Université Pierre & Marie Curie — Année 2010-2011
Master de Mathématiques — MM014 Théorie des groupes
Professeur: J.F.Dat — A.Guilloux

Adresse mail de Antonin Guilloux : aguillou@math.jussieu.fr

Feuille 1

Cette feuille d'exercices porte sur les groupes cycliques, les groupes $\mathbb{Z}/n\mathbb{Z}$, les groupes symétriques et autres groupes classiques.

Théorèmes d'isomorphisme

Exercice 1 Soient G un groupe, H un sous groupe distingué de G et K un sous groupe de G.

a) Montrer que $KH = HK$ est un sous groupe de G, que H est un sous groupe distingué de HK et que $H \cap K$ est un sous groupe distingué de K.

b) Montrer que les groupes $K/(H \cap K)$ et KH/H sont isomorphes.

Exercice 2 Soient G un groupe et H un sous groupe distingué de G.

a) Montrer que la projection canonique $\pi : G \to G/H$ induit une bijection entre l'ensemble des sous groupes A de G contenant H et l'ensemble des sous groupes A/H de G/H.

b) Montrer que A est distingué dans G si et seulement si A/H est distingué dans G/H.

c) Montrer que les groupes $(G/H)/(A/H)$ et G/A sont isomorphes.

Exercice 3 Soient G et G' deux groupes finis, et $\varphi : G \to G'$ un morphisme de groupe. On note $Cl(G)$ (resp.$Cl(G')$) l'ensemble des classes de conjugaisons de G (resp. G').

1. Montrer que φ induit une application $\widetilde{\varphi} : Cl(G) \to Cl(G')$.
   On suppose désormais que $\widetilde{\varphi}$ est une bijection, et on va montrer que φ est un isomorphisme de groupes.
2. Montrer que φ est injective.
3. Montrer que $G' = \cup_{k \in G'} k\varphi(G)k^{-1}$.
4. Montrer que si h et k ont même classe à droite modulo $\varphi(G)$, alors $h\varphi(G)h^{-1} = k\varphi(G)k^{-1}$.
5. En déduire que φ est surjective.

Groupes cycliques

Exercice 4 Soit $n \geq 1$ un entier naturel.

a) Soit $k \in \mathbb{Z}$ un entier. Quel est le cardinal du sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de k modulo n ? Si $m \geq 1$, combien y a t-il de morphismes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

b) Soit d un diviseur de n. Combien y a t-il d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$? Démontrer la relation

$$\forall n \geq 1, \quad \sum_{d|n} \varphi(d) = n$$

c) Soit G un sous-groupe fini du groupe multiplicatif d'un corps commutatif, et n son ordre. Pour chaque diviseur d de n, on note $\psi(d)$ le nombre d'éléments de G qui sont d'ordre d. Montrer que $\psi(d)$ vaut 0 ou $\varphi(d)$.

d) Montrer que l'on a $\sum_{d|n} \psi(d) = n$.

e) Déduire de ce qui précède que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Exercice 5 Soit G un groupe commutatif, et x, y deux éléments de G d'ordre respectif m et n.

a) Montrer que si m et n sont premiers entre eux, xy est d'ordre mn.

b) Montrer que dans le cas général, il existe un diviseur m' de m et un diviseur n' de n tels que m' et n' soient premiers entre eux et $m'n' = \text{ppcm}(m, n)$.

c) Montrer qu'il existe dans G un élément d'ordre $\text{ppcm}(m, n)$.

d) Montrer que si G est d'*exposant* N, c'est-à-dire que $\forall g \in G, g^N = 1$ et N est le plus petit entier non nul jouissant de cette propriété, G admet un élément d'ordre N. Montrer que ce n'est pas forcément le cas si G n'est pas commutatif.

e) En déduire une autre démonstration du fait que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Restes chinois

Exercice 6 Soit $m \geq 1$ et $n \geq 1$ deux entiers naturels, et

$$\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

l'homomorphisme naturel. Quel est l'image de π et quel est son noyau ? Résoudre dans $\mathbb{Z}$ les congruences suivantes :

a) $k \equiv 3 \pmod 5$ et $k \equiv 5 \pmod 7$,

b) $k \equiv 7 \pmod{15}$ et $k \equiv 4 \pmod 6$,

c) $k \equiv 2 \pmod{21}$ et $k \equiv 12 \pmod{35}$.

Exercice 7 1. Donner l'ordre des groupes suivants, et dire (en justifiant brièvement les réponses) s'ils sont cycliques :

$$(\mathbb{Z}/11\mathbb{Z})^*, (\mathbb{Z}/10\mathbb{Z})^*, (\mathbb{Z}/9\mathbb{Z})^*, (\mathbb{Z}/16\mathbb{Z})^*.$$

2. On pose maintenant $N = 8.9.10.11$. Calculer l'exposant du groupe $(\mathbb{Z}/N\mathbb{Z})^*$.
3. Déterminer le nombre d'entiers $a \in [1, ..., N]$ tels que $a^5 \equiv 1 \pmod{N}$.

Exercice 8

a) Montrer que le groupe $Aut(\mathbb{Z}/n\mathbb{Z})$ des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est naturellement isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$. En déduire qu'il est commutatif.

b) Montrer que si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition de n en facteurs premiers, on a

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*.$$

c) Soit p un nombre premier impair. Montrer qu'il existe un élément d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, et aussi dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$, si $\alpha \geq 1$. Montrer que l'ordre de la classe de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est $p^{\alpha-1}$. En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique.

d) Expliciter la structure de $(\mathbb{Z}/2\mathbb{Z})^*$, $(\mathbb{Z}/4\mathbb{Z})^*$ et $(\mathbb{Z}/8\mathbb{Z})^*$. Montrer que pour $\alpha \geq 2$, l'ordre de la classe de 5 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est $2^{\alpha-2}$. Montrer que dans ce cas

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

qui n'est pas cyclique.

e) Expliciter $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Remarquer qu'il n'est pas commutatif.

Groupe symétrique

Exercice 9 Ecrire la table de multiplication de $\mathcal{S}_3$. Enumérer tous les sous-groupes de $\mathcal{S}_3$ et de $\mathcal{A}_4$. Lesquels sont distingués ?

Exercice 10 Montrer que le groupe symétrique $\mathcal{S}_n$ admet les systèmes minimaux de générateurs suivants :

a) Les transpositions $(1, i)$ pour $2 \leq i \leq n$.

b) Les transpositions $(i, i+1)$ pour $1 \leq i \leq n-1$.

c) Le cycle $(1, 2, \ldots, n)$ et la transposition $(1, 2)$.

d) Si n est premier, le cycle $(1, 2, \ldots, n)$ et n'importe quelle transposition.

Exercice 11 Montrer que le groupe alterné $\mathcal{A}_n$ est engendré par les 3-cycles. Montrer que $\mathcal{A}_n$ admet les systèmes de générateurs suivants :

a) Les 3-cycles $(1, 2, i)$ pour $3 \leq i \leq n$.

b) Les 3-cycles $(i, i+1, i+2)$ pour $1 \leq i \leq n-2$.

c) Montrer que le premier système est minimal, mais que le second ne l'est pas si $n \geq 5$.

Exercice 12

a) Soit G un sous-groupe distingué de $\mathcal{A}_n$. Montrer que si G contient un 3-cycle, alors $G = \mathcal{A}_n$.

b) Soit $\sigma \in \mathcal{A}_n$. Montrer qu'au moins une des propriétés suivante est vraie :
- $\sigma = 1$,
- σ est un 3-cycle,
- σ est un produit de $n/2$ transpositions disjointes,
- σ est un produit de 3-cycles et de 1-cycles disjoints,
- il existe une permutation $\tau \in \mathcal{A}_n$ telle que $\tau\sigma\tau^{-1}\sigma^{-1}$ est un 3-cycleé. On pourra considérer séparément le cas où σ a un cycle de longueur au moins 4.

c) En déduire que pour $n \geq 5$, $\mathcal{A}_n$ est un groupe simple.

Exercice 13 On rappelle que toute permutation $\sigma \in \mathcal{S}_n$ se décompose de façon unique en cycles de supports disjoints, et on lui fait correspondre une partition $k = k(\sigma)$ de la façon suivante : k_i est le nombre de i-cycles qui interviennent dans cette décomposition.

a) Montrer qu'une permutation τ de $\mathcal{S}_n$ commute avec un n-cycle σ si et seulement si τ est une puissance de σ.

b) Montrer que dans le cas général, le commutant de σ, c'est-à-dire le sous-groupe de $\mathcal{S}_n$ formé des permutations τ telles que $\sigma\tau = \tau\sigma$ a pour cardinal

$$\prod_i i^{k_i} k_i!.$$