École Normale Supérieure, Année 2021-2022

1e année, Algèbre 1

TD n° 8 : Notes et corrections

Exercice 1. Révisions

1. Montrer qu'on a une suite exacte

$$1 \to \mathrm{PSL}_n(K) \to \mathrm{PGL}_n(K) \xrightarrow{\overline{\det}} K^\times/K^{\times n} \to 1.$$

2. Rappeler brièvement comment obtenir les isomorphismes

$$\mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z}) \cong \mathrm{S}_3 \text{ et } \mathrm{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \cong \mathrm{S}_4.$$

3. Soit $\mathbb{F}_4$ le corps à 4 éléments[1]. Par la même méthode, montrer

$$\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathrm{A}_5.$$

4. Soit $n \geqslant 2$ un entier, pour tout sous-groupe $H \subset \mathrm{S}_n$ d'indice n montrer $H \cong \mathrm{S}_{n-1}$. En déduire un isomorphisme exceptionnel qui décrit une action transitive de H sur $\{1, \dots, n\}$.

Correction exercice 1

1. On sait que $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^\times \cdot \mathrm{Id}_n$ le quotient de $\mathrm{GL}_n(K)$ par son centre. La restriction du déterminant au centre est donné pour $\lambda \in K^\times$ par $\det(\lambda \cdot \mathrm{Id}_n) = \lambda^n \in K^{\times,n}$. Ainsi la composé du déterminant avec la réduction $K^\times \to K^\times/K^{\times,n}$ est nulle sur le centre, donc définit par passage au quotient, un morphisme de groupe $\overline{\det}\colon \mathrm{PGL}_n(K) \to K^\times/K^{\times,n}$ qui est surjectif. On obtient le diagramme suivant, où on vient de justifier les lignes en pointillés.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mu_n(K)\cdot \mathrm{Id}_n & \longrightarrow & K^\times \cdot \mathrm{Id}_n & \xrightarrow{\lambda \longmapsto \lambda^n} & K^{\times,n}\cdot \mathrm{Id}_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{SL}_n(K) & \longrightarrow & \mathrm{GL}_n(K) & \xrightarrow{\det} & K^\times & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{PSL}_n(K) & \longrightarrow & \mathrm{PGL}_n(K) & \overset{\overline{\det}}{\dashrightarrow} & K^\times/K^{\times,n} & \dashrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

C'est un diagramme commutatif dont les lignes et les colonnes sont exactes. C'est une *suite exacte de suites exactes* au sens où la première ligne est le noyau de la "flèche de flèches" verticale de la deuxième à la troisième ligne.

- Les quatres petits carrés sont bien commutatifs par construction.
- Les colonnes sont exactes par définition. On rappelle qu'un élément du centre de $\mathrm{SL}_n(K)$ est une homothétie de déterminant 1 et donc son rapport $\lambda \in K^\times$ vérifie $\lambda^n = 1$, i.e. $\lambda \in \mu_n(K)$.
- les deux premières lignes sont exactes par définition.
- Il reste à justifier que $\mathrm{Ker}\left(\overline{\det}\right) = \mathrm{PSL}_n(K)$. Comme le diagramme commute et que la deuxième ligne se surjecte sur la troisième, $\mathrm{Ker}(\det) = \mathrm{SL}_n(K)$ suffit.

[1] Le corps à 4 éléments est décrit par $\mathbb{F}_4 \coloneqq \{0, 1, \alpha, 1+\alpha\}$ où $1 + \alpha + \alpha^2 = 0$.

2. Ces isomorphismes exceptionnels sont dans le cours. Rappellons le principe de la recette. Le groupe $\mathrm{PGL}_{n+1}(K)$ agit simplement transitivement sur $\mathbb{P}^n(K)$, l'espace projectif. Or, notons $\mathbb{F}_q$ le corps fini à q éléments, on obtient un morphisme injectif $\rho_n\colon \mathrm{PGL}_{n+1}(K) \hookrightarrow \mathrm{S}_N$ où $N = |\mathbb{P}^n(\mathbb{F}_q)|! = (q^n + \cdots + q + 1)!$. Rappelons que

$$|\mathrm{PGL}_{n+1}(\mathbb{F}_q)| = q^{\frac{n(n+1)}{2}} \prod_{k=2}^{n+1} (q^k - 1),$$

Comme ρ_n est un morphisme injectif entre ensemble fini il suffit de montrer qu'ils ont même cardinal pour obtenir un isomorphisme, ce qui est une vérification numérique.

En spécialisant en $n = 1$ on a $|\mathrm{PGL}_2(\mathbb{F}_q)| = q(q^2 - 1)$. Pour $q = 2$, $2 \cdot 3 = 6 = (2 + 1)!$ donc on a bien $\mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z}) \cong \mathrm{S}_3$ et de même pour pour $q = 3$, $3 \cdot 8 = 24 = (3 + 1)!$, ce qui donne $\mathrm{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \cong \mathrm{S}_4$

- Rappelons que A_N est l'unique sous-groupe d'indice 2 dans S_N. On répète la recette précédente $4 \cdot 15 = 60 = \frac{5!}{2}$ et donc $\mathrm{PGL}_2(\mathbb{F}_4) \subset \mathrm{S}_5$ est d'indice 2 ce qui conclut $\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathrm{A}_5$.

3. Soit $H \subset \mathrm{S}_n$ un sous-groupe d'indice n d'indice n. Posons $X = \mathrm{S}_n/H$, l'ensemble de cardinal n des classes à droites et $g_1, g_2, \ldots g_n \in \mathrm{S}_n$ des représentants de ses classes où on impose $g_1 = \mathrm{id}_n$. Le groupe S_n opère à gauche sur X par translation ce qui définit un morphisme $\mathrm{S}_n \to \mathrm{S}_X$, soit un endomorphisme $\varphi\colon \mathrm{S}_n \to \mathrm{S}_n$ tel que

$$\sigma \in \mathrm{S}_n \longmapsto \varphi_\sigma, \quad \text{déterminé par } \sigma g_i H = g_{\varphi_\sigma(i)} H.$$

Or on obtient $H = \mathrm{Stab}_{\mathrm{S}_N}(g_0 H)$ mais alors $\operatorname{Ker}\varphi \subset H$ et donc $\operatorname{Ker}\varphi$ est un sous-groupe distingué de S_n d'indice au moins n. Ainsi, φ est injectif et donc $\varphi \in \mathrm{Aut}(\mathrm{S}_n)$ est un automorphisme tel que $\varphi\colon H \xrightarrow{\sim} \mathrm{S}_n(1) \coloneqq \{\sigma \in \mathrm{S}_n \mid \sigma(1) = 1\}$. Comme $\mathrm{S}_n(1) \cong \mathrm{S}_{n-1}$ on a bien obtenu $H \cong \mathrm{S}_{n-1}$. On a même montré qu'il existait un automorphisme de S_n qui réalise cette isomorphisme, en particulier, si cette automorphisme est intérieur, H est le stabilisateur d'un point de $\{1, \ldots, n\}$ et n'agit donc pas transitivement.

Appliquons la recette projective à $n = 1$ et $q = 5$. On obtient $|\mathrm{PGL}_2(\mathbb{F}_5)| = 5 \cdot 24 = 120 = \frac{6!}{6} = \frac{|\mathbb{P}^1(\mathbb{F}_5)|}{6}$ et donc on obtient $\mathrm{PGL}_2(\mathbb{F}_5)$ comme sous-groupe d'indice 6 dans S_6. Par ce qui précède, on a

$$\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathrm{S}_5.$$

Or, $\mathrm{PGL}_2(\mathbb{F}_5)$ agit transitivement sur $\mathbb{P}^1(\mathbb{F}_5)$ qui est un ensemble à 6 éléments. Ainsi on a un sous-groupe de S_6 d'indice 6 mais qui agit transitivement sur $\{1, \ldots, 6\}$. En particulier, tout automorphisme de S_6 n'est pas intérieur ! C'est le seul groupe symétrique qui à un automorphisme extérieur.

Exercice 2. [Blocs d'une action]

Soit G un groupe agissant transitivement sur X. On dit qu'une partie non vide $B \subset X$ est un *bloc* (de cette action) si pour tout $g \in G$ on a soit $g(B) = B$, soit $g(B) \cap B = \emptyset$. La partie X, et les singletons de X, sont des blocs, dits *triviaux*.

1. Déterminer les blocs des actions transitives usuelles suivantes : de S_n sur $\{1, \ldots, n\}$, de K_4 sur $\{1, 2, 3, 4\}$, de $\mathrm{GL}(E)$ sur $E \backslash \{0\}$.

2. Montrer que $B \subset X$ est un bloc si, et seulement si, les parties de la forme $g(B)$ avec $g \in G$ forment une partition de X.

Si B est un bloc, son stabilisateur est le sous-groupe $G_B = \{g \in G; g(B) = B\}$ de G.

3. Soient $B \subset C$ deux blocs. Montrer $G_B \subset G_C$, et $G_B = G_C \iff B = C$.

4. Soit $x \in X$ et H un sous-groupe de G contenant G_x. Montrer que $B \coloneqq Hx$ est l'unique bloc de G contenant x et vérifiant $G_B = H$.

5. En déduire que $B \mapsto G_B$ est une bijection croissante entre l'ensemble des blocs contenant x et celui des sous-groupes de G contenant G_x.

Correction exercice 2

1. Montrons que les blocs pour l'action de S_n sur $\Delta_n = \{1, \ldots, n\}$ sont triviaux. Pour S_3 c'est clair donc supposons $n \geqslant 4$. Soit $B \subsetneq \Delta_n$ un bloc strict et soit $i, j \in B$ deux éléments distincts $i \neq j$. Alors, il existe $\sigma \in \mathrm{S}_n$ tel que $\sigma(i) \neq B$ et $\sigma(j) \in B$. Ainsi B ne peut contenir plus d'un élément.

2. C'est la définition. Soit $B \subset X$ une partie, la famille $\{gB\}_{g\in G}$ est une famille couvrante et $gB \cap B \neq \iff gB = B$ est la condition pour que cette famile définisse une patition mais aussi la condition que B soit un bloc.

3. Soit $g \in G$ alors
$$gB = B \implies gC \cap C \neq \iff gC = C$$
donc $g \in G_B \implies g \in G_C$ i.e. $B \subset C \implies G_B \subset G_C$ et si on a la réciproque à la première implication alors on a $G_C \subset G_B$ donc $G_C = G_B$ et comme c'est une succession d'équivalences on a $C = B$.

4. Montrons que $B = H \cdot x$ est un bloc. En effet, on a la partition en classes $G = \sqcup_{Hg\in H\backslash G} gH$ qui nous donne que $Hg \cdot x \cap H \cdot x \neq \emptyset \implies g \cdot x \in H \implies Hg = H$. On voit au passage que $G_B = H$ et par la question précédente que H est l'unique sous-groupe content G_x tel que $G_B = H$.

5. On a montrer qu'elle était strictement croissante en 3 et on a construit un inverse en 4.

Exercice 3. Actions primitives

Une action transitive d'un groupe G sur un ensemble X est dite *primitive* si on a $|X| \geq 2$ et si ses seuls blocs sont les blocs triviaux.

1. Montrer qu'une action 2-transitive est primitive.

2. On suppose que G agit primitivement sur X, et on se donne N un sous-groupe distingué de G. Montrer que les N-orbites dans X sont des blocs.

3. En déduire que le critère d'Iwasawa vaut encore en remplaçant dans son énoncé l'hypothèse "2-transitivement" par "primitivement".

4. En utilisant l'exercice précédent, montrer qu'une action transitive de G sur X est primitive si, et seulement si, ses stabilisateurs sont des sous-groupes maximaux de G.

5. Montrer qu'une action de G sur X est 2-transitive si, et seulement si, elle est transitive et pour un $x \in X$ (ou tous) et $g \in G \smallsetminus G_x$, on a $G = G_x \cup G_x g G_x$.

Correction exercice 3

1. Soit G un groupe et X un G-ensemble, supposons que G opère 2-transitivement sur X. Soit $x \in X$, on sait que G_x opère transitivement sur $X \setminus \{x\}$. Ainsi, le singleton $\{x\}$ est l'unique partie stricte de X contenant x, on conclut que les blocs sont tous triviaux et donc que l'action est primitive.

2. On sait qu'on a la partition $X = \bigsqcup_{[x]\in X/N} \mathrm{O}$ où $[x] \coloneqq N \cdot x$ est la N-orbite associée à $x \in X$. De plus, comme N est distingué dans G, pour tout $g \in G$ on a $g \cdot [x] = [g \cdot x]$ et en particulier, N opère trivialement sur les orbites. On en déduit que l'action de G sur X/N se factorise par G/N et on obtient une partition pour $x_0 \in X$,
$$X = \bigsqcup_{g\in G/N} gN \cdot x_0.$$
Ainsi, pour deux parties de la forme $gN \cdot x_0$ elles sont soit disjointe soit égales i.e pour $\mathrm{O} = N \cdot x_0$ on a $\forall g \in G, \mathrm{O} \cap g\mathrm{O} \neq \emptyset \implies \mathrm{O} = g\mathrm{O}$ qui est bien la condition pour que l'orbite $N \cdot x_0$ soit un bloc.

3. Avec les notations de la question précédente, si l'action de G est primitive, alors les blocs des N-orbites sont triviales i.e.
$$N \cdot x_0 = \begin{cases} X & \text{l'action de } N \text{ est transitive} \\ x_0 & \text{l'action de } N \text{ est triviale} \end{cases}.$$
Donc un sous-groupe distingué de G agit soit trivialement, soit transitivement. Pour le critère d'Iwasawa, on suppose que N n'agit pas trivialement et on utilise la 2-transitivité pour montrer que N agit transitivement, ce qu'on vient de déduire de la primitivité de l'action. Le reste de la preuve ne change pas, (cf. cours 15, proposition 3.11).

4. C'est une application directe de la bijection croissante du 5. de l'exercice précédent : on est dans le cas où pour tout $x \in X$, $\{x\}$ et X sont les seuls blocs contenant x et donc G et G_x sont les seuls sous-groupes contenant G_x i.e. les stabilisateurs sont des sous-groupes maximaux si et seulement si les blocs de l'action sont triviaux.

5. Supposons qie G opère 2-transitivement sur X. Alors pour $h, g \in G$ tel que $h \cdot x \neq x, g \cdot x \neq x$, i.e. $h, g \notin G_x$, alors par la 2-transitivité il existe $s \in G_x$ tel que $h \cdot x = sg \cdot x = sgs^{-1} \cdot x$ et donc $h \in sgs^{-1}G_x$, ainsi on a montré que $h \notin G_x \implies h \in G_x g G_x$ et donc $G = G_x \cup G_x g G_x$. La réciproque devrait s'obtenir en remontant l'argument.

Exercice 4.

On se propose de détermine les groupes finis G tels que $\mathrm{Aut}(G)$ opère transitivement sur $G \setminus \{e\}$.

1. Montrer que pour tout $n \geqslant 1$, $(\mathbb{Z}/p\mathbb{Z})^n$ vérifie cette propriété. On va montrer que se sont les seuls.
2. Montrer que G est abélien. On pourra considérer l'action de $\mathrm{Int}(G)$ sur G pour montrer que tout les automorphismes sont extérieurs.
3. Montrer que si $G[p] \neq 0$, pour p un entier premier, alors $G[p^k] = G[p]$ et finalement $G[\ell] = 0$, pour tout entier ℓ premier à p.
4. Conclure.

Correction exercice 4

1. Le groupe $(\mathbb{Z}/p\mathbb{Z})^n$ est canoniquement un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel et donc $\mathrm{Aut}\left[(\mathbb{Z}/p\mathbb{Z})^n\right] \cong \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ qui agit transitivement sur $(\mathbb{Z}/p\mathbb{Z})^n \setminus \{0\}$.
2. Il est plus naturel pour cet exercice de tout de suite remarqué que tout élément différent du neutre dans G est du même ordre, donc que G est un p-groupe pour p premier : on a alors que le centre de G n'est pas trivial et la transitivité permet de conclure que G est abélien et comme pour p un diviseur premier de $|G|$ il existe un élément d'ordre p on conclut que tout élément est d'ordre p donc que $G \cong (\mathbb{Z}/p\mathbb{Z})$.

   Montrons que tout automorphisme de G est extérieur. Rappellons qu'on a un morphisme surjectif $\mathrm{int}_\bullet \colon G \to \mathrm{Int}(G)$ de noyau le centre $Z(G)$. Considérons l'action de $\mathrm{Int}(G)$ sur $G \setminus \{e\}$. Alors, tout élément $\mathrm{int}_g \in \mathrm{Int}(G)$ fixe la partie $\langle g \rangle \setminus \{e\}$ qui est de cardinal au moins 1. Si cette partie contient uniquement g alors $g^2 = e$ et G est d'exposant 2, auquel cas il est abélien. On trouve alors $|G| > |\mathrm{Int}(G)|$ et $Z(G) \neq e$ mais comme $\mathrm{Aut}(G)$ agit transitivement, tout élément est dans le centre. Ainsi $G = Z(G)$, c'est-à-dire G est abélien.
3. Tous les éléments différent du neutre ont même ordre par la transitivité. En particulier, s'il existe un élément d'ordre p^n, sa puissance p^{n-1} sera d'ordre p mais alors, tout élément est d'ordre p. On en déduit que $G = G[p]$, ce qui signifie que G est un p-groupe abélien élémentaire.
4. On a montré que G était un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel et comme il est fini, il est de dimension fini c'est à dire $G = (\mathbb{Z}/p\mathbb{Z})^n$ pour $n = \log_p(|G|)$.