Les exercices étoilés (*) s'adressent aux seuls étudiants inscrits à l'unité MO12

Feuille d'exercices 1

Groupes cycliques et corps finis

Exercice 1. *Etude des sous-groupes de* $\mathbb{Z}/n\mathbb{Z}$

(1) Montrez que tout groupe cyclique d'ordre n *est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$*;*

(2) Montrez que tout sous-groupe d'un groupe cyclique est cyclique;

(3) Montrez que pour $d|n$*, il existe un unique sous-groupe d'ordre* d *de* $\mathbb{Z}/n\mathbb{Z}$*;*

(4) Donnez le cardinal du sous-groupe engendré par k *dans* $\mathbb{Z}/n\mathbb{Z}$*;*

(5) Montrez que $n = \sum_{d|n} \varphi(d)$ *où* $\phi(d)$ *est l'indicatrice d'Euler, c'est à dire le nombre de générateurs de* $\mathbb{Z}/d\mathbb{Z}$*.*

Exercice 2. *(i) Donnez l'ordre de* k *dans* $\mathbb{Z}/n\mathbb{Z}$ *et déduisez-en le cardinal de l'ensemble des éléments d'ordre* d *(resp. d'ordre divisant* d*) dans* $\mathbb{Z}/n\mathbb{Z}$*.*

(ii) Donnez le cardinal de l'ensemble des éléments d'ordre divisant d *dans* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*.*

(iii) Pour $d = pq$ *avec* p *et* q *premiers divisant* n*, donnez le nombre d'éléments d'ordre* d *dans* $(\mathbb{Z}/n\mathbb{Z})^2$*;*

(iv) Quel est le cardinal de l'ensemble des éléments d'ordre p^α *dans* $\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_r}\mathbb{Z}$ *pour* $0 < \alpha \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_r$*.*

Exercice 3. *Soit* $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *l'application qui à* $k \in \mathbb{Z}$ *associe sa classe modulo* n *et* m*. Précisez le noyau et l'image de* π*. Donnez alors l'ensemble des* $k \in \mathbb{Z}$ *tels que*

(i) $k \equiv 2 \bmod 5$ *et* $k \equiv 4 \bmod 7$*;*

(ii) $k \equiv 3 \bmod 10$ *et* $k \equiv 2 \bmod 6$*;*

(iii) $k \equiv 4 \bmod 10$ *et* $k \equiv 2 \bmod 6$*;*

Que peut-on dire de la congruence de k *modulo* 10 *sachant* $k \equiv 3 \bmod 6$ *?*

Exercice 4. *Résoudre dans* $\mathbb{Z}$ *les congruences suivantes:*

(i) $3x \equiv 4 \bmod 7$*;*

(ii) $9x \equiv 12 \bmod 21$*;*

(iii) $103x \equiv 612 \bmod 676$*.*

Exercice 5. *Donnez la congruence modulo* 18 *de* 1823^{242} *puis celle de* 2222^{321} *modulo* 20*.*

Exercice 6. *Montrez en utilisant le théorème chinois que* $n^7 \equiv n \bmod 42$*.*

Exercice 7. *Donnez les morphismes de groupe $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ puis ceux de $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$. Trouvez une condition nécessaire et suffisante sur m et n pour que tout morphisme $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ soit nul.*

Exercice 8. *(*) Corps finis: définition, exemples, applications*

(1) Montrez que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

(2) Justifier pour n divisant n', l'écriture $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ et étudier la réciproque. Donner un sens et justifier l'égalité:

$$\overline{\mathbb{F}}_p = \bigcup_{n>1} \mathbb{F}_{p^{n!}}.$$

(3) Montrer les isomorphismes suivant (donner si possible un générateur du groupe des inversibles):

(i) $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$;

(ii) $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1)$;

(iii) $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4+X+1)$; *donner dans cet isomorphisme l'image de* $\mathbb{F}_4 \subset \mathbb{F}_8$ *et en déduire* $\mathbb{F}_{16} \simeq \mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+X+1)$.

(iv) $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+X+1)$.

(4) **Le solitaire:** *utiliser la description du corps $\mathbb{F}_4$ pour donner deux invariants du jeu du solitaire (cf TD).*

Exercice 9. *Etude de $(\mathbb{Z}/n\mathbb{Z})^\times$:*

(1) Montrez que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$. En déduire que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est abélien.

(2) Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Prouver que $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$.

(3) Soit p premier impair et $\alpha \geqslant 2$.

- *Montrez que pour tout $k \in \mathbb{N}$, il existe $\lambda \in \mathbb{N}\backslash\{0\}$ premier avec p tel que $(1+p)^{p^k} = 1+\lambda p^{k+1}$. En déduire l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.*
- *En utilisant le point (1) de l'exercice 8, constatez que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$;*
- *En considérant le morphisme naturel, $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$, montrez que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ contient un élément x d'ordre $p-1$:*
- *Montrez $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/(\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$;*

(4) Le cas de 2.

- *Déterminer $(\mathbb{Z}/2\mathbb{Z})^\times$ et $(\mathbb{Z}/4\mathbb{Z})^\times$;*
- *Soit $\alpha \geqslant 3$ et $k \in \mathbb{N}$. Montrez que $5^{2^k} = 1+\lambda 2^{k+2}$ avec l impair. En déduire l'ordre de 5 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.*

– *En considérant le morphisme canonique de* $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ *dans* $(\mathbb{Z}/4\mathbb{Z})^\times$*, montrer que* $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2})$.

Le groupe des permutations

Pour $n > 0$, on note $\mathcal{S}_n$ le groupe des permutations de l'ensemble $\{1, \cdots, n\}$, et $\mathcal{A}_n$ son sous-groupe des permutations paires.

Exercice 10. *Systèmes de générateurs*

(a) Montrez que $\mathcal{S}_n$ *est engendré par les systèmes suivants et pas par un sous-ensemble strict:*

- *les transpositions* $(1, i)$ *pour* $i = 2, \cdots, n$*;*
- *les transpositions* $(i, i+1)$ *pour* $i = 1, \cdots, n-1$*;*
- *le cycle* $(1, \cdots, n)$ *et la transposition* $(1, 2)$.

(b) Montrez que $\mathcal{A}_n$ *pour* $n \geqslant 3$*, est engendré par les* 3*-cycles.*

Exercice 11. *Décomposition en cycles à supports disjoints*

(a) Donnez la décomposition en cycles à supports disjoints de $(1, 2, 3) \circ (2, 4) \circ (1, 3)$ *et de* $(1, 2, \cdots, n-1) \circ (1, n)$.

(b) Classes de conjugaisons

- *Quelle est la décomposition en cycles à supports disjoints de* $\sigma s \sigma^{-1}$ *en fonction de celle de* s *?*
- *Quel est l'ordre maximal d'un élément de* $\mathcal{S}_5$ *?*
- *Quelle est la décomposition en cycles à supports disjoints de* c^k*, où* $c = (1, \cdots, n)$ *?*

(c) Commutants:

- *Donnez le centre de* $\mathcal{S}_n$*;*
- *Quel est le commutant de* $(1, \cdots, n)$ *?*
- *Donnez une formule du cardinal du commutant de* $\sigma \in \mathcal{S}_n$ *en fonction de sa décomposition en cycles à supports disjoints.*

Exercice 12. *Simplicité de* $\mathcal{A}_n$

(a) Etudiez les cas $n \leqslant 4$.

(b) $n = 5$*: soit* H *un sous-groupe distingué de* $\mathcal{A}_5$ *non trivial:*

- *montrez que les éléments d'ordre* 2 *sont conjugués dans* $\mathcal{A}_5$*;*
- *montrez que si* H *contient un* 5*-cycle, il les contient tous,*
- *en déduire que* $H = \mathcal{A}_5$*, i.e. que* $\mathcal{A}_5$ *est simple*

(c) $n \geqslant 5$*: soit* H *un sous-groupe distingué de* $\mathcal{A}_n$ *non trivial et soit* $\sigma \in H$ *différent de l'identité. Soit alors* $a \in \{1, \cdots, n\}$ *tel que* $b = \sigma(a) \neq a$.

- *Soient* $c \in \{1, \cdots, n\} \backslash \{a, b, \sigma(b)\}$ *et* $\tau = (acb)$. *Montrez que* $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ *"dérange" au plus* 5 *éléments et que* $\rho \neq \mathrm{Id}$.

- *Soit* $E \subset \{1, \cdots, n\}$ *de cardinal* 5 *contenant le support de* ρ. *En considérant l'application* $i : \mathcal{A}_5 \simeq \mathcal{A}(E) \longrightarrow \mathcal{A}_n$ *définie par* $i(\sigma)_{|E} = \sigma$ *et* $i(\sigma)_{\{1,\cdots,n\}\backslash E} = \mathrm{Id}$ *et en remarquant que* $\rho \in H$, *montrez la simplicité de* $\mathcal{A}_n$.

- *En déduire que* $D(\mathcal{A}_n) = D(\mathcal{S}_n) = \mathcal{A}_n$.

(d) Montrez que pour $n \geqslant 5$, *les seuls sous-groupes distingués de* $\mathcal{S}_n$ *sont:* $\{\mathrm{Id}\}$, $\mathcal{A}_n$ *et* $\mathcal{S}_n$.

Exercice 13. *(*) Petits groupes algébriques et groupes de permutations*
Montrez que $PGL_2(\mathbb{F}_2) \simeq \mathcal{S}_3$, $PGL_2(\mathbb{F}_3) \simeq \mathcal{S}_4$, $PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$ *et* $PGL_2(\mathbb{F}_5) \simeq \mathcal{S}_5$ [1]. *En déduire que* $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$ *et* $PSL_2(\mathbb{F}_5) \simeq \mathcal{A}_5$.

Groupe opérant sur un ensemble: généralités

Exercice 14. *Un p-groupe est un groupe de cardinal une puissance de p (p premier). Montrez que le centre d'un p-groupe n'est pas réduit à l'élément neutre et en déduire qu'un p-groupe G possède des sous-groupes distingués de tous ordres (divisant* $|G|$ *bien sûr!).*

Exercice 15. *Soit G un groupe fini, p le plus petit facteur premier de* $|G|$, *H un sous groupe d'indice p. Montrer que H est distingué dans G.*

Exercice 16. *Soit H un sous-groupe d'indice n de* $\mathcal{S}_n$. *Montrer que H est isomorphe à* $\mathcal{S}_{n-1}$. *Indication: On traitera les cas* $n \leqslant 4$ *séparément. Pour* $n \geqslant 5$ *considérer "le" morphisme* $\phi : \mathcal{S}_n \to \mathcal{S}(\mathcal{S}_n/H)$. *Montrer que* ϕ *est injectif et donner l'image de H.*

Exercice 17. *(*) On va montrer le théorème de Wedderburn, à savoir que tout corps fini est commutatif.*

(i) Soit k un corps fini et Z son centre de cardinal q; montrez que q est une puissance d'un nombre premier p et que $|k| = q^n$, *pour* $n \in \mathbb{N}$.

(ii) On suppose k non commutatif, soit $n > 1$, *et on fait opérer* $k^\times$ *sur lui-même par automorphismes intérieurs. On note* $\omega(x)$ *l'orbite de* $x \in k^\times$ *et* $k_x^\times$ *son stabilisateur. Montrez que* $|k_x| = q^d$ *pour un diviseur d de n et donnez le cardinal de* $\omega(x)$.

(iii) Soit $\Phi_n(X)$ *le n-ième polynôme cyclotomique; montrez que* $\Phi_n(q)$ *divise le cardinal de* $\omega(x)$ *pour* $x \notin Z$.

(iv) En écrivant l'équation aux classes montrez que $\Phi_n(q)$ *divise* $q - 1$.

(v) Montrez que si $z \in \mathbb{C}$ *est de module* 1, *alors* $|q - z| > q - 1$ *et conclure.*

[1] Pour ce dernier utiliser l'exercice 11