1e année, Algèbre 1

TD n° 3 : Notes et corrections

La fin de la feuille comprend : le complément II du cours sur les quaternions d'Hamilton et quelques définitions.

1 Sous-groupes distingués et groupes quotients

Exercice 1.

Soient H un sous-groupe distingué d'indice fini n de G, et $g \in G$. Montrer $g^n \in H$.

Correction exercice 1

Soit $\pi\colon G \to G/H$ le morphisme quotient. Alors G/H est un groupe fini d'ordre n et donc pour tout $x \in G/H, x^n \equiv 0 \mod H$. Ainsi, l'application $G \mapsto G/H$, donnée par $g \mapsto \pi(g)^n = \pi(g^n)$ est nulle. C'est-à-dire que $g^n \in H$

Exercice 2.

1. Soit G un groupe tel que $G/\mathrm{Z}(G)$ est monogène, montrer que G est abélien.
2. Examiner le cas $G = \mathrm{H}_8$.

Correction exercice 2

1. Notons que $\mathrm{Z}(G)$ est bien un sous-groupe distingué de G. Soit $\pi\colon G \to G/\mathrm{Z}(G)$ le morphisme quotient. On se donne $g_0 \in G$ tel que $\pi(g_0)$ est un générateur. Posons l'application $\mathrm{Z}(G) \times \mathbb{Z} \to G$ donnée par $(z, k) \mapsto z g_0^k$. Alors on remarque qu'elle est surjective par la partition en classes et que c'est bien un morphisme pour la structure de groupe produit sur $\mathrm{Z}(G) \times \mathbb{Z}$.
2. Le centre de H_8 ne peux pas contenir I, J et K donc il est contenu dans $\{1, -1\}$. Comme -1 est central on en déduit que $\mathrm{Z}(G) = \{1, -1\}$ et donc le quotient $G/\mathrm{Z}(G)$ est d'ordre 4 donc abélien. S'il était cyclique G serait abélien ce qui n'est pas le cas donc $G/\mathrm{Z}(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$ le groupe de Klein. Ce quotient est engendré par les classe de toute pair d'éléments d'ordre 4 dans G. Remarquez qu'on peut facilement en déduir qu'a isomorphisme près H_8 est l'unique groupe d'ordre 8 contenant un unique élément d'ordre 2.

Exercice 3. Centre et automorphismes intérieurs

Soit G un groupe.

1. Montrer que $\mathrm{int}\colon G \to \mathrm{Aut}(G), g \mapsto \mathrm{int}_g$, est un morphisme de groupes de noyau $\mathrm{Z}(G)$.
2. En déduire que l'image, soit $\mathrm{Int}(G)$, est un sous-groupe de $\mathrm{Aut}(G)$ et que $\mathrm{Z}(G)$ est un sous-groupe distingué de G. Montrer finalement que $G/\mathrm{Z}(G) \cong \mathrm{Int}(G)$.
3. Montrer que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

Correction exercice 3

1. Soit $g, g' \in G$, alors comme $\mathrm{int}_{gg'}\colon x \mapsto gg'x(gg')^{-1} = g(g'xg'^{-1})^{-1}1$ et on a bien $\mathrm{int}_{gg'} = \mathrm{int}_g \circ \mathrm{int}_{g'}$. De plus $\ker(\mathrm{int}) = \{g \in G \mid \mathrm{int}_g = \mathrm{id}_G\} = \{g \in G \mid \forall x \in G, \underbrace{\mathrm{int}_g(x)}_{gxg^{-1}} = x\} = \mathrm{Z}(G)$.
2. L'image d'un groupe par un morphisme est bien un sous-groupe donc $\mathrm{Int}(G) = \mathrm{im}(\int) \subset \mathrm{Aut}(G)$ est un sous-groupe et par la propriété universelle le morphisme surjectif $G \xrightarrow{\mathrm{int}} \mathrm{Int}(G)$ se factorise par un isomorphisme $G/\mathrm{Z}(G) \xrightarrow{\sim} \mathrm{Int}(G)$.

Exercice 4.

Soient G un groupe et H, K deux sous-groupes de G, notons $HK \coloneqq \{hk; h \in H,\ k \in K\}$.

1. Montrer que si K est distingué G, alors HK est un sous-groupe de G.
2. En déduire que si H et K sont distingués dans G alors $H \times K \xrightarrow{\sim} HK \iff H \cap K = \{e_G\}$.
3. Examiner le cas $G = \mathrm{H}_8$.

Correction exercice 4

1. On doit vérifier $HKHK \subset HK$ et $HK = (HK)^{-1}$, donc il suffit de vérifier $KH = HK$. Ainsi, on doit vérifier pour tout $h \in H$ qu'il existe $h' \in H$ tel que $hK = Kh'$ mais comme K est distingué on conclut en posant $h' \coloneqq h$.
2. Posons c: $H \times K \to G$ donnée par $(h, k) \mapsto khk^{-1}h^{-1} = \mathrm{int}_k(h)h^{-1}$. Ainsi, comme H est a fortiori distingué dans $HK \supset K$ et stable par produit, $\mathrm{im(c)} \subset H$; puis de même, $\mathrm{im(c)} \subset K \subset H \cap K$. L'application produit $H \times K \to HK$ est bien surjective et définit un morphisme injectif si, et seulement si, $\mathrm{im}(c) = \{e_G\}$, ce qui traduit l'équivalence.
3. Tout les sous-groupes non-triviaux de H_8 sont abéliens, distingués dans H_8 mais H_8 n'est lui même pas abélien, ce qui conclue. On peut aussi remarquer qu'ils contiennent tous le centre de H_8.

Exercice 9.

Soit p un nombre premier.

1. Montrer qu'il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^2 + y^2 = -1$.

On considère les deux matrices $I, J \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$

$$I \coloneqq \begin{bmatrix} x & y \\ y & -x \end{bmatrix}, \quad J \coloneqq \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

1. Vérifier $I^2 = -1$, $J^2 = -1$ et $IJ = -JI$.
2. On suppose $p > 2$. Montrer que $\{1, I, J, IJ\}$ forment une base du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.
3. En déduire que H_8 est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ pour tout nombre premier $p > 2$.

Correction exercice 9

1. Si $\left(\dfrac{-1}{p}\right) = 1$ alors il suffit de prendre $(x, y) \coloneqq (i, 0)$ où ß $\in \mathbb{Z}/p\mathbb{Z}$ est une racine carré de -1 i.e., $i^2 = -1$. Sinon, on peut faire la substitution $x = \frac{1}{u}$ et $y = \frac{v}{u}$ pour obtenir $\frac{1}{u^2} + \frac{v^2}{u^2} = -1$ ce qui donne $-u^2 = 1 + v^2$. Il y a $\frac{p-1}{2}$-valeurs non-triviales possible pour le membre de gauche. Or, l'idée est de penser aux fonctions trigonométriques : l'application $t \mapsto t^2 + 1$ ne s'annule nulle part sur $\mathbb{Z}/p\mathbb{Z}$, donc on obtient $\frac{p+1}{2}$ valeurs possible pour le membre de droite. Ainsi il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ tel que $-u^2 = 1 + v^2$donc $x^2 + y^2 = -1$
2. Se sont deux matrices de SL_2 de trace nulle, donc leur polynôme caractéristique vaut $X^2 + 1$ ce qui donne $J^2 = I^2 = -\mathrm{id}$. On calcul IJ et JI,

$$IJ = \begin{bmatrix} y & -x \\ -x & -y \end{bmatrix}, \quad JI = \begin{bmatrix} -y & x \\ x & y \end{bmatrix}.$$

3. Il suffit de déterminer que c'est une famille libre puisqu'elle à le bon cardinal. Il est déjà claire que id est indépendante des trois autres matrices et de l'espace qu'ils engendrent. Soit $a, b, c \in \mathbb{Z}/p\mathbb{Z}$, on calcul $(aI + bJ + cIJ)^2 = -(a^2 + b^2 + c^2)\mathrm{id}_2$.

Exercice 10. Quaternions de Hurwitz

On considère l'élément $\omega = \frac{1+I+J+K}{2}$ de $\mathbb{H}$ et on pose $\mathrm{Hur} \coloneqq \mathbb{Z} + \mathbb{Z}\,I + \mathbb{Z}\,J + \mathbb{Z}\,K + \mathbb{Z}\omega$.

1. Montrer que Hur est un sous-anneau de $\mathbb{H}$, et $\chi_q \in \mathbb{Z}[t]$ pour tout $q \in \mathrm{Hur}$.
2. Montrer $\mathrm{Hur}^\times = \{q \in \mathrm{Hur} \mid \mathrm{n}(q) = 1\}$. En déduire $|\mathrm{Hur}^\times| = 24$, puis lister les 24 éléments de Hur, ainsi que leurs polynômes caractéristiques.
3. On suppose p premier impair. En utilisant l'exercice 1 3., exhiber un morphisme d'anneaux surjectif $\varphi : \mathrm{Hur} \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Vérifier que l'on a $\mathrm{tr}(\varphi(q)) = \mathrm{tr}(q) \bmod p$, et donc $\det \varphi(q) = \mathrm{n}(q) \bmod p$, pour tout $q \in \mathrm{Hur}$.
4. En déduire $\mathrm{Hur}^\times \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.
5. Montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ pour tout $p > 2$ premier (un fait assez surprenant!).