TD1 : Outils de la théorie des groupes

Diego Izquierdo

Les exercices de ce TD portent sur certains aspects de la théorie des groupes qui seront utilisés dans le cours d'Algèbre 2. Les deux premiers seront utiles dès la première partie du cours, alors que les exercices 3-9 ne seront utiles que dans la deuxième partie (théorie de Galois). L'exercice 1 est à préparer avant le TD ; l'exercice 8 étant plus difficile que les autres, il est conseillé de l'attaquer uniquement après avoir traité tous les autres exercices. Les notions de suite exacte et de produit semi-direct n'ayant pas été vues en cours d'Algèbre 1, ne traitez (pour l'instant) ni la question 6.(d) de l'exercice 2 ni l'exercice 9.

Exercice 1 (à préparer) : Groupe des unités de $\mathbb{Z}/n\mathbb{Z}$

Dans cet exercice, nous voulons étudier la structure du groupe des unités d'un groupe cyclique. On rappelle que tout sous-groupe fini du groupe des unités d'un corps est cyclique. Cela entraîne en particulier que $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ pour tout nombre premier p.

1. Rappeler quel est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$.

2. Soient p un nombre premier impair et $m > 1$ un entier.
- (a) Montrer que $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \mod p^m$, puis que $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$.
- (b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/p^{m-1}\mathbb{Z}$.
- (c) Montrer qu'il existe $x_0 \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ d'ordre $p-1$.
- (d) Montrer que $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \to (\mathbb{Z}/p^m\mathbb{Z})^\times, (a,b) \mapsto x_0^a(1+p)^b$ est un isomorphisme. En déduire que $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z}$.

3. Soit $m > 2$ un entier.
- (a) Montrer que $5^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m$, puis que 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$.
- (b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/2^m\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2^{m-2}\mathbb{Z}$.
- (c) En s'inspirant de la question 2.(d), montrer que $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

4. Quelle est la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$? Quand ce groupe est-il cyclique ?

5. *Exemples :* Donner un générateur du groupe $(\mathbb{Z}/162\mathbb{Z})^\times$. Donner un élément d'ordre maximal dans $(\mathbb{Z}/2592\mathbb{Z})^\times$.

Exercice 2 : Dual d'un groupe abélien fini

Soit A un groupe abélien fini. On appelle dual de A l'ensemble $\hat{A}$ constitué des caractères de A (c'est-à-dire des morphismes de groupes $A \to \mathbb{C}^\times$). On peut munir $\hat{A}$ d'une loi de groupe abélien définie par $(\chi\chi')(a) = \chi(a)\chi'(a)$.

1. Montrer que le dual de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
2. Soit B un groupe abélien fini. Montrer que $\widehat{A \times B} \cong \hat{A} \times \hat{B}$.
3. Soit $f : A \to B$ un morphisme de groupes abéliens finis. Montrer que $\hat{f} : \hat{B} \to \hat{A}, \chi \mapsto \chi \circ f$ est un morphisme de groupes.
4. Soit $f : A \to B$ un morphisme de groupes.
  (a) Montrer que, si f est surjectif, alors $\hat{f}$ est injectif.
  (b) Supposons f injectif. Soient $b_1, ..., b_r$ des éléments de B tels que, pour chaque $s \in \{1, ..., r\}$, on a $b_s \notin \langle A, b_1, b_2, ..., b_{s-1}\rangle$ et $B = \langle A, b_1, b_2, ..., b_r\rangle$. Montrer que, pour chaque $s \in \{1, ..., r+1\}$, tout caractère de $\langle A, b_1, b_2, ..., b_{s-1}\rangle$ peut s'étendre en un caractère de $\langle A, b_1, b_2, ..., b_s\rangle$. En déduire que $\hat{f}$ est surjectif.
5. Soit e l'exposant du groupe A, c'est-à-dire le plus petit commun multiple des ordres des éléments de A. On rappelle qu'il existe un élément a de A d'ordre e.
  (a) Montrer qu'il existe un caractère $\chi \in \hat{A}$ tel que $\chi(a)$ est d'ordre e.
  (b) En déduire que $A = \langle a\rangle \times \mathrm{Ker}(\chi)$ puis que A est un produit de groupes cycliques.
6. À l'aide des questions précédentes, montrer les assertions suivantes :
  (a) Le groupe A est isomorphe à son dual.
  (b) Le morphisme $A \to \hat{\hat{A}}, a \mapsto (\chi \mapsto \chi(a))$ est un isomorphisme.
  (c) Si B est un sous-groupe de A, alors le dual de A/B s'identifie au noyau de la surjection $\hat{A} \to \hat{B}$.
  (d) Si $0 \to B \to A \to C \to 0$ est une suite exacte de groupes abéliens finis, il en est de même de $0 \to \hat{C} \to \hat{A} \to \hat{B} \to 0$.
  (e) Tout sous-groupe de A est isomorphe à un quotient de A.

Exercice 3 : Sous-groupes de D_8
On appelle D_8 le groupe des isométries du carré. Quels sont les sous-groupes de D_8 ? Lesquels sont distingués ?

Exercice 4 : Sous-groupes transitifs du groupe symétrique
Soit $n \geq 1$. Un sous-groupe de S_n est dit transitif s'il agit transitivement sur $\{1, 2, ..., n\}$.
1. Montrer que n divise l'ordre de tout sous-groupe transitif de S_n.
2. En déduire quels sont les sous-groupes transitifs de S_p pour p premier.
3. Montrer que tout conjugué d'un sous-groupe transitif est transitif.
4. Nous allons déterminer tous les sous groupes transitifs de S_4.
  (a) Quels sont les sous-groupes transitifs de S_4 d'ordre 12 ?
  (b) Exhiber un 2-Sylow H de S_4 et montrer que $H \cong D_8$.
  (c) Déterminer tous les sous-groupes transitifs de H. On pourra utiliser

l'exercice 3.

(d) Quels sont les sous-groupes transitifs de S_4 à conjugaison près ?

Exercice 5 : Générateurs du groupe symétrique

1. Soit $n \geq 1$. Montrer que la transposition $(1\ 2)$ et le n-cycle $(1\ 2\ ...\ n)$ engendrent S_n.

2. Dans le cas où n est premier, montrer que l'on peut remplacer la transposition $(1\ 2)$ par n'importe quelle transposition et le n-cycle $(1\ 2\ ...\ n)$ par n'importe quel n-cycle.

3. Soit p un nombre premier. Soit G un groupe fini qui agit fidèlement et transitivement sur un ensemble $X = \{x_1, ..., x_p\}$ à p-éléments. Supposons qu'il existe $g \in G$ tel que $g \cdot x_1 = x_2$, $g \cdot x_2 = x_1$ et $g \cdot x_i = x_i$ pour $i \geq 2$. Montrer que $G \cong S_p$.

Exercice 6 : Autour du groupe affine

Soient $m \geq 1$ un entier naturel et R un anneau. Posons :

$$GA_m(R) = \left\{ \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} | A \in GL_m(R), a \in R^m \right\} \subseteq GL_{m+1}(R).$$

1. Pour $g \in GA_m(R)$ et $x \in R^m$, on pose $g \cdot x = Ax + a$. Montrer que cela définit une action fidèle et transitive sur R^m.

À partir de maintenant, on suppose que $m = 1$ et que $R = \mathbb{Z}/n\mathbb{Z}$.

2. Montrer que $GA_1(\mathbb{Z}/n\mathbb{Z})$ s'identifie à un sous-groupe transitif de S_n, autrement dit, montrer qu'il existe un morphisme de groupes injectif $f : GA_1(\mathbb{Z}/n\mathbb{Z}) \to S_n$.

3. Montrer que $GA_1(\mathbb{Z}/n\mathbb{Z})$ possède un sous-groupe distingué isomorphe à D_{2n}. Pour quelles valeurs de n l'image de ce sous-groupe par f est-elle contenue dans A_n ?

4. Montrer que pour $n \in \{3, 4, 6\}$ on a $GA_1(\mathbb{Z}/n\mathbb{Z}) \cong D_{2n}$.

5. Dresser la liste des sous-groupes de $GA_1(\mathbb{Z}/5\mathbb{Z})$. Lesquels sont distingués ?

Exercice 7 : Groupes résolubles

On rappelle qu'un groupe G est dit résoluble s'il existe une suite de sous-groupes emboîtés $G = G_0 \rhd G_1 \rhd ... \rhd G_r = 1$. telle que G_{i+1}/G_i est abélien pour $i \in \{0, 1, ..., r-1\}$. Pour chaque groupe G on note $D(G)$ son sous-groupe dérivé et $D^n(G) = D(D^{n-1}(G))$.

1. Montrer qu'un groupe G est résoluble si, et seulement si, il existe un entier naturel n tel que $D^n(G) = 1$.

2. (a) Montrer que tout sous-groupe d'un groupe résoluble est résoluble.

(b) Montrer que tout quotient d'un groupe résoluble est résoluble.
(c) Montrer que si G est un groupe possédant un sous-groupe distingué résoluble H tel que G/H est résoluble, alors G est résoluble.

3. (a) Pour quelles valeurs de n le groupe S_n est-il résoluble ?
(b) Pour quelles valeurs de n le groupe D_{2n} est-il résoluble ?
(c) Pour quelles valeurs de n le groupe $GA_1(\mathbb{Z}/n\mathbb{Z})$ est-il résoluble ?

Exercice 8 (difficile) : Sous-groupes résolubles transitifs de S_p
Soit p un nombre premier. Dans cet exercice, nous allons étudier les sous-groupes résolubles transitifs de S_p. Pour ce faire, on rappelle qu'il est possible de voir $GA_1(\mathbb{Z}/p\mathbb{Z})$ comme sous-groupe de S_p, et on note $\tau \in GA_1(\mathbb{Z}/p\mathbb{Z})$ la translation $x \mapsto x+1$.

0. *(Question préliminaire)* Montrer que si $g \in S_p$ vérifie $g\tau g^{-1} \in GA_1(\mathbb{Z}/p\mathbb{Z})$, alors $g \in GA_1(\mathbb{Z}/p\mathbb{Z})$.

1. Montrer que tout sous-groupe de S_p conjugué à un sous-groupe de $GA_1(\mathbb{Z}/p\mathbb{Z})$ contenant τ est un sous-groupe résoluble transitif de S_p.

2. Soit H un sous-groupe résoluble transitif de S_p. On considère une suite de sous-groupes emboîtés $H = H_0 \rhd H_1 \rhd ... \rhd H_r = 1$ telle que, pour $i \in \{0, ..., r-1\}$, le groupe H_i/H_{i+1} est cyclique d'ordre premier.
(a) Expliquer pourquoi une telle suite existe.
(b) En tant que sous-groupes de S_p, les H_i (pour $i \in \{0, ..., r\}$ agissent sur $\mathbb{Z}/p\mathbb{Z}$. Montrer que H_{r-1} agit transitivement sur $\mathbb{Z}/p\mathbb{Z}$, puis que $H_{r-1} \cong \mathbb{Z}/p\mathbb{Z}$.
(c) En déduire que H est conjugué à un sous-groupe de $GA_1(\mathbb{Z}/p\mathbb{Z})$ contenant τ.
(d) Combien de sous-groupes résolubles transitifs possède S_p à conjugaison près ?

3. Montrer qu'un élément non trivial d'un sous-groupe résoluble transitif de S_p possède au plus un point fixe.

4. Soit H un sous-groupe transitif de S_p tel que tout élément de H a au plus un point fixe. Soit S l'ensemble des éléments de H n'ayant pas de point fixe.
(a) Montrer que S est stable par conjugaison par tout élément de H.
(b) Montrer que $|S| = p-1$, puis qu'il existe un p-cycle σ tel que $S = \{\sigma, \sigma^2, ..., \sigma^{p-1}\}$.
(c) Déduire de ce qui précède que H est un groupe résoluble.

Exercice 9 : Produits semi-directs

1. Montrer que $S_n \cong A_n \rtimes \mathbb{Z}/2\mathbb{Z}$. Le produit est-il direct ?
2. Montrer que $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Le produit est-il direct ?
3. Montrer que $GA_m(R) \cong R^m \rtimes GL_m(R)$. Le produit est-il direct ?