Série 1

Exercice 1. Démontrer les assertions du paragraphe 1.1.4 du cours.

Exercice 2. Soit $X = \{\text{a}, \text{au}, \text{et}, \text{bas}, \text{eau}, \text{cru}, \text{elu}, \text{me}, \text{ne}, \text{met}, \text{bar}\}$ un ensemble de mots et R la relation d'équivalence sur X définie par

$$x\,R\,y \quad \Leftrightarrow \quad x \text{ et } y \text{ commencent par la même lettre.}$$

Déterminer l'ensemble quotient X/R. Qu'elle est la classe d'équivalence de elu ?

Exercice 3. Déterminer la décomposition canonique de l'application

$$\begin{aligned} f\colon \mathbb{R} &\rightarrow \mathbb{R} \\ x &\rightarrowtail \cos x. \end{aligned}$$

Exercice 4. Soient X et Y des ensembles non-vides et $Z \subset X$. Sur Y^X, on définit la relation

$$f R g \quad \Leftrightarrow \quad f\lceil_Z = g\lceil_Z.$$

1. Montrer que R est une relation d'équivalence.
2. Montrer que l'application $\phi\colon Y^X \rightarrow Y^Z$ définie par $\phi\colon f \mapsto f\lceil_Z$ est compatible avec R.
3. Montrer que l'application

   $$\bar{\phi}\colon Y^X/R \rightarrow Y^Z,$$

   obtenue par passage au quotient, est bijective (indication: construire l'application réciproque $\bar{\phi}^{\,-1}$). En conclure que Y^X/R est équipotent à Y^Z.
4. Montrer que les classes d'équivalence de R sont équipotentes à $Y^{X\setminus Z}$.
5. Montrer que si X et Y sont finis $|Y^X| = |Y^Z| \cdot |Y^{X\setminus Z}|$.
6. Montrer par induction sr $|X|$ que $|Y^X| = |Y|^{|X|}$.

Exercice 5. Soit X un ensemble non-vide. A un sous-ensemble $A \subset X$ on associe la fonction caractéristique

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{sinon.} \end{cases}$$

1. Montrer que l'application $\phi\colon A \mapsto \chi_A$ est une bijection de 2^X dans $\{0,1\}^X$.
2. Montrer que si X est fini, $|2^X| = 2^{|X|}$. (Indication: utiliser le résultat de l'exercice 2)

Série 2

Exercice 1. Montrer que l'ensemble $\mathbb{Z}$ est dénombrable.

Exercice 2. Soient $(A_i)_{i\in I}$ et $(B_i)_{i\in I}$ des familles d'ensembles disjoints

$$A_i \cap A_j = \varnothing \quad \text{et} \quad B_i \cap B_j = \varnothing,$$

pour $i \neq j$. Montrer que si, pour tout $i \in I$, A_i et B_i sont équipotents alors les réunions $\cup_{i\in I} A_i$ et $\cup_{i\in I} B_i$ sont équipotentes. (Indication: définir une application f par $f(x) = f_i(x)$ si $x \in A_i$ où les $f_i: A_i \to B_i$ sont des bijections).

Exercice 3. Montrer que $\mathbb{N} \times \mathbb{N}$ est dénombrable.

Exercice 4. Soit G un ensemble non-vide muni d'une loi de composition interne associative et telle que, pour tout $a, b \in G$:

i. Il existe $x \in G$ tel que $a \cdot x = b$.

ii. Il existe $y \in G$ tel que $y \cdot a = b$.

Montrer que G est un groupe

Exercice 5. Soit G un ensemble muni d'une loi de composition interne associative et telle que :

i. Il existe un élément neutre à droite $e \in G$ tel que $a \cdot e = a$ pour tout $a \in G$.

ii. Pour tout $a \in G$ il existe un symétrique à droite $a' \in G$ tel que $a \cdot a' = e$.

Montrer que G est un goupe.

Série 3

Exercice 1. Soit $m>0$ un entier et $G=\mathbb{Z}_m=\{\bar{0},\bar{1},\ldots,\overline{m-1}\}$.

1. Montrer que G est cyclique.
2. Montrer que $(\bar{n})=G$ si et seulement si $\bar{1}\in(\bar{n})$.
3. Montrer que $\bar{n}$ est un générateur de G si et seulement si n et m sont premiers entre eux.

Exercice 2. Soit $m>0$ un entier, $\xi=e^{2i\pi/m}$ et $C_m=\{\xi^k|k\in\mathbb{Z}\}$.

1. Montrer que C_m est un sous-groupe de $\mathbb{C}^*$.
2. Montrer que C_m est un groupe cyclique.
3. Soit $\bar{k}=k+m\mathbb{Z}\in\mathbb{Z}_m$. Montrer que pour tout $n\in\bar{k}$ on a $\xi^n=\xi^k$. En conclure que $\phi(\bar{k})=\xi^k$ définit une application $\phi\colon\mathbb{Z}_m\to C_m$.
4. Montrer que ϕ est un isomorphisme.
5. Montrer que l'ordre du groupe C_m est m.

Exercice 3. Soit G un groupe cyclique et $\phi\in\mathrm{Hom}(G,H)$.

1. Montrer que si $a\in G$ est un générateur de G, alors $\phi(a)$ est un générateur de $\mathrm{Im}\,\phi$.
2. Montrer que $\mathrm{Im}\,\phi$ est un sous-groupe cyclique de H.

Exercice 4.

1. Montrer que si $k\equiv k'$ et $n\equiv n'$ (mod m) alors $kn\equiv k'n'$ (mod m). En conclure que $\bar{k}\cdot\bar{n}=\overline{kn}$ définit une loi de composition interne associative et commutative dans $\mathbb{Z}_m$.
2. Montrer que $\bar{1}$ est un élément neutre pour cette loi.
3. Montrer que $\bar{n}$ admet un symétrique pour cette loi si et seulement si n et m sont premiers entre eux.
4. Montrer que $\mathbb{Z}_m^*=\{\bar{k}\in\mathbb{Z}_m|\,k$ et m sont premiers entre eux$\}$ est un groupe abélien.

Série 4

Exercice 1. Soit G un groupe cyclique et $a \in G$ un générateur.

1. Soit H un sous-groupe de G. Montrer que G/H est cyclique et que $a \cdot H$ est un générateur de G/H. (Indication: considérer la surjection canonique $\pi: G \to G/H$ et utiliser l'exercice 3 de la série 3.)
2. Soit $H \neq \{e\}$ un sous-groupe de G. Montrer que H est cyclique et que si $\mu = \min\,\{k \in \mathbb{N}^* | a^k \in H\}$ alors a^μ est un générateur de H. (Indication: la même que pour la question précédente.)
3. Montrer que l'ensemble de tous les générateurs de G est
$$\{a^k | k \text{ et } |G| \text{ sont premiers entre eux}\},$$
si G est fini et $\{a, a^{-1}\}$ sinon.

Exercice 2. Soient G un groupe cyclique et $a \in G$ un générateur.

1. Soit $H \neq \{e\}$ un sous-groupe de G. Montrer que le quotient G/H est fini et que $H = (a^{[G:H]})$.
2. Montrer que si G est fini et $n \in \mathbb{Z}$ on a
$$\omega(a^n) = \frac{|G|}{(n, |G|)},$$
où $(\cdot, \cdot)$ dénote le PGCD.
3. On suppose que G est fini. Montrer que pour tout diviseur d de $|G|$ il existe un et un seul sous-groupe G_d de G d'ordre d. Déterminer un générateur de G_d.

Série 5

Exercice 1. Soit m un entier positif. On considère le groupe additif

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\},$$

et le groupe multiplicatif (exercice 4, série 3)

$$\mathbb{Z}_m^* = \{\bar{u} \in \mathbb{Z}_m | u \text{ et } m \text{ sont premiers entre eux}\}.$$

i. Montrer que l'application ϕ: $\mathrm{Aut}(\mathbb{Z}_m) \to \mathbb{Z}_m$ définie par $\phi(\sigma) = \sigma(\bar{1})$ est un morphisme.
ii. Montrer que $\mathrm{Im}\,\phi = \mathbb{Z}_m^\star$.
iii. Montrer que $\mathrm{Aut}(\mathbb{Z}_m) \simeq \mathbb{Z}_m^\star$. (Indication : utiliser le théorème d'isomorphisme).
iv. Déterminer le centre du groupe $\mathrm{Aut}(\mathbb{Z}_m)$.

Exercice 2. Montrer que $\mathbb{Z}_3^* \simeq \mathbb{Z}_4^* \simeq \mathbb{Z}_6^* \simeq C_2$ et que $\mathbb{Z}_8^* \simeq \mathbb{Z}_{12}^* \simeq C_2 \times C_2$.

Exercice 3. Trouver deux groupes non-isomorphes G et H tels que

$$\mathrm{Aut}(G) \simeq \mathrm{Aut}(H).$$

Exercice 4. On considère le groupe diédral de degré $n \geqslant 2$,

$$D_n = \{I, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\},$$

où ρ est une rotation du plan d'angle $2\pi/n$ et σ une réflexion.

i. Montrer de $\mathcal{R}_n = \{I, \rho, \ldots, \rho^{n-1}\}$ est un sous-groupe distingué de D_n.
ii. Montrer que $\mathcal{S} = \{I, \sigma\}$ est un sous-groupe de D_n et que $D_n = \mathcal{R}_n \cdot \mathcal{S}$.
iii. D_n est-il le produit direct de $\mathcal{R}_n$ et de $\mathcal{S}$? (Indication : considérer séparément les cas $n = 2$ et $n \geqslant 3$.)
iv. Montrer que si n est impair, tous les sous-groupes distingués propres de D_n sont abéliens. En conclure que D_n est indécomposable. (Indication : si un sous-groupe distingué H contient un élément a il doit contenir tous ses conjugués. Les classes de conjugaison de D_n ont été calculées en cours.)
v. Montrer que si $n \geqslant 4$ est pair, D_n est décomposable si et seulement si $n/2$ est impair et que dans ce cas

$$D_n = D_{n/2} \otimes Z(D_n),$$

où $Z(D_n)$ est le centre de D_n. (Indication : montrer que D_n n'a que 2 sous-groupes distingués non-abéliens H_1 et H_2. Montrer qu'ils sont d'ordre n et en conclure qu'une décomposition de D_n doit prendre la forme $H_i \otimes K$ où K est un sous-groupe cyclique d'ordre 2 distingué. Montrer que le seul sous-groupe satisfaisant cette condition est le centre de D_n.)

.

Série 6

Exercice 1. On considère le groupe symétrique S_N.

i. Montrer qu'un cycle $c = (i_1 i_2 \ldots i_\ell) \in S_N$, de longueur ℓ, est un élément d'ordre ℓ.

ii. Montrer qu'une permutation $\sigma = c_1 \cdots c_n \in S_N$, produit de cycles disjoints $c_1, \ldots, c_n$ de longueurs respectives $\ell_1, \ldots, \ell_n$, est d'ordre $\mathrm{PPCM}(\ell_1, \ldots, \ell_n)$.

iii. Montrer que la signature d'une telle permutation est donnée par

$$\varepsilon(\sigma) = (-1)^{(\ell_1+1)+\cdots+(\ell_n+1)}.$$

Exercice 2. On considère le groupe symétrique S_5.

i. Déterminer ses classes de conjugaison ainsi que le cardinal de chacune de ces classes.

ii. Calculer l'exposant de S_5.

iii. Montrer que le groupe alterné A_5 est le seul sous-groupe propre distingué de S_5.

iv. Montrer que A_5 est simple