déduire des questions précédentes que

$$H = \{c^p a^q b^r,\ (p,q,r) \in \{0,1\}^3\}.$$

Donner une liste exhaustive des éléments de H. Quel est son cardinal ?

7- Question de cours : donner la définition de sous-groupe distingué. Montrer que le sous-groupe engendré par a est distingué dans H. Quel est son cardinal ?

8- Montrer que tous les sous-groupes à 4 éléments de H sont distingués. Combien y en a-t-il ?

9- Est-il vrai que tous les sous-groupes de H sont distingués ? Le groupe H est-il commutatif ?

UVSQ 2006/2007 16 mars 2007
Licence de sciences et technologies
LSMA212 (groupes et géométries)

Corrigé succinct du partiel

Question de cours

Si $n \geq 5$, $\mathfrak{A}_n$ est simple (théorème du cours). Si $n = 1$, 2 ou 3, $\mathfrak{A}_n$ est également simple car il est cyclique, respectivement d'ordre 1, 2 ou 3. Le seul cas où $\mathfrak{A}_n$ n'est pas simple est le cas $n = 4$. Dans ces conditions, le groupe de Klein $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ en est un sous-groupe distingué.

Problème 1

1- $S_2 = \sigma_1^2 - 2\sigma_2$.

2- En développant, on obtient $\sigma_2^2 = (XY+XZ+YZ)^2 = P+2\sigma_1\sigma_3$. Ainsi, $P = \sigma_2^2 - 2\sigma_1\sigma_3$: le polynôme $Q(X, Y, Z) = Y^2 - 2XZ$ convient.

3- La transposition qui échange X et Y et fixe Z permute les deux premiers facteurs de R et laisse le troisième invariant ; elle fixe donc R. On montre ainsi de la même manière que R est fixé par les trois transpositions du groupe symétrique $\mathfrak{S}_3$. Comme ces dernières engendrent $\mathfrak{S}_3$, toutes les permutations fixent R : il est symétrique.

On développe : $R = (2X^2 - S_2)(2Y^2 - S_2)(2Z^2 - S_2) = 8\sigma_3^2 - 4S_2P + S_2^3$. En utilisant les questions précédentes, on obtient $R = \sigma_1^6 - 6\sigma_1^4\sigma_2 + 8\sigma_1^3\sigma_3 + 8\sigma_1^2\sigma_2^2 - 16\sigma_1\sigma_2\sigma_3 + 8\sigma_3^2$.

Problème 2

2- $a = (1, 3, 2, 4)(5, 7, 6, 8)$ et $b = (1, 5, 2, 6)(3, 8, 4, 7)$ sont des permutations paires.

3- Un calcul immédiat fournit $a^2 = b^2 = c$. Cela montre que c commute avec a et b, donc avec tous les éléments de H puisque ce dernier est engendré par a et b.

4- $c^2 = \mathrm{id}$ et $a^4 = b^4 = \mathrm{id}$ alors que $a^2 = b^2 = c \neq \mathrm{id}$. Donc c est d'ordre 2, et a et b sont d'ordre 4. Par le calcul, $ab = (1, 7, 2, 8)(3, 5, 4, 6)$ et $ba = cab = (1, 8, 2, 7)(3, 6, 4, 5)$. Par ailleurs, $cab = a^3b$ puisque $c = a^2$.

5- Par une récurrence immédiate, on montre que $b^pa^q = a^{3q}b$ pour tous $p, q \in \mathbb{Z}$. On note $I = \{a^pb^q,\ (p, q) \in \mathbb{Z}^2\}$. Que I soit non vide est évident. Si $p, q \in \mathbb{Z}$, alors $(a^pb^q)^{-1} = b^{-q}a^{-p} = a^{-3p}b^{-q} \in I$; cela montre que I est stable par passage à l'inverse. Si $p, q, r, s \in \mathbb{Z}$, alors $a^pb^qa^rb^s = a^{p+3r}b^{q+s} \in I$; cela montre que I est stable pour le produit. Au bout du compte, I est un sous-groupe de H. Comme le groupe I contient $a = a^1b^0$ et $b = a^0b^1$, il contient le sous-groupe engendré par a et b, c'est-à-dire H. Ainsi, $I = H$.

6- Soit $J = \{c^pa^qb^r,\ (p, q, r) \in \{0, 1\}^3\}$. Clairement, $J \subseteq H$ puisque $c = a^2$. Inversement, soient α et β dans $\mathbb{Z}$ et $x = a^\alpha b^\beta \in H$. On effectue la division euclidienne de α et de β par 2 : soient γ et δ dans $\mathbb{Z}$ et p et q dans $\{0, 1\}$ tels que $\alpha = 2\gamma + p$ et $\beta = 2\delta + q$. Alors, $x = c^\gamma a^p c^\delta b^q = c^{\gamma+\delta}a^pb^q$ (c est central d'après la question **3-**). Si $r \in \{0, 1\}$ désigne le reste de la division euclidienne de $\gamma + \delta$ par 2, alors $x = c^ra^pb^q \in J$. Cela montre que $H = J$.

Ainsi H est-il l'ensemble des $8 = 2^3$ permutations distinctes $\{\mathrm{id}, c, a, b, ab, ca, cb, cab\}$ (avec $ca = a^3$, $cb = b^3$, $cab = (ab)^3$).

7- On note $\langle a\rangle$ le groupe engendré par a. En utilisant les relations entre a et b des questions précédentes, $bab^{-1} = (ba)b^3 = a^3b^4 = a^3 \in \langle a\rangle$. Puisque $H = \langle a, b\rangle$, cela suffit à montrer

que $\langle a \rangle$ est distingué dans H. Comme a est d'ordre 4, le cardinal de $\langle a \rangle = \{\mathrm{id}, a, a^2, a^3\}$ est 4.

8- Les éléments d'ordre 4 de H sont a, b, ab, $a^3 = ca$, $b^3 = cb$ et $(ab)^3 = cab$. Donc H contient trois sous-groupes d'ordre 4, qui sont $\langle a \rangle$, $\langle b \rangle$ et $\langle ab \rangle$. Par un raisonnement analogue à celui de **7-**, ils sont tous distingués dans H.

9- Si un sous-groupe de H contient a et b, il égale H. Si un sous-groupe de H contient a^3 et b, il contient $a = (a^3)^3$; il égale donc H. Si un sous-groupe de H contient a et ab, il contient $b = a^3(ab)$; il égale donc H. Par des raisonnements analogues, on montre que les seuls sous-groupes de H contenant deux éléments d'ordre 4 sont H et les sous-groupes d'ordre 4 eux-mêmes.

Ainsi, outre les sous-groupes d'ordre 4, les sous-groupes de H sont :
- l'unique sous-groupe d'ordre 2 qui est central, donc distingué (c'est $\langle c \rangle$) ;
- $\{\mathrm{id}\}$ et H.

Tous sont distingués. Pour autant, H n'est pas abélien puisque a et b ne commutent pas.

NB : avec la théorie élémentaire des groupes finis, dresser la liste des sous-groupes de H est immédiat car on sait *a priori* que les seuls cardinaux possibles sont les diviseurs de 8.

UVSQ 2006/2007 21 mai 2007
Licence de sciences et technologies
LSMA212 (groupes et géométries)

Examen
(deux heures)

Question de cours (5 points)

1- Donner la définition de sous-groupe distingué. Donner un exemple d'un groupe non commutatif G et d'un sous-groupe distingué H de G tel que $H \notin \{\{1\}, G\}$.

2- Enoncer le premier théorème d'isomorphisme pour les groupes.

3- Soit G un groupe agissant sur un ensemble E. Montrer que tous les groupes d'isotropie des éléments d'une même orbite sont conjugués.

Problème 1 (5 points)

On note $\mathrm{SL}(2,\mathbb{Z})$ le sous-groupe de $\mathrm{SL}(2,\mathbb{R})$ défini par

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ (a,b,c,d) \in \mathbb{Z}^4,\ ad - bc = 1 \right\}$$

et $\mathrm{SL}(2,\mathbb{Z}/11\mathbb{Z})$ le groupe spécial linéaire sur le corps $\mathbb{Z}/11\mathbb{Z}$.

1- Pour tout entier x, on note $\overline{x}$ la classe de x modulo 11. Montrer que l'application

$$\begin{array}{rccc} f: & \mathrm{SL}(2,\mathbb{Z}) & \to & \mathrm{SL}(2,\mathbb{Z}/11\mathbb{Z}) \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \end{array}$$

est un homomorphisme de groupes.

2- On note $\Gamma = \{M \in \mathrm{SL}(2,\mathbb{Z}),\ f(M) = I_2\}$ où I_2 désigne la matrice identité de $\mathrm{SL}(2,\mathbb{Z}/11\mathbb{Z})$. Montrer que Γ est un sous-groupe distingué de $\mathrm{SL}(2,\mathbb{Z})$.

3- On admettra que le groupe $\mathrm{SL}(2,\mathbb{Z}/11\mathbb{Z})$ est engendré par les deux matrices

$$S = \begin{pmatrix} \overline{0} & \overline{1} \\ -\overline{1} & \overline{0} \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Montrer que f se factorise en un isomorphisme de groupes

$$\mathrm{SL}(2,\mathbb{Z})/\Gamma \xrightarrow{\sim} \mathrm{SL}(2,\mathbb{Z}/11\mathbb{Z}).$$

Problème 2 (10 points)

Dans l'espace vectoriel $\mathbb{R}^2$, on note $e_1 = (1,0)$, $e_2 = (0,1)$ et $\mathcal{C}$ le carré $\mathcal{C} = \{e_1, e_2, -e_1, -e_2\}$. On note G le sous-groupe des endomorphismes inversibles de $\mathbb{R}^2$ qui stabilisent $\mathcal{C}$:

$$G = \{g \in \mathrm{GL}(2,\mathbb{R}),\ g(\mathcal{C}) = \mathcal{C}\}.$$

1- On considère l'action de G sur $\mathcal{C}$, définie par $g.v = g(v)$ pour tout $(g,v) \in G \times \mathcal{C}$ (on ne demande pas de montrer que ceci est une action, on l'admettra).
Question de cours : montrer comment cette action définit un homomorphisme de groupes

$$\varphi : G \to \mathfrak{S}_{\mathcal{C}}.$$

Montrer que φ est injectif.

2- Dessiner le carré et montrer que cette action est transitive (on pourra par exemple considérer les matrices des symétries par rapport aux diagonales ou aux médianes de $\mathcal{C}$).

3- Soit $g \in G$ tel que $g(e_1) = e_1$. Montrer que $g(e_2) \in \{e_2, -e_2\}$. En déduire la liste des éléments de G qui fixent e_1.

4- Déduire l'ordre de G des questions **2-** et **3-**.

5- Numéroter les sommets du carré et donner la liste des permutations paires et des permutations impaires de $\varphi(G)$.

6- Montrer que l'application déterminant est une surjection $G \to \{-1,1\}$ et que G est isomorphe à un produit semi-direct

$$G \equiv \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}.$$

UVSQ 2006/2007 6 septembre 2007
Licence de sciences et technologies
LSMA212 (groupes et géométries)

Examen, seconde session
(deux heures)

Problème 1 (7 points)

1- (Question de cours) Soit n un entier naturel non nul. Montrer que le groupe quotient $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R})$ est isomorphe au groupe multiplicatif $\mathbb{R}^*$.

2- Montrer que l'application

$$\begin{array}{ccc} \mathbb{R}^* \times \mathrm{SL}(3,\mathbb{R}) & \to & \mathrm{GL}(3,\mathbb{R}) \\ (x,g) & \mapsto & xg \end{array}$$

est un homorphisme de groupes injectif. Le groupe $\mathrm{GL}(3,\mathbb{R})$ est-il isomorphe au produit direct $\mathbb{R}^* \times \mathrm{SL}(3,\mathbb{R})$?

3- L'homorphisme de groupes

$$\begin{array}{ccc} \mathbb{R}^* \times \mathrm{SL}(2,\mathbb{R}) & \to & \mathrm{GL}(2,\mathbb{R}) \\ (x,g) & \mapsto & xg \end{array}$$

est-il injectif ? Est-il surjectif ?

4- L'homorphisme de groupes

$$\begin{array}{ccc} \mathbb{C}^* \times \mathrm{SL}(2,\mathbb{C}) & \to & \mathrm{GL}(2,\mathbb{C}) \\ (x,g) & \mapsto & xg \end{array}$$

est-il injectif ? Est-il surjectif ?

Problème 2 (13 points)

Soit n un entier supérieur ou égal à 4. Pour toute permutation $\sigma \in \mathfrak{S}_n$, on note Z_σ le *centralisateur* de σ :

$$Z_\sigma = \{\tau \in \mathfrak{S}_n,\ \sigma\tau = \tau\sigma\}\ ;$$

c'est un sous-groupe de $\mathfrak{S}_n$ (on ne demande pas de démontrer cela).

1- Centralisateur d'un 3-cycle

1.1- Soient t une puissance du 3-cycle (123) et $s \in \mathfrak{S}_{\{4,\ldots,n\}}$. On considérera le groupe $\mathfrak{S}_{\{4,\ldots,n\}}$ comme un sous-groupe de $\mathfrak{S}_n$ en prolongeant toute permutation de $\{4,\ldots,n\}$ à $\{1,\ldots,n\}$ par l'identité sur $\{1,2,3\}$. Montrer que le produit ts est dans $Z_{(123)}$.

1.2- On note T le groupe engendré par (123). Montrer que l'application

$$\begin{array}{ccc} T \times \mathfrak{S}_{\{4,\ldots,n\}} & \to & \mathfrak{S}_n \\ (t,s) & \mapsto & ts \end{array}$$

est un homomorphisme injectif de groupes. En déduire que $|Z_{(123)}| \geq 3.(n-3)!$.

1.3- On considère l'action de $\mathfrak{S}_n$ sur lui-même par conjugaison, définie par $\sigma.\tau = \sigma\tau\sigma^{-1}$ pour toutes permutations σ et τ. Décrire l'orbite du 3-cycle (123) (**question de cours**) et calculer son cardinal. En déduire que l'ordre de $Z_{(123)}$ égale $3.(n-3)!$.

1.4- Montrer que $Z_{(123)}$ est isomorphe au produit direct de groupes $\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_{n-3}$.

1.5- Si c est n'importe quel 3-cycle de $\mathfrak{S}_n$, est-il vrai que son centralisateur Z_c est encore isomorphe au produit direct $\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_{n-3}$?

2- Centralisateur d'un produit de deux transpositions à supports disjoints

2.1- (Question de cours) On note K le groupe engendré par (12)(34) et (13)(24). Est-il abélien ? Quel est son ordre ?

2.2- Calculer le cardinal de l'orbite de (12)(34) sous l'action de $\mathfrak{S}_n$ sur lui-même par conjugaison. En déduire que l'ordre de $Z_{(12)(34)}$ est $8.(n-4)!$.

2.3- Montrer que le sous-groupe engendré par K et par la transposition (12) est contenu dans $Z_{(12)(34)}$. Est-il abélien ? Quel est son ordre ?

2.4- Montrer que si κ est un produit de deux transpositions à supports disjoints de $\mathfrak{S}_n$, son centralisateur Z_κ est isomorphe à $Z \times \mathfrak{S}_{n-4}$ où Z est un produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ entre les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

UVSQ 2009/2010
Licence de sciences et technologie, santé
LSMA212 (groupes et géométries)
12 mai 2010

Examen final (deux heures)

1 Questions de cours (5 points)

1.1- Pour quelles valeurs de $n \in \mathbb{N}^*$ le groupe alterné $\mathfrak{A}_n$ est-il simple ?

1.2- Est-il vrai que toute permutation de $\mathfrak{S}_9$ est un produit de 5-cycles ?

1.3- Montrer que le groupe multiplicatif $\mathbb{U}$ de toutes les racines de l'unité dans le corps des nombres complexes est isomorphe au groupe quotient $\mathbb{Q}/\mathbb{Z}$.

2 Premier problème (7 points)

Soient A et B les matrices de $\mathrm{GL}(2, \mathbb{C})$ définies par

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

On note H le sous-groupe de $\mathrm{GL}(2, \mathbb{C})$ engendré par A et B.

2.1- Calculer les ordres de A et B dans H et montrer les relations $BA = A^3B = -AB$.

2.2- Montrer que $\{A^pB^q,\ (p,q) \in \mathbb{Z}^2\}$ est un sous-groupe de $\mathrm{GL}(2, \mathbb{C})$. On le note K.

2.3- Montrer que $H = K$.

2.4- On note I l'élément neutre du groupe $\mathrm{GL}(2, \mathbb{C})$. Montrer que

$$H = \{(-I)^pA^qB^r,\ (p,q,r) \in \{0,1\}^3\}$$

et donner une liste exhaustive des éléments de H. Quel est l'ordre de H ?

2.5- Question de cours : donner la définition de sous-groupe distingué.
Montrer que le sous-groupe engendré par A est distingué dans H. Quel est son ordre ?

2.6- Pour chaque entier n, donner la liste des sous-groupes de H d'ordre n.

2.7- Les sous-groupes de H sont-ils tous distingués ? Le groupe H est-il commutatif ?

3 Second problème (8 points)

Soit $\mathcal{C}$ le "rectangle" de $\mathbb{R}^2$ défini par

$$\mathcal{C} = \{(1,2), (-1,2), (-1,-2), (1,-2)\}.$$

On note G le groupe des automorphismes linéaires de $\mathbb{R}^2$ qui préservent $\mathcal{C}$, c'est-à-dire

$$G = \{f \in \mathrm{GL}(\mathbb{R}^2),\ f(\mathcal{C}) = \mathcal{C}\}.$$

3.1- Dessiner $\mathcal{C}$ et montrer que $G = \{f \in \mathrm{GL}(\mathbb{R}^2),\ f(\mathcal{C}) \subseteq \mathcal{C}\}$.

3.2- On note $s \in \mathrm{GL}(\mathbb{R}^2)$ l'automorphisme dont la matrice dans la base canonique de $\mathbb{R}^2$ est $\begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix}$. Montrer que $s \in G$.

3.3- On considère l'action naturelle de G sur $\mathcal{C}$, définie par $f.c = f(c)$ pour tous $f \in G$ et $c \in \mathcal{C}$ (on ne demande pas de démontrer que c'est une action). Montrer que cette action est transitive.

3.4- On note $G_{(1,2)}$ le sous-groupe d'isotropie de $(1,2)$. Montrer que $|G_{(1,2)}| = 2$ et expliciter les éléments de $G_{(1,2)}$.

3.5- Calculer l'ordre de G.

3.6- On note $A = (1,2)$, $B = (-1,2)$, $C = (-1,-2)$ et $D = (1,-2)$. On note

$$\varphi : G \to \mathfrak{S}_{\mathcal{C}}$$

l'homomorphisme de groupes induit par l'action de G sur $\mathcal{C}$. Calculer le noyau de φ et l'image de s par φ. Montrer que l'image de φ contient le groupe de Klein de $\mathfrak{S}_{\mathcal{C}}$, qui en est le sous-groupe engendré par les produits de transpositions à supports disjoints. On notera K ce groupe de Klein.

3.7- Le groupe G est-il isomorphe au sous-groupe de $\mathfrak{S}_{\mathcal{C}}$ engendré par K et la transposition (B, D) ? Est-il commutatif ?

UVSQ 2009/2010
Licence de sciences et technologie, santé
LSMA212 (groupes et géométries)
12 mai 2010

Examen final : corrigé succinct

1- Questions de cours

1.1- $\mathfrak{A}_n$ est-il simple si, et seulement si $n \neq 4$.

1.2- La réponse est non. En effet, un 5-cycle est une permutation paire. Ainsi, le groupe engendré par les 5-cycles est inclus dans $\mathfrak{A}_9$; il est donc différent de $\mathfrak{S}_9$.

1.3- L'application $x \mapsto \exp(2i\pi x)$ est un homomorphisme de groupes $(\mathbb{Q}, +) \to (\mathbb{U}, \times)$. Il est surjectif et son noyau est $\mathbb{Z}$. On conclut avec le premier théorème d'isomorphisme.

2- Premier problème

2.1- Par le calcul, on trouve $A^2 = B^2 = -I$. Donc A et B sont d'ordre 4. Les relations $BA = A^3B = -AB$ se montrent par le calcul.

2.2- Soit $K = \{A^pB^q,\ (p,q) \in \mathbb{Z}^2\}$. On montre d'abord que si p et q sont des entiers relatifs, $A^pB^q = (-1)^{pq}B^qA^p$, à partir de la relation $AB = -BA$ (montrer d'abord par récurrence sur n que $A^nB = (-1)^nBA^n$ si n est positif, puis par récurrence sur q que pour tout p positif, $A^pB^q = (-1)^{pq}B^qA^p$. Pour passer aux négatifs, utiliser $A^{-1} = A^3$ et $B^{-1} = B^3$: si $p \leq 0$ et $q \geq 0$, $A^pB^q = A^{-3p}B^q$ et on est ramené au cas d'exposants positifs ou nuls, ce qui donne $A^pB^q = (-1)^{-3pq}B^qA^{-3p} = (-1)^{pq}B^qA^p$. Idem pour les deux autres cas.
Soient maintenant p, p', q et q' dans $\mathbb{Z}$. Alors, $A^pB^qA^{p'}B^{q'} = (-1)^{p'q}A^{p+p'}B^{q+q'} = A^{2p'q+p+p'}B^{q+q'} \in K$. Par ailleurs, $(A^pB^q)^{-1} = B^{-q}A^{-p} = (-1)^{pq}A^{-p}B^{-q} = A^{2pq-p}B^{-q}$ est également dans K. On a montré que K, qui est évidemment non vide, est stable par mutiplication et par passage à l'inverse : c'est un sous-groupe.

2.3- Comme A et B sont dans K (prendre respectivement $(p,q) = (1,0)$ puis $(p,q) = (0,1)$), le groupe H, engendré par A et B, est inclus dans K. Inversement, tout élément de K s'écrit comme produit de A, B, et de leurs inverses. Donc K est inclus dans H.

2.4- L'inclusion $\supseteq$ est évidente. Soit $A^aB^b \in H$ où a et b sont des entiers relatifs. D'après la question précédente, tout élément de H s'écrit ainsi. Soient $q, r \in \{0,1\}$ et $s, t \in \mathbb{Z}$ tels que $a = 2s + q$ et $b = 2t + r$ (division euclidienne par 2). Alors, $A^aB^b = (-1)^{st}A^qB^r$. Si on note p le reste de la division euclidienne de st par 2, on obtient ainsi $p, q, r \in \{0,1\}$ tels que $A^aB^b = (-I)^pA^qB^r$.
En prenant toutes les valeurs de $p, q, r \in \{0,1\}$, on obtient $H = \{\pm I, \pm A, \pm B, \pm AB\}$. Comme AB est distinct de $\pm I, \pm A, \pm B$ (calcul), cela montre que $|H| = 8$.

2.5- Puisque H est engendré par A et B, il suffit de montrer que $BAB^{-1} \in \langle A \rangle$ pour montrer que $\langle A \rangle \triangleleft B$. Or, $BAB^{-1} = BAB^3 = (-1)^3B.B^3A = -A = A^3 \in \langle A \rangle$. Puisque A est d'ordre 4, $|\langle A \rangle| = 4$.

2.6- Si n n'est pas un diviseur de 8, H n'a pas de sous-groupe d'ordre n (théorème de Lagrange). Le groupe trivial est le seul sous-groupe d'ordre 1 et H est son seul sous-groupe d'ordre 8. Restent les sous-groupes d'ordre 2 ou 4. Dans la liste des éléments de H, seul $-I$ est d'ordre 2 ; cela montre que $\langle -1 \rangle$ est le seul sous-groupe d'ordre 2 de H. Les sous-groupes d'ordre 4 sont $\langle A \rangle = \{\pm I, \pm A\}$, $\langle B \rangle$ et $\langle AB \rangle$.

2.7- Les sous-groupes d'ordre 4 sont d'indice 2, donc distingués. Le sous-groupe d'ordre 2 est central, donc distingué. Cela montre que tous les sous-groupes de H sont distingués dans H.
Pourtant, $AB = -BA \neq BA$: le groupe H n'est pas abélien.

3- Second problème

3.1- Si $f \in \mathrm{GL}(\mathbb{R}^2)$ vérifie $f(\mathcal{C}) \subseteq \mathcal{C}$, puisque f est une bijection, l'image par f de $\mathcal{C}$ a exactement 4 éléments et est contenue dans $\mathcal{C}$: c'est $\mathcal{C}$. Donc $\{f \in \mathrm{GL}(\mathbb{R}^2),\ f(\mathcal{C}) \subseteq \mathcal{C}\} \subseteq G$. L'autre inclusion est évidente.

3.2- Par le calcul, $s(1,2) = (1,2) \in \mathcal{C}$, $s(-1,2) = (1,-2) \in \mathcal{C}$. Donc $s \in G$ (inutile de calculer $s(-1,-2)$ ni $s(1,-2)$ puisque s est linéaire : $s(-x) = s(x)$ pour tout $x \in \mathbb{R}^2$).

3.3- Pour montrer que l'action est transitive, il suffit de montrer que tout élément de $\mathcal{C}$ est l'image de $(1,2)$ par (au moins) un élément de G. On le montre au cas par cas:
(i) $\mathrm{id}(1,2) = (1,2)$ et $\mathrm{id} \in G$ (!!!) ;
(ii) $s(1,2) = (1,-2)$ d'après la question **3.2-** ;
(iii) $-\mathrm{id} \in G$ (vérification facile) et $-\mathrm{id}(1,2) = (-1,-2)$;
(iv) $-s = -\mathrm{id}\,.s \in G$ et $-(s)(1,2) = (-1,2)$.
Donc l'action est transitive.

3.4- Si $f \in G$ fixe $(1,2)$, elle fixe aussi $(-1,-2)$ puisqu'elle est linéaire. Donc f fixe aussi $(-1,2)$ et $(1,-2)$, ou les échange. Dans tous les cas, puisque $((1,2),(-1,2))$ est une base de $\mathbb{R}^2$, tout $f \in G$ est déterminée par l'image de $(-1,2)$. Ou bien $f(-1,2) = f(-1,2)$ auquel cas $f = \mathrm{id}$. Ou bien $f(-1,2) = (1,-2)$ auquel cas $f = s$. Ainsi, $G_{(1,2)} = \{\mathrm{id}, s\}$ est d'ordre 2.

3.5- Puisque l'action n'a qu'une orbite à 4 éléments et puisque le groupe d'isotropie d'un élément de cette orbite est d'ordre 2, la formule des classes montre que $|G| = 4 \times 2 = 8$.

3.6- Par définition, $\varphi(g)(c) = g.c$ pour tous $g \in G$ et $c \in \mathcal{C}$.
Si $g \in \ker(\varphi)$, alors g fixe tous les éléments de $\mathcal{C}$. Or g est linéaire et $\mathcal{C}$ contient une base de $\mathbb{R}^2$. Donc $g = \mathrm{id}$: g est injectif.
On a vu que $s.A = A$, $s.B = D$, $s.C = C$ et $s.D = B$. Autrement dit, $\varphi(s)$ est la transposition (B,D).
$-\mathrm{id} \in G$ et $\varphi(-\mathrm{id}) = (A,C)(B,D)$. Donc $(A,C)(B,D) \in \mathrm{im}(\varphi)$. Par ailleurs, l'endomorphisme de $\mathbb{R}^2$ dont la matrice dans la base canonique est $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ envoie A sur B et C sur D : il est dans G et son image par φ est $(A,B)(C,D)$. Donc $(A,B)(C,D) \in \mathrm{im}(\varphi)$. Ainsi, le groupe engendré par $(A,B)(C,D)$ et $(A,C)(B,D)$, qui est le groupe de Klein K, est contenu dans $\mathrm{im}(\varphi)$.

3.7- Puisque φ est injectif, il définit un isomorphisme de G sur son image. Cette dernière est donc un groupe d'ordre 8. Par ailleurs, $\mathrm{im}(\varphi)$ contient K et la transposition (B,D). Donc elle contient le groupe engendré par K et (B,D) qui est d'ordre supérieur ou égal à 8. Cela montre que $\mathrm{im}(\varphi) = \langle K, (B,D)\rangle \sim G$.
Ce groupe n'est pas commutatif car $(B,D).(A,B)(C,D) = (A,D,C,B)$ alors que $(A,B)(C,D).(B,D) = (A,B,C,D)$.

UVSQ 2009/2010
Licence de sciences et technologie, santé
LSMA212 (groupes et géométries)
25 juin 2010

Examen final (deux heures)

1 Questions de cours (6 points)

1.1 Donner la définition d'un sous-groupe distingué.

1.2 Enoncer le premier théorème d'isomorphisme pour les groupes.

1.3 Prouver que le groupe quotient $\mathrm{GL}(n, \mathbb{C})/\mathrm{SL}(n, \mathbb{C})$ est isomorphe au groupe multiplicatif $\mathbb{C}^*$.

2 Problème (14 points)

On note $\mathrm{GL}(\mathbb{R}^2)$ le groupe des endomorphismes inversibles de l'espace vectoriel réel $\mathbb{R}^2$. On note $\mathcal{G}_1$ l'ensemble des droites vectorielles de $\mathbb{R}^2$. On considère l'*action naturelle* de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_1$, définie par

$$\forall g \in \mathrm{GL}(\mathbb{R}^2),\ \forall D \in \mathcal{G}_1,\ g \cdot D = g(D)$$

(on ne demande pas de démontrer que cela définit une action).

2.1 L'action naturelle de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_1$ est-elle transitive ?

2.2 On suppose que $f \in \mathrm{GL}(\mathbb{R}^2)$ a la propriété suivante : pour tout $u \in \mathbb{R}^2$, il existe $\lambda_u \in \mathbb{R}$ tel que $f(u) = \lambda_u u$.

2.2.1 Soit (u, v) une famille libre de vecteurs de $\mathbb{R}^2$. En calculant $f(u + v)$ de deux façons, montrer que $\lambda_u = \lambda_v$.

2.2.2 Soit (u, v) une famille liée de vecteurs de $\mathbb{R}^2$. En considérant un troisième vecteur linéairement indépendant de u et v, montrer que $\lambda_u = \lambda_v$.

2.2.3 Déduire des questions précédentes que f est une *homothétie vectorielle*, c'est-à-dire qu'il existe $a \in \mathbb{R}^*$ tel que $f = a\,\mathrm{id}_{\mathbb{R}^2}$.

2.3 Soit $\varphi : \mathrm{GL}(\mathbb{R}^2) \to \mathfrak{S}_{\mathcal{G}_1}$ l'homomorphisme de groupes induit par l'action de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_1$. Calculer le noyau de φ.

2.4 On note $\mathcal{G}_2$ l'ensemble formé des couples de droites vectorielles distinctes de $\mathbb{R}^2$. On considère l'*action naturelle* de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_2$, définie par

$$\forall g \in \mathrm{GL}(\mathbb{R}^2),\ \forall (D_1, D_2) \in \mathcal{G}_2,\ g \cdot (D_1, D_2) = (g(D_1), g(D_2)).$$

Dire rapidement pourquoi cela définit bien une action. Est-elle transitive ?

2.5 Si $(D_1, D_2) \in \mathcal{G}_2$, on note $\mathrm{Isot}(D_1, D_2)$ le groupe d'isotropie de (D_1, D_2) sous l'action naturelle de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_2$. On note $I = \mathbb{R}(1, 0)$ et $J = \mathbb{R}(0, 1)$ les droites portées par les vecteurs de la base canonique de $\mathbb{R}^2$. Montrer que pour tout $(D_1, D_2) \in \mathcal{G}_2$, les groupes $\mathrm{Isot}(D_1, D_2)$ et $\mathrm{Isot}(I, J)$ sont conjugués dans $\mathrm{GL}(\mathbb{R}^2)$.

2.6 Montrer que le groupe $\mathrm{Isot}(I, J)$ est le groupe des automorphismes de $\mathbb{R}^2$ dont la matrice dans la base canonique de $\mathbb{R}^2$ est diagonale, et que ce groupe est isomorphe au groupe multiplicatif produit $\mathbb{R}^* \times \mathbb{R}^*$.

2.7 Montrer que pour tout $(D_1, D_2) \in \mathcal{G}_2$, $\mathrm{Isot}(D_1, D_2)$ est isomorphe à $\mathbb{R}^* \times \mathbb{R}^*$.

2.8 On note $\mathcal{G}_3$ l'ensemble formé des triplets de droites vectorielles distinctes de $\mathbb{R}^2$. On considère l'*action naturelle* de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_3$, définie par

$$\forall g \in \mathrm{GL}(\mathbb{R}^2),\ \forall (D_1, D_2, D_3) \in \mathcal{G}_3,\ g \cdot (D_1, D_2, D_3) = (g(D_1), g(D_2), g(D_3))$$

(on ne demande pas de vérifier que cela définit une action).

2.8.1 Montrer que si $(D_1, D_2, D_3) \in \mathcal{G}_3$, il existe $v_1 \in D_1$ et $v_2 \in D_2$ tels que $v_1 + v_2$ soit une base de D_3.

2.8.2 Montrer que l'action naturelle de $\mathrm{GL}(\mathbb{R}^2)$ sur $\mathcal{G}_3$ est transitive.

2.8.3 Montrer que pour tout $(D_1, D_2, D_3) \in \mathcal{G}_3$, le groupe d'isotropie de (D_1, D_2, D_3) pour l'action naturelle de $\mathrm{GL}(\mathbb{R}^2)$ est le groupe des homothéties vectorielles (voir la question **2.2.3** pour la définition d'une homothétie vectorielle).

UVSQ 2010/2011
Licence de sciences et technologie, santé
LSMA610 (groupes et géométries)
lundi 16 mai 2011

Examen
(deux heures)

1 Question de cours (3 points)

Soient A un anneau et B un sous-anneau de A. Donner la définition d'un élément de A algébrique sur B. Donner un exemple d'un nombre réel non rationnel algébrique sur $\mathbb{Q}$ (avec la preuve de son algébricité).

2 Exercice (5 points)

2.1 Soient G un groupe et $Z(G)$ son centre. On suppose que $Z(G)$ a un sous-groupe H tel que le groupe-quotient G/H soit monogène. Montrer qu'il existe $g \in G$ tel que G soit engendré par $H \cup \{g\}$. En déduire que G est nécessairement abélien.

2.2 Soient p un nombre premier et G un groupe d'ordre p^2. En considérant le quotient de G par son centre, montrer que G est abélien. En déduire que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou au groupe produit $(\mathbb{Z}/p\mathbb{Z})^2$.

3 Problème (12 points)

Soit p un nombre premier. On note $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ le groupe des matrices carrées 2×2 à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ inversibles. On note $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ son sous-groupe des matrices dont le déterminant égale 1.

3.1 Question de cours
Démontrer que $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ est un sous-groupe distingué de $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ et que le groupe quotient $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})/\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ est isomorphe au groupe multiplicatif $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.

3.2 Question de cours
Démontrer que l'ordre de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ égale $p(p^2 - 1)$.

3.3 Soit

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Montrer que U est un sous-groupe de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ et calculer son ordre.

3.4 U est-il cyclique ?

3.5 U est-il distingué dans $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$?

3.6 Montrer que U est un p-sous-groupe de Sylow de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$. Calculer le nombre de p-sous-groupes de Sylow de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$.

3.7 Montrer que l'action par conjugaison de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ sur l'ensemble de ses p-sous-groupes de Sylow induit un homomorphisme de groupes

$$\varphi : \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z}) \to \mathfrak{S}_{p+1}$$

où $\mathfrak{S}_{p+1}$ désigne le groupe des permutations de $p+1$ objets. Combien cette action a-t-elle d'orbites ?

3.8 On note

$$I(U) = \left\{ g \in \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z}),\ gUg^{-1} = U \right\}$$

le groupe d'isotropie de U sous l'action de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ définie au **3.7**. Calculer l'ordre de $I(U)$.

3.9 On note

$$D = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix},\ x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \right\}.$$

Le sous-ensemble D est-il un sous-groupe de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$? Calculer son cardinal.

3.10 Montrer que $I(U)$ contient le sous-groupe $\langle D, U \rangle$ de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ engendré par U et D. En déduire que $I(U) = \langle D, U \rangle$.

3.11 En calculant le noyau de φ, montrer que le quotient $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})/\{\pm I_2\}$ est isomorphe à un sous-groupe de $\mathfrak{S}_{p+1}$.

3.12 Montrer que $\mathrm{SL}(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3$ et que $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})/\{\pm I_2\} \simeq \mathfrak{A}_4$ où $\mathfrak{A}_4$ désigne le groupe des permutations paires de 4 objets.

UVSQ 2010/2011
Licence de sciences et technologie, santé
LSMA610 (groupes et géométries)
lundi 16 mai 2011

Corrigé succinct de l'examen

2 Exercice
2.1 Soit $g \in G$ tel que le quotient G/H soit engendré par gH. Alors, pour tout $x \in G$, il existe $n \in \mathbb{Z}$ tel que $xH = g^n H$. En particulier, $x \in g^n H$. Cela montre que g et H engendrent G.
Comme H est central ($H \subseteq Z(G)$), g commute avec tout élément de H. Puisque G est engendré par g et H, il est commutatif.
2.2 Puisque G est un p-groupe, son centre n'est pas réduit à $\{1\}$. Comme l'ordre de $Z(G)$ divise p^2, le théorème de Lagrange assure que ce nombre vaut p ou p^2. Si $|Z(G)| = p$, le quotient $G/Z(G)$ est cyclique puisqu'il est d'ordre premier p ; d'après la question **2.1**, cela entraîne que G est abélien et donc que $|Z(G)| = |G| = p^2 \neq p$, ce qui contredit l'hypothèse $|Z(G)| = p$. Ainsi, $|Z(G)| = p^2$, ce qui signifie que $G = Z(G)$ est abélien.
Si G contient un élément d'ordre p^2, il est cyclique, isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Sinon, tous les éléments de $G \setminus \{1\}$ sont d'ordre p ; soient alors $x \in G \setminus \{1\}$ et $y \in G$ tel que $y.\langle x \rangle$ engendre le groupe $G/\langle x \rangle$ qui est d'ordre p donc cyclique. Alors, $G = \langle x, y \rangle$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.

3 Problème
3.1 L'application déterminant $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ est un homomorphisme surjectif de groupes dont le noyau est $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$. Cela montre, d'après le premier théorème d'isomorphisme, que $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ est un sous-groupe distingué de $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ et que le groupe quotient

$$\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) / \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$$

est isomorphe au groupe multiplicatif $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.
3.2. L'ordre de $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ égale $(p^2-1)(p^2-p)$ (question de cours, compter les bases). D'après la question **3.1**, l'ordre de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ est donc $(p^2-1)(p^2-p)/(p-1) = p(p^2-1)$.
3.3 Un calcul matriciel élémentaire montre que le produit et l'inverse d'éléments de U sont encore dans U. Comme U est non vide, cela montre que U est un sous-groupe de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$.
Par ailleurs, l'application $a \in \mathbb{Z}/p\mathbb{Z} \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in U$ est évidemment bijective (c'est même un isomorphisme de groupes), ce qui entraîne que $|U| = p$.
3.4 U est cyclique car son ordre est un nombre premier.
5. Le calcul matriciel $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ montre que U n'est pas distingué dans $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$.
6. Puisque $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z}) = p(p^2-1)$, les p-Sylow de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ sont d'ordre p. Comme U est un sous-groupe d'ordre p de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$, c'en est un p-Sylow.
D'après les théorèmes de Sylow, le nombre n de p-Sylow de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ divise $p(p^2-1)$ et est congru à 1 modulo p : soit $m \in \mathbb{N}^*$ tel que $nm = p^2 - 1$ (d'après le théorème de Gauß, n divise p^2-1 puisqu'il est premier avec p). Alors, $m \equiv -1\ [p]$. En particulier, $m \geq p-1$. Par ailleurs, $n \neq 1$ car U, qui est un p-Sylow, n'est pas distingué (ses conjugués sont aussi des p-Sylow) ; ainsi, $n \geq p+1$ puisque $n \equiv 1\ [p]$. Des inégalités $m \geq p-1$ et $n \geq p+1$ et de l'égalité $nm = (p-1)(p+1)$ on déduit que $n = p+1$ (et que $m = p-1$).
7. L'action par conjugaison de $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ sur l'ensemble $\mathcal{S}$ de ses p-sous-groupes de Sylow induit un homomorphisme de groupes $\varphi : \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z}) \to \mathfrak{S}_{\mathcal{S}} \simeq \mathfrak{S}_{p+1}$.
Les p-Sylow sont tous conjugués (théorèmes de Sylow), ce qui signifie que cette action n'a qu'une seule orbite (elle est transitive).

8. L'unique orbite de l'action a $p+1$ éléments. On en déduit que les groupes d'isotropie ont tous pour ordre $|I(U)| = |\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})|/(p+1) = p(p-1)$.
9. D est non vide, stable par produit et passage à l'inverse (calcul élémentaire) : c'est un sous-groupe de $\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})$. L'application $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \mapsto \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} \in D$ est un isomorphisme de groupes (calcul élémentaire, de nouveau). Donc D est un sous-groupe (cyclique) d'ordre $p-1$.
10. U est évidemment dans son groupe d'isotropie $I(U)$. Par ailleurs, le calcul matriciel

$$\begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix}^{-1} = \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \in U$$

montre que $D \subseteq I(U)$. Puisque $I(U)$ contient D et U, il contient le groupe $\langle D, U\rangle$ qu'ils engendrent. Le groupe $\langle D, U\rangle$ contient le sous-groupe U d'ordre p et le sous-groupe D d'ordre $p-1$. D'après le théorème de Lagrange, puisque p et $p-1$ sont premiers entre eux, $|\langle D, U\rangle|$ est un multiple de $p(p-1) = |I(U)|$. Comme $I(U)$ contient $\langle D, U\rangle$, cela entraîne que $I(U) = \langle D, U\rangle$.
11. Soit $g \in \ker(\varphi)$. Alors, g stabilise (par conjugaison) tous les p-Sylow de $\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})$. En particulier, g est dans $I(U)$ qui est formé de matrices trigonales supérieures. En conjuguant comme dans la question **5**, on obtient que g est aussi une matrice trigonale inférieure. En rassemblant ces deux résultats, on conclut que g est une matrice diagonale de $\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})$, c'est-à-dire un élément de D. Soit $x \in \mathbb{Z}/p\mathbb{Z}$, $x \neq 0$, tel que $g = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix}$. Alors, si $t = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, le groupe tUt^{-1} est un p-Sylow de $\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})$. Ainsi, g le stabilise ce qui signifie que $gtUt^{-1}g^{-1} = tUt^{-1}$, c'est-à-dire que $t^{-1}gt \in I(U)$. Or, le calcul montre que $t^{-1}gt = \begin{pmatrix} x & 0 \\ -x+1/x & 1/x \end{pmatrix}$ qui n'est dans $I(U)$ que lorsque $x = 1$ ou $x = -1$ ($I(U)$ n'est formé que de matrices trigonales supérieures).
Par ailleurs, I_2 et $-I_2$ sont dans le noyau de φ puisqu'elles sont dans le centre de $\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})$. On a ainsi montré que $\ker(\varphi) = \{\pm I_2\}$.
La propriété universelle du quotient montre alors que φ induit un homomorphisme injectif de groupes $\overline{\varphi} : \operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})/\{\pm I_2\} \to \mathfrak{S}_{p+1}$ Le quotient $\operatorname{SL}(2,\mathbb{Z}/p\mathbb{Z})/\{\pm I_2\}$ est alors isomorphe à son image qui est un sous-groupe de $\mathfrak{S}_{p+1}$.
12. Cas $p = 2$: dans ce cas, $I_2 = -I_2$ et φ est injectif. Comme $|\operatorname{SL}(2,\mathbb{Z}/2\mathbb{Z})| = |\mathfrak{S}_3| = 6$, φ est un isomorphisme de groupes.
Cas $p = 3$: dans ce cas, $|\operatorname{SL}(2,\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\}| = 12$ est isomorphe à un sous-groupe d'ordre 12 de $\mathfrak{S}_4$. Comme le seul sous-groupe d'indice 2 de $\mathfrak{S}_4$ est $\mathfrak{A}_4$ (théorème du cours), cela montre l'isomorphisme demandé.

UVSQ 2010/2011
Licence de sciences et technologie, santé
LSMA610 (groupes et géométries)
Mardi 21 juin 2011

Examen
(deux heures)

1 Question de cours (5 points)

1. Qu'est-ce qu'un polynôme symétrique ?

2. Soient n un entier naturel non nul et $k \in \{1, \ldots, n\}$. Donner la définition du $k^{\text{ième}}$ polynôme symétrique élémentaire à n indéterminées.

3. Exprimer le second polynôme de Newton (somme des carrés des indéterminées) en fonction des polynômes symétriques élémentaires.

2 Problème 1 (9 points)

Si G est un groupe, on appelle *caractère* de G tout homomorphisme de groupes $G \to \mathbb{C}^*$.

1. Si χ_1 et χ_2 sont des caractères d'un groupe G, montrer que l'application

$$\begin{array}{rccc} \chi_1\chi_2 : & G & \longrightarrow & \mathbb{C}^* \\ & g & \longmapsto & \chi_1(g)\chi_2(g) \end{array}$$

est encore un caractère de G et que l'opération $(\chi_1, \chi_2) \mapsto \chi_1\chi_2$ confère à l'ensemble des caractères de G une structure de groupe. Dans toute la suite du problème, on notera $\widehat{G}$ le groupe des caractères du groupe G.

2. Soient G un groupe, N un sous-groupe distingué de G et $p : G \to G/N$ la projection canonique. Montrer que l'application

$$\begin{array}{ccc} \widehat{G/N} & \longrightarrow & \widehat{G} \\ \chi & \longmapsto & \chi \circ p \end{array}$$

est un homomorphisme injectif de groupes.

3. Montrer que $\widehat{\mathbb{Z}}$ est isomorphe à $\mathbb{C}^*$.

4. Montrer que si un groupe est cyclique, il est isomorphe à son groupe des caractères.

5. Question de cours
On note K le sous-groupe de Klein du groupe symétrique $\mathfrak{S}_4$. Donner une définition de K. Quel est l'ordre de K ? Est-il commutatif ?

6. On note $\mathfrak{A}_4$ le sous-groupe de $\mathfrak{S}_4$ formé de ses permutations paires. Calculer l'ordre du groupe $\mathfrak{A}_4/K$; son groupe des caractères est-il cyclique ?

7. Montrer que $\widehat{\mathfrak{A}_4}$ n'est pas le groupe trivial.

8. Question de cours
Soit $n \geq 5$ un entier naturel. Quels sont les sous-groupes distingués du groupe alterné $\mathfrak{A}_n$?

9. Montrer que si $n \geq 5$, le groupe des caractères de $\mathfrak{A}_n$ est trivial.

3 Problème 2 (6 points)

Soit G un groupe *infini*. On suppose que G contient un sous-groupe H différent de G dont l'indice dans G est *fini*.

1- On note $n = [G : H]$. Montrer que l'action de G par translation à gauche sur les classes à gauche modulo H, définie par $x.yH = xyH$ pour tous x et y dans G, induit un homomorphisme de groupes

$$\varphi : G \to \mathfrak{S}_n.$$

2- Montrer que φ n'est pas injectif.

3- Montrer que

$$\ker(\varphi) = \bigcap_{x \in G} xHx^{-1}$$

et en déduire que $\ker(\varphi) \neq G$.

4- Montrer que G n'est pas simple.

UVSQ 2011/2012
Licence de sciences et technologie, santé
LSMA510 (combinatoire), L3 mathématiques et L3 informatique
Jeudi 29 mars 2012

Examen partiel (une heure et demie)

1 Question de cours (4 points)

1- Donner un exemple d'un sous-groupe **non** distingué (en justifiant qu'il ne l'est pas).

2- Démontrer soigneusement que les groupes $\mathbb{C}/\mathbb{Z}$ et $\mathbb{C}^*$ sont isomorphes.

2 Problème 1 (5 points)

1- Question de cours
Dans le groupe symétrique $\mathfrak{S}_5$, quel est l'inverse du 5-cycle (12345) ? Calculer le produit (123)(12345).

2- Montrer que pour tout entier naturel $n \geq 5$, le groupe alterné $\mathfrak{A}_n$ est engendré par ses 5-cycles.

3- Soient $\sigma = (1234)(5678)$ et $\tau \in \mathfrak{S}_8$. Montrer que le conjugué $\tau\sigma\tau^{-1}$ est un produit de deux 4-cycles à supports disjoints.

4- On appelle permutation $(4,4)$ tout produit de deux 4-cycles à supports disjoints. Démontrer que si $n \geq 8$, le sous-groupe de $\mathfrak{S}_n$ engendré par les permutations $(4,4)$ est le groupe alterné $\mathfrak{A}_n$.

3 Problème 2 (5 points)

Pour tout entier naturel non nul n, on note $\mathrm{GL}(n,\mathbb{C})$ le groupe des matrices carrées 2×2 à coefficients complexes inversibles et $\mathrm{SL}(n,\mathbb{C})$ son sous-groupe des matrices dont le déterminant égale 1.

1- Montrer que l'application

$$\begin{array}{rccc} f: & \mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C}) & \longrightarrow & \mathrm{GL}(n,\mathbb{C}) \\ & (z,A) & \longmapsto & zA \end{array}$$

est un homomorphisme de groupes.

2- Calculer l'image de f.

3- Montrer que le noyau de f est isomorphe au groupe $\mathbb{U}_n$ des racines $n^{\text{ièmes}}$ complexes de l'unité.

4- Montrer que $\mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C})$ contient un sous-groupe distingué H isomorphe à $\mathbb{U}_n$ tel que $\mathrm{GL}(n,\mathbb{C})$ soit isomorphe au groupe quotient $\mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C})/H$.

4 Problème 3 (6 points)

Soient n un entier naturel impair et G un groupe fini d'ordre $2n$.

L'objet du problème consiste à montrer que G contient nécessairement un sous-groupe distingué d'ordre n.

1- On note 1 le neutre de G. Soit $E = \{x \in G,\ x^2 \neq 1\}$. Montrer que pour tout $x \in G$,

$$x \in E \Longrightarrow x^{-1} \in E.$$

En déduire successivement que le cardinal de E est un nombre pair, que le cardinal de $G \setminus E$ est également pair, et enfin que G contient au moins un élément d'ordre 2.

2- Soit z un élément d'ordre 2 de G. On note

$$\begin{array}{rccc} \sigma : & G & \longrightarrow & G \\ & x & \longmapsto & zx. \end{array}$$

Montrer que σ est une permutation d'ordre 2 sans point fixe de G et calculer sa signature.

3- On note $\mathfrak{S}_G$ le groupe des permutations de G. Soit $\Phi : G \longrightarrow \mathfrak{S}_G$ l'application définie par :

$$\forall y \in G,\ \forall x \in G,\ \Phi(y)(x) = yx.$$

Question de cours : montrer que Φ est un homomorphisme de groupes.
Qu'est $\Phi(z)$?

4- On note $f = \varepsilon \circ \Phi : G \longrightarrow \{-1, 1\}$, où ε désigne la signature. Montrer que f est surjectif. En déduire que G contient un sous-groupe distingué d'ordre n.

UVSQ 2010/2011
Licence de sciences et technologie, santé
LSMA510 (combinatoire), L3 mathématiques et L3 informatique
Jeudi 29 mars 2012

Corrigé succinct du partiel

1 Problème 1

1- $(12345)^{-1} = (15432)$ et $(123)(12345) = (13452)$.
2- On déduit de **1-** que $(123) = (13452)(15432)$. Quitte à renuméroter, cela montre que tout 3-cycle de $\mathfrak{A}_n$ est un produit de deux 5-cycles dès lors que $n \geq 5$. Comme les 3-cycles engendrent $\mathfrak{A}_n$, cela suffit à montrer que les 5-cycles l'engendrent également.
3- D'une part, $\tau\sigma\tau^{-1} = (\tau(1234)\tau^{-1})(\tau(5678)\tau^{-1})$. D'autre part, le conjugué d'un 4-cycle est encore un 4-cycle (formule de conjugaison des cycles). Ainsi $\tau\sigma\tau^{-1}$ est-il un produit de deux 4-cycles.
4- Soit H le sous-groupe de $\mathfrak{S}_n$ engendré par les permutations $(4,4)$. Comme les permutations $(4,4)$ sont paires, H est un sous-groupe de $\mathfrak{A}_n$, non trivial. Par ailleurs, le **3-** montre que H est un sous-groupe distingué dans $\mathfrak{S}_n$, donc dans $\mathfrak{A}_n$. Mais puisque $n \geq 5$, $\mathfrak{A}_n$ est un groupe simple. Donc $H = \mathfrak{A}_n$.

2 Problème 2

1- $f(z,A)f(z',A') = (zA)(z'A') = zz'AA' = f(zz',AA')$ (notations évidentes). Donc f est un homomorphisme de groupes.
2- $\mathrm{im}(f) = \mathrm{GL}(n,\mathbb{C})$. En effet, soient $P \in \mathrm{GL}(n,\mathbb{C})$ et $d = \det(P) \in \mathbb{C}^*$. Soit alors $z \in \mathbb{C}^*$ tel que $z^n = d$ (un tel z existe car le corps des nombres complexes est algébriquement clos). Soit alors $A = z^{-1}P$. Clairement, $\det(A) = \det(z^{-1}P) = z^{-n}\det P = 1$, ce qui montre que $A \in \mathrm{SL}(n,\mathbb{C})$. Enfin, $f(z,A) = P$, c'est fait exprès.
3- $\ker(f) = \{(z,A) \in \mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C}),\ zA = I_n\}$. Soit $(z,A) \in \ker(f)$. Alors, z est une racine $n^{ième}$ de l'unité puisque $1 = \det(zA) = z^n\det(A) = z^n$. Par ailleurs, $A = z^{-1}I_n$. On a ainsi montré que $(z,A) \in \ker(f) \Longrightarrow z \in \mathbb{U}_n$ et $A = \frac{1}{z}I_n$. Inversement, si $z \in \mathbb{U}_n$, il est clair que $(z, z^{-1}I_n) \in \ker(f)$. Bref, $\ker(f) = \left\{\left(z, z^{-1}I_n\right)\ z \in \mathbb{U}_n\right\}$.
Par conséquent, l'image de l'application $\varphi : z \in \mathbb{U}_n \longmapsto \left(z, z^{-1}I_n\right) \in \mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C})$ égale $\ker(f)$. Par ailleurs, on vérifie facilement que φ est un homomorphisme injectif de groupes. Au bout du compte, φ définit un isomorphisme de groupes entre $\mathbb{U}_n$ et $\ker(f)$.
4- Soit $H = \ker(f) \triangleleft \mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C})$. Puisque f est surjectif, le premier théorème d'isomorphisme pour les groupes montre que f se factorise en un isomorphisme de groupes entre $\mathrm{GL}(n,\mathbb{C})$ et le quotient $\mathbb{C}^* \times \mathrm{SL}(n,\mathbb{C})/H$. Enfin, le **3-** montre que H est isomorphe à U_n.

3 Problème 3

1- Pour tout $x \in G$, $x^2 = 1 \Longleftrightarrow (x^{-1})^2 = 1$; ainsi, $x \in E \Longleftrightarrow x^{-1} \in E$. On en déduit que chaque fois que $x \in E$, on a simultanément $x^{-1} \in E$ et $x \neq x^{-1}$: les éléments de E se comptent par deux, ce qui prouve que le cardinal de E est pair (pour une preuve plus formelle, on peut par exemple considérer l'application $x \mapsto x^{-1}$ comme une permutation de E, involutive et sans point fixe : sa décomposition en produit de cycles à supports disjoints est un produit de transpositions dont la réunion des supports est E ; cela prouve la parité du cardinal de E).

Puisque $F = G \setminus E$ a $2n - \mathrm{Card}(E)$ éléments, son cardinal est également pair. Par ailleurs, F contient exactement 1 et tous les éléments d'ordre 2 de G ; par conséquent, puisque son cardinal est pair, F contient un élément différent de 1, c'est-à-dire un élément d'ordre 2 de G.
2- σ est une bijection de G sur G dont la réciproque est $x \mapsto z^{-1}x$ (vérification immédiate) : c'est bien une permutation de G.
Un pont fixe de σ est un élément de x de G tel que $zx = x$. En multipliant cette égalité par x^{-1} à droite, cela implique que $z = 1$ ce qui n'est pas. Ainsi, σ n'a pas de point fixe.
Enfin, $\sigma^2 = \mathrm{id}_G$. Ainsi, σ est une permutation d'ordre 2 (une involution) qui n'a pas de point fixe : sa décomposition en produit de cycles à supports disjoints est un produit de $|G|/2 = n$ transpositions. En particulier, sa signature est $(-1)^n = -1$ puisque n est impair.
3- Par définition de σ et de Φ, il vient immédiatement que $\Phi(z) = \sigma$.
4- Comme composé de deux homomorphismes de groupes, f est lui-même un homomorphisme de groupes. Puisque la signature de σ est -1, $f(z) = -1$. Ainsi, -1 est dans l'image de f ce qui suffit à prouver que f est surjectif. Alors, le noyau de f est un sous-groupe distingué de G dont l'ordre est $|G|/2 = n$.

UVSQ 2011/2012
Licence de sciences et technologie, santé
LSMA610 (algèbre et géométries), L3 mathématiques
Jeudi 24 mai 2012

Examen (deux heures)

1 Question de cours (4 points)

1- Soit G un groupe agissant sur un ensemble X. Démontrer que pour tout $x \in X$ et pour tout $g \in G$, les sous-groupes d'isotropie de x et de $g.x$ sont conjugués.

2- Donner un exemple d'action transitive d'un groupe sur un ensemble infini.

2 Problème 1 (6 points)

On dit qu'un groupe est *à engendrement fini* lorsqu'il admet un système générateur fini. Autrement dit, un groupe Γ est à engendrement fini lorsqu'il existe une partie finie de Γ qui engendre Γ.

L'objet de ce problème est de montrer qu'un sous-groupe d'un groupe à engendrement fini n'est pas nécessairement à engendrement fini.

1- Soit G le sous-ensemble de $\mathrm{GL}(2, \mathbb{R})$ défini par

$$G = \left\{ \begin{pmatrix} 2^n & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix},\ (n, p, q) \in \mathbb{Z}^3 \right\}.$$

Montrer que G est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

2- Si m et p sont des entiers relatifs, calculer

$$\begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix}.$$

Montrer soigneusement que le groupe G est engendré par les deux matrices

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

3- On note

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{p}{2^q},\ (p, q) \in \mathbb{Z}^2 \right\}.$$

Montrer que $\mathbb{Z}\left[\frac{1}{2}\right]$ est un sous-groupe additif de $\mathbb{R}$ qui n'est pas à engendrement fini.

4- Soit H le sous-groupe de G défini par

$$H = \left\{ \begin{pmatrix} 1 & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix},\ (p, q) \in \mathbb{Z}^3 \right\}$$

(on ne demande pas de montrer que H est un sous-groupe de G).
Démontrer que H est isomorphe à $\mathbb{Z}\left[\frac{1}{2}\right]$. En déduire que H n'est pas à engendrement fini.

3 Problème 2 (10 points)

Soit $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ le groupe multiplicatif des matrices carrées de dimension deux à coefficients dans $\mathbb{Z}/37\mathbb{Z}$ dont le déterminant vaut 1. On note I_2 l'élément neutre de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$.

1- Justifier rapidement pourquoi l'anneau $\mathbb{Z}/37\mathbb{Z}$ est un corps.

2- Question de cours : montrer que l'ordre de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ égale $36 \times 37 \times 38$.

3- On note

$$D = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix},\ x \in \mathbb{Z}/37\mathbb{Z},\ x \neq 0 \right\}.$$

Montrer que D est un sous-groupe de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ et que l'application

$$x \mapsto \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix}$$

définit un isomorphisme de groupes entre le groupe multiplicatif $\mathbb{Z}/37\mathbb{Z} \setminus \{0\}$ et D.

4- Question de cours : pourquoi le groupe multiplicatif $\mathbb{Z}/37\mathbb{Z} \setminus \{0\}$ est-il cyclique ?

5- Combien le groupe D contient-il de sous-groupes d'ordre 9 ?

6- Quel est l'ordre des 3-Sylow de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$? Montrer que $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ contient un 3-Sylow cyclique. Les 3-Sylow de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ sont-ils tous cycliques ?

7- Montrer que $\{-I_2, I_2\}$ est un sous-groupe distingué de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$. Dans toute la suite, on note G le groupe quotient

$$G = \mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})/\{-I_2, I_2\}.$$

8- Quel est l'ordre de G ? Quel est l'ordre des 3-Sylow de G ?

9- A l'aide de la question **8-**, montrer que les 3-Sylow de G sont cycliques.

[On peut montrer, plus généralement, que si p est un nombre premier supérieur ou égal à 5, les 3-Sylow de $\mathrm{PSL}(2, \mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})/\{-I_2, I_2\}$ sont toujours cycliques.]

UVSQ 2011/2012
Licence de sciences et technologie, santé
LSMA610 (algèbre et géométries), L3 mathématiques
Jeudi 24 mai 2012

Corrigé succinct de l'examen

1 Question de cours

2- Par exemple, le groupe $(\mathbb{Z},+)$ agit transitivement sur lui-même par translation (cette action est définie par $n.m = n+m$). Une autre exemple : $\mathrm{GL}(\mathbb{R}^2)$ agit transitivement sur les vecteurs non nuls du plan (pour l'action naturelle).

2 Problème 1

1- D'une part, $\begin{pmatrix} 2^n & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^m & \frac{r}{2^s} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^{n+m} & \frac{r2^{n+q}+p2^s}{2^{s+q}} \\ 0 & 1 \end{pmatrix} \in G$ et d'autre part $\begin{pmatrix} 2^n & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2^{-n} & \frac{-p}{2^{q+n}} \\ 0 & 1 \end{pmatrix} \in G$. Donc G est un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$.

2- $\begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^m & p2^m \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^m & p \\ 0 & 1 \end{pmatrix}$. On note $D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Soit G' le groupe engendré par D et J. Comme D et J sont dans G (facile), $G \supseteq G'$. Par ailleurs, le calcul précédent montre que pour tous $n,p,q \in \mathbb{Z}$,

$$\begin{pmatrix} 2^n & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix} = D^{-q}J^pD^{n+q} \in G'.$$

Cela montre que $G \subseteq G'$.

3- D'une part, $\frac{p}{2^q} + \frac{r}{2^s} = \frac{p2^s+r2^q}{2^{q+s}} \in \mathbb{Z}\left[\frac{1}{2}\right]$; d'autre part, $-\frac{p}{2^q} = \frac{-p}{2^q} \in \mathbb{Z}\left[\frac{1}{2}\right]$. Donc $\mathbb{Z}\left[\frac{1}{2}\right]$ est un sous-groupe de $(\mathbb{R},+)$.
Soit $A = \{\frac{p_1}{2^{q_1}},\dots,\frac{p_N}{2^{q_N}}\}$ une partie finie de $\mathbb{Z}\left[\frac{1}{2}\right]$, où N est un entier naturel non nul. Soit alors $q = \max\{q_1,\dots,q_N\}$. Alors, le nombre rationnel $\frac{1}{2^{q+1}} \in \mathbb{Z}\left[\frac{1}{2}\right]$ mais il n'est pas une combinaison linéaire à coefficents entiers des $\frac{p_k}{2^{q_k}}$ car son numérateur est trop grand : $\frac{1}{2^{q+1}}$ n'est pas dans le sous-groupe engendré par A. Cela montre que $\mathbb{Z}\left[\frac{1}{2}\right]$ n'est pas à engendrement fini.

4- L'application $x \in \mathbb{Z}\left[\frac{1}{2}\right] \longmapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in H$ est un isomorphisme de $\mathbb{Z}\left[\frac{1}{2}\right]$ sur H (vérification immédiate). Comme $\mathbb{Z}\left[\frac{1}{2}\right]$ n'est pas à engendrement fini, H non plus.

3 Problème 2

1- $\mathbb{Z}/37\mathbb{Z}$ est un corps car 37 est un nombre premier.

2- Question de cours. L'ordre de $\mathrm{GL}(2,\mathbb{Z}/37\mathbb{Z})$ est $(37^2-1)(37^2-37)$ et puisque $\mathrm{SL}(2,\mathbb{Z}/37\mathbb{Z})$ est le noyau du déterminant, $|\mathrm{SL}(2,\mathbb{Z}/37\mathbb{Z})| = (37^2-1)(37^2-37)/(37-1) = 36\times 37\times 38$.

3- Pour tout $x \in \mathbb{Z}/37\mathbb{Z} \setminus \{0\}$, soit $d(x) = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix}$. Puisque $\det d(x) = 1$, D est une partie non vide de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$. En outre, si x et y sont dans $\mathbb{Z}/37\mathbb{Z} \setminus \{0\}$, un calcul immédiat montre que $d(x)d(y) = d(xy)$ et que $d(x)^{-1} = d(1/x)$. Cela montre à la fois que D est un sous-groupe de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ et que $d : \mathbb{Z}/37\mathbb{Z} \setminus \{0\} \to \mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ est un homomorphisme de groupes. En outre, $\mathrm{im}(d) = D$ par définition de D. Enfin, le noyau de d est évidemment trivial, ce qui achève de démontrer que d est un isomorphisme de groupes entre $\mathbb{Z}/37\mathbb{Z} \setminus \{0\}$ et D.

4- Question de cours. Puisque $\mathbb{Z}/37\mathbb{Z}$ est un corps fini, son groupe multiplicatif est cyclique, d'ordre 36.

5- Puisque D est isomorphe à $\mathbb{Z}/37\mathbb{Z} \setminus \{0\}$, il est également cyclique d'ordre 36. Comme 9 divise 36, on en déduit que D contient un unique sous-groupe d'ordre 9 (qui est son unique 3-Sylow, par ailleurs).

6- Puisque $36 \times 37 \times 38 = 3^2 \times q$ où q est un entier qui n'est pas multiple de 3, les 3-Sylow de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$ sont d'ordre 9. Ainsi, le sous-groupe d'ordre 9 de D est un 3-Sylow de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$. Comme tout sous-groupe d'un groupe cyclique est cyclique, ce 3-Sylow est également cyclique. Enfin, puisque les 3-Sylow sont tous conjugués, ils sont isomorphes et donc également cycliques.

7- $\{-I_2, I_2\}$ est un sous-groupe central et donc distingué de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$.

8- $|G| = \frac{1}{2}|\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})| = 18 \times 37 \times 38$ et, là encore, les 3-Sylow de G sont d'ordre 9.

9- Soient $p : \mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z}) \to G$ la projection canonique et S un 3-Sylow de $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$. Comme $-I_2$ est d'ordre 2, il n'est pas dans S. Ainsi, la restriction de p à S est-elle injective, ce qui montre que $p(S)$ est un sous-groupe d'ordre 9 de G isomorphe à S, autrement dit un 3-Sylow cyclique de G. Les 3-Sylow de G sont donc également cycliques.

UVSQ 2011/2012
Licence de sciences et technologie, santé
LSMA610 (algèbre et géométries), L3 mathématiques
Mardi 26 juin 2012

Examen (deux heures)

1 Question de cours (4 points)

1- Enoncer la propriété universelle du quotient pour les groupes.

2- Donner la définition d'une action *transitive* d'un groupe sur un ensemble ainsi qu'un exemple argumenté d'action transitive d'un groupe sur l'ensemble $\mathbb{C}$ des nombres complexes.

2 Problème 1 (6 points)

Si $F(X_1, X_2, X_3, X_4)$ est une fraction rationnelle à coefficients rationnels à quatre indéterminées X_1, X_2, X_3 et X_4 et si $\sigma \in \mathfrak{S}_4$, on note

$$\sigma.F\left(X_1, X_2, X_3, X_4\right) = F\left(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)}, X_{\sigma(4)}\right).$$

Cela définit une action à gauche du groupe $\mathfrak{S}_4$ sur le corps des fractions rationnelles (on ne demande pas de démontrer cela).

On note B la fraction rationnelle *birapport*, définie par

$$B\left(X_1, X_2, X_3, X_4\right) = \frac{X_3 - X_1}{X_3 - X_2} \times \frac{X_4 - X_2}{X_4 - X_1} = \frac{\dfrac{X_3 - X_1}{X_3 - X_2}}{\dfrac{X_4 - X_1}{X_4 - X_2}}.$$

1- Question de cours
Donner la définition du sous-groupe de Klein de $\mathfrak{S}_4$. On le notera $\mathcal{K}$.

2- Montrer que $\mathcal{K}$ est un sous-groupe du groupe d'isotropie de $B\left(X_1, X_2, X_3, X_4\right)$ pour l'action de $\mathfrak{S}_4$ définie ci-dessus.

3- En considérant l'action des transpositions (12), (13) et (14) ainsi que celle des 3-cycles (124) et (142), montrer que l'orbite de $B = B\left(X_1, X_2, X_3, X_4\right)$ sous l'action de $\mathfrak{S}_4$ contient les cinq autres fractions distinctes

$$\frac{1}{B}\ ,\ \frac{B}{B-1}\ ,\ 1-B\ ,\ \frac{1}{1-B}\ ,\ 1-\frac{1}{B}.$$

4- En justifiant soigneusement, calculer le groupe d'isotropie et l'orbite de $B\left(X_1, X_2, X_3, X_4\right)$ sous l'action de $\mathfrak{S}_4$.

3 Problème 2 (10 points)

On note $\mathrm{SL}(2,\mathbb{Z})$ le groupe multiplicatif des matrices carrées de dimension 2 à coefficients entiers relatifs et de déterminant 1. On note S et J les deux éléments suivants de $\mathrm{SL}(2,\mathbb{Z})$:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

1- Calculer S^n et J^n pour tout $n \in \mathbb{Z}$.

2- Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, tel que $b \neq 0$.

Montrer qu'il existe $q \in \mathbb{Z}$ tel que $J^q A$ soit de la forme $\begin{pmatrix} a' & c' \\ b & d' \end{pmatrix}$ où a', c' et d' sont des entiers tels que $0 \leq a' \leq |b| - 1$.

3- Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, tel que $b \neq 0$ et $|a| \leq |b| - 1$. Existe-t-il $q \in \mathbb{Z}$ tel que $S^q A$ soit de la forme $\begin{pmatrix} b & c' \\ -a & d' \end{pmatrix}$ où c' et d' sont des entiers ?

4- Montrer que pour tout $A \in \mathrm{SL}(2,\mathbb{Z})$, il existe P dans le sous-groupe engendré par S et J tel que PA soit une puissance de J.
[On pourra remarquer en le justifiant que si $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$*, alors a et b sont premiers entre eux.]*

5- Déduire des questions précédentes que S et J engendrent le groupe $\mathrm{SL}(2,\mathbb{Z})$.

6- Soit N un nombre entier naturel. On note $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ le groupe multiplicatif des matrices carrées de dimension 2 à coefficients dans $\mathbb{Z}/N\mathbb{Z}$ et de déterminant 1. Montrer avec soin que si $\overline{x}$ désigne la classe modulo N de l'entier x, l'application

$$\begin{array}{rccc} R & : & \mathrm{SL}(2,\mathbb{Z}) & \longrightarrow & \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z}) \\ & & \begin{pmatrix} a & c \\ b & d \end{pmatrix} & \longmapsto & \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} \end{array}$$

est un homomorphisme de groupes.

7- En utilisant et en adaptant la question **5-**, montrer que R est surjectif (on pourra montrer que $R(S)$ et $R(J)$ engendrent $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$).

8- On note

$$\Gamma(N) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),\ a \equiv d \equiv 1\ [N] \text{ et } b \equiv c \equiv 0\ [N] \right\}.$$

Montrer que $\Gamma(N)$ est un sous-groupe distingué de $\mathrm{SL}(2,\mathbb{Z})$ et que le quotient $\mathrm{SL}(2,\mathbb{Z})/\Gamma(N)$ est un groupe fini.

9- Si p est un nombre premier, calculer l'ordre du groupe quotient $\mathrm{SL}(2,\mathbb{Z})/\Gamma(p)$.