Examen du cours d'Algèbre 1, ENS Ulm, 18 Janvier 2022

Aucun document n'est autorisé. Temps de composition : 3h. On soignera la rédaction.

Problème 1. *On veut montrer que* $\mathrm{PGL}_2(\mathbb{Z}/11\mathbb{Z})$ *possède un sous-groupe isomorphe à* A_5 (Galois).

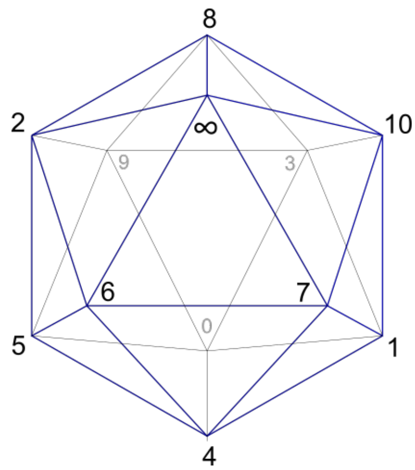
(i) Soit G un groupe simple possédant un sous-groupe H d'indice n avec $n \geq 2$. En considérant l'action par translations de G sur G/H, montrer que $|G|$ divise $n!$.

(ii) En déduire que si $g, h \in \mathrm{A}_5$ sont d'ordres respectifs 3 et 5, alors g et h engendrent A_5.

On pose $X := \mathbb{Z}/11\mathbb{Z} \coprod \{\infty\}$ et on rappelle que $\mathrm{PGL}_2(\mathbb{Z}/11\mathbb{Z})$ s'identifie naturellement au sous-groupe de S_X constitué des homographies de X.

(iii) Donner la décomposition en cycles de l'homographie $x \mapsto \frac{7x+1}{x+5}$ vue comme bijection de X. On donne les congruences $2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 10^2 \equiv 1 \bmod 11$.

(iv) Conclure en contemplant l'icosaèdre suivant.



Problème 2. *Soit G un groupe possédant un sous-groupe distingué Z vérifiant $Z \simeq \mathbb{Z}/2\mathbb{Z}$ et $G/Z \simeq \mathrm{A}_5$. On se propose de montrer que l'on a soit $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$, soit*[1] $G \simeq \widetilde{\mathrm{A}_5}$ (Schur).

(i) Montrer que Z est inclus dans le centre de G.

(ii) On suppose que G possède un sous-groupe distingué N distinct de $\{1\}$, Z et G. Montrer que N est un complément de Z dans G. On pourra considérer la projection canonique $\pi : G \to G/Z$.

(iii) (suite) En déduire $N \simeq \mathrm{A}_5$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{A}_5$.

1. On rappelle que $\widetilde{\mathrm{A}_5}$ est un sous-groupe de $\mathrm{Sp}(1)$ contenant $\{\pm 1\}$ et dont l'image dans le groupe quotient $\mathrm{Sp}(1)/\{\pm 1\} \simeq \mathrm{SO}(3)$ est isomorphe à A_5. Dans ce problème, le groupe $\widetilde{\mathrm{A}_5}$ n'interviendra qu'à la question *(xi)*.

On suppose désormais que les seuls sous-groupes distingués de G sont $\{1\}$, Z et G. On note z l'unique élément non trivial de Z et on fixe $r : G \to \mathrm{GL}_n(\mathbb{C})$ une représentation de G.

(iv) *Montrer* $\mathrm{D}(G) = G$.

(v) *Montrer* $r(G) \subset \mathrm{SL}_n(\mathbb{C})$.

(vi) *On suppose r irréductible. Montrer que l'on a* $r(z) = 1_n$ *ou* $r(z) = -1_n$.

(vii) *On suppose* $r(z) = -1_n$. *Montrer* $n \equiv 0 \bmod 2$ *et que r est injective.*

On choisit un ensemble de représentants $\{U_i\}_{i\in I}$ des classes d'isomorphisme de $\mathbb{C}[G]$-modules irréductibles dans lesquels z n'agit pas par l'identité.

(viii) *Montrer* $\sum_{i\in I} (\dim U_i)^2 = |G| - |G/Z| = 60$.

(ix) *En déduire qu'il existe $i \in I$ avec* $\dim U_i = 2$.

(x) *Montrer que G est isomorphe à un sous-groupe fini de* $\mathrm{SL}_2(\mathbb{C})$.

(xi) *En déduire $G \simeq \widetilde{\mathrm{A}_5}$. On utilisera sans démonstration le fait que tout sous-groupe fini de $\mathrm{SL}_2(\mathbb{C})$ est conjugué à un sous-groupe de* $\mathrm{Sp}(1)$.

(xii) *(Application) Montrer* $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \widetilde{\mathrm{A}_5}$.

Problème 3. *Dans tout ce problème, p désigne un nombre premier. Soient G un sous-groupe de S_p avec $p \mid |G|$, et $0 \le r < p$ l'unique entier tel que $\frac{|G|}{p} \equiv r \bmod p$. On se propose de montrer que si r est premier, et si on a $|G| \neq pr$, alors le groupe G est simple* (« *critère de simplicité de Chapman* ») .

Partie 1 : applications

Dans cette partie, on admet le critère de simplicité de Chapman et on en donne trois applications.

(i) *Retrouver que le groupe* A_5 *est simple.*

(ii) *Retrouver que le groupe $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ est simple en le faisant agir sur* $(\mathbb{Z}/2\mathbb{Z})^3 \smallsetminus \{0\}$.

(iii) *Le groupe M_{11} est un sous-groupe de S_{11} construit par E. Mathieu en 1861. On admet que son action naturelle sur $\{1, \ldots, 11\}$ est 4-transitive, et que le seul élément de M_{11} fixant 4 points dans $\{1, \ldots, 11\}$ est l'identité. Déterminer $|\mathrm{M}_{11}|$ et montrer que M_{11} est simple.*[2]

Partie 2 : préliminaires sur S_p

On pose $X = \mathbb{Z}/p\mathbb{Z}$ et on note Aff_X le sous-ensemble de S_X constitué des bijections de la forme $x \mapsto ax+b$ avec $a, b \in \mathbb{Z}/p\mathbb{Z}$. On note enfin $c \in \mathrm{Aff}_X$ la bijection $x \mapsto x + 1$.

(i) *Vérifier que Aff_X est un sous-groupe de S_X et donner son ordre.*

(ii) *Montrer que le normalisateur de $\langle c\rangle$ dans S_X est* Aff_X.

2. Le groupe M_{11} est le plus petit des groupes simples dits *sporadiques*.

Partie 3 : l'invariant r d'un sous-groupe transitif de S_p

Soit G un sous-groupe de S_p.

(i) Montrer les équivalences entre :

(a) p divise $|G|$,

(b) G contient un p-cycle,

(c) G agit transitivement sur $\{1, \ldots, p\}$.

On suppose désormais ces propriétés satisfaites. On note r_G l'unique élément $0 \leq r < p$ tel que $\frac{|G|}{p} \equiv r \bmod p$. On fixe P un p-Sylow de G, $\mathrm{N}_G(P)$ le normalisateur de P dans G, et on note n_G le nombre des p-Sylow de G.

(ii) Rappeler pourquoi on a $|P| = p$ et $|G| = |\mathrm{N}_G(P)|\, \mathrm{n}_G$.

(iii) Montrer $|\mathrm{N}_G(P)| = p\, \mathrm{r}_G$ et que r_G divise $p-1$.

(iv) On suppose $\mathrm{r}_G = 1$. Montrer que G possède exactement n_G éléments qui ne sont pas d'ordre p.

(v) (suite) En considérant les stabilisateurs dans G des éléments de $\{1, \ldots, p\}$, montrer $\mathrm{n}_G = 1$.

Partie 4 : démonstration du théorème

Soient G un sous-groupe de S_p avec r_G premier et $\mathrm{n}_G > 1$, et N un sous-groupe distingué non trivial de G.

(i) Montrer que les orbites de $\{1, \ldots, p\}$ sous l'action de N ont toutes même cardinal.

(ii) En déduire que p divise $|N|$.

(iii) Montrer $\mathrm{n}_N = \mathrm{n}_G$.

(iv) Montrer que r_N divise r_G.

(v) Conclure.

Problème 4. *Soit M un $\mathbb{Z}[i]$-module dont le groupe abélien sous-jacent est libre de rang fini r. On se propose d'abord de montrer que r est pair et que le $\mathbb{Z}[i]$-module M est libre de rang $r/2$.*

(i) Montrer que M est de type fini.

(ii) Soient $m \in M$ et $a \in \mathbb{Z}[i] \smallsetminus \{0\}$ avec $a\, m = 0$. Montrer $m = 0$.

(iii) Conclure.

(Application) *On se place dans un plan euclidien P, de produit scalaire $(x, y) \mapsto x.y$, et on se donne L un réseau de P, c'est-à-dire un sous-groupe additif engendré par une $\mathbb{R}$-base de P.*

(iv) On suppose que L est stable par la rotation d'angle $\pi/2$. Montrer qu'il existe $u, v \in P$ avec

$$u.u = v.v, \;\; u.v = 0 \;\text{ et }\; L = \mathbb{Z}u + \mathbb{Z}v.$$