Exercices de D04
Université Rennes 1

Feuille 2

1. ORDRE D'UN ELEMENT ET GROUPES QUOTIENTS

Exercice 1.0.1. Pour tout entier n>1, trouver un élément d'ordre n de $GL(2,\mathbb{R})$.

Exercice 1.0.2. a) Trouver un groupe fini d'ordre n qui n'a pas d'élément d'ordre n.
b) Soit G un groupe admettant un élément d'ordre n. Montrer qu'il existe un élément d'ordre d pour tout diviseur d de n.

Exercice 1.0.3. Montrer que le seul morphisme possible d'un groupe à 13 éléments dans un groupe à 17 éléments est le morphisme trivial.

Exercice 1.0.4. Trouver les entiers $n > 1$ pour lesquels il existe un groupe fini G possédant un unique élément d'odre n. (Penser aux générateurs de $\frac{\mathbb{Z}}{n\mathbb{Z}}$).

Exercice 1.0.5. Soit x et y deux éléments d'un groupe G.
a) Montrer que x et x^{-1} ont même ordre.
b) Montrer que x et yxy^{-1} ont même ordre.
c)xy et yx ont même ordre.

Exercice 1.0.6. Soit G un groupe. g est un élément de G on appelle conjugué de g tout élément du type hgh^{-1} où h appartient à G.
Montrer que deux éléments conjugués ont même ordre.

Exercice 1.0.7. Montrer que si un groupe posséde un unique élément d'ordre 2, cet élément appartient au centre du groupe.

Exercice 1.0.8. Soit G un groupe et g,h deux éléments de G.
a) Montrer que si $gh = hg$ et $< g > \cap < h >= \{e\}$ alors gh est d'ordre ppcm (ordre(g), ordre(h)).
b) Montrer que si $gh = hg$ et d'ordres premiers ente eux alors gh est d'ordre ordre(g)ordre(h).
c) Montrer que les deux conditions $gh = hg$ et $< g > \cap < h >= \{e\}$ sont nécessaires.
On pourra penser à D_4 et $\frac{\mathbb{Z}}{10\mathbb{Z}}$

Exercice 1.0.9. Soit p un entier premier et G un groupe.Montrer que le nombre d'élḿents d'ordre p est un multiple de $p - 1$.

Exercice 1.0.10. a) On note $GL(2,\mathbb{Z})$ le groupe des matrices inversibles à coeffficients dans $\mathbb{Z}$. Montrer que toute matrice de $GL(2,\mathbb{Z})$ a pour déterminant 1 ou -1.
b) On considére les deux éléments de $GL(2,\mathbb{Z})$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Calculer les ordres de A, B et AB.

Exercice 1.0.11. Soit $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ l'ensemble des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ pour la multiplication. Montrer que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ est isomorphe à $Aut(\frac{\mathbb{Z}}{n\mathbb{Z}})$.

Indication : On pourra montrer que l'application $f : (\frac{\mathbb{Z}}{n\mathbb{Z}})^\times \to Aut(\frac{\mathbb{Z}}{n\mathbb{Z}})$ définie par $f(\bar{k}) = f_{\bar{k}}$ où $f_{\bar{k}}(\bar{x}) = k\bar{x}$ est un isomorphisme. On fera attention à vérifier que f et $f_{\bar{k}}$ sont bien définies.

Exercice 1.0.12. Soit G un groupe et g, h deux éléments de G d'ordre respectifs s et t et tels que $gh = hg$. On va montrer qu'il existe un élément de G d'ordre le ppcm(s, t).

a) Montrez qu'il existe des entiers u, v, u', v' tes que $s = uu', t = vv', uv =$ppcm(s, t).

Indication : Utiliser la décomposition en facteurs premiers de s et t.

b) Montrer que $g^{u'}h^{v'}$ est d'ordre $uv =$ ppcm(s, t).

c) On pose $G = (\frac{\mathbb{Z}}{41\mathbb{Z}})^\times$ le groupe des éléments inversibles pour la multiplication de $\frac{\mathbb{Z}}{41\mathbb{Z}}$.

Calculer les ordres de $\bar{2}$ et $\bar{3}$. En déduire que $(\frac{\mathbb{Z}}{41\mathbb{Z}})^\times$ est cyclique et en donner un générateur.

Exercice 1.0.13. Soit $G = \{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \in M_2(\mathbb{R}) b \neq 0\}$ et $N == \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})\}$

a) Montrer que G est un sous-groupe de $GL(2, \mathbb{R})$ et que N est un sous-groupe distingué de G.

b) Montrer que $\frac{G}{N}$ est isomorphe à $\mathbb{R}^*$.

Exercice 1.0.14. Soit $G = \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. Trouver deux sous-groupes de G, H_1 et H_2 isomorphes tels que $\frac{G}{H_1}$ et $\frac{G}{H_2}$ ne soient pas isomorphes.

On pourra remarquer que H_1 et H_2 ne peuvent etre que d'ordre 2.

Exercice 1.0.15. L'affirmation suivante est-elle vraie ?

Un morphisme de groupe préserve l'ordre des éléments. Et si on remplace le mot morphisme par isomorphisme ?

Exercice 1.0.16. Soit H un sous-groupe distingué de G. Montrer que $Z(H)$ est un sous-groupe distingué de G.

En général $Z(H)$ n'est pas contenu dans $Z(G)$ (cf l'exercice plus bas sur les quaternions)

Exercice 1.0.17. Soit G un groupe et H un sous-groupe distingué de G. L'affirmation suivante est-elle vraie ?

Si g est élément de G d'ordre n alors $\bar{g}$ est d'ordre n dans $\frac{G}{H}$.

Exercice 1.0.18. Soit Gun groupe et H un sous-groupe distingué de G tel que $\frac{G}{H}$ soit d'ordre n.

a) Montrer que si H est d'ordre 2 alors H est un sous-groupe distingué de $Z(G)$. ($Z(G)$ est le centre de G)

b) Montrer que si $x \in G$ et $x^k \in H$ avec $k$et n premiers entre eux alors $x \in H$.

Exercice 1.0.19. Soit G un groupe. Montrer que si $\frac{G}{Z(G)}$ est monogène alors G est commutatif ($Z(G)$ est le centre de G).

Exercice 1.0.20. Rappelons que $D_4 =< r, s >$ où r est d'ordre 4,s d'ordre 2 et $rs = sr^3$.

Montrer que r^2 appartient à $Z(D_4)$.

Quel est le centre, $Z(D_4)$, de D_4. A quel groupe connu $\frac{D_4}{Z(D_4)}$ est -il isomorphe ?

Exercice 1.0.21. (*Le groupe des quaternions)*
Soit $\mathbb{H}$ le groupe engendré par a et b tels que a est d'ordre 4, $b^2 = a^2$ et $ab = ba^3$.
a) Montrer que $\mathbb{H} = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.
b) Montrer que $\mathbb{H}$ a un seul élément d'ordre 2.
c) Montrer que tous les sous-groupes de $\mathbb{H}$ sont distingués. (Cependant $\mathbb{H}$ n'est pas abélien).

Exercice 1.0.22. Les affirmations suivantes sont t'elles vraies ?
Si G est un groupe et H un sou-groupe distingué de G
a) $\frac{G}{H}$ isomorphe à $K \Rightarrow G$ est isomorphe à $H \times K$. *Penser à* D_4
b) $\frac{G}{H}$ isomorphe à $G \Rightarrow G = \{e\}$ *Penser à* $\frac{\mathbb{C}^*}{U_n}$

Exercice 1.0.23. Soit G un groupe et $D(G) =< xyx^{-1}y^{-1} >$ (dit groupe dérivé de G)
a) Montrer que si H est un sous-groupe distingué de G alors $\frac{G}{H}$ est commutatif si et seulement si $D(G) \subset H$.
b) Montrer que tout morphisme f :$G \to G'$ où G' est commutatif se factorise par $\frac{G}{D(G)}$

Exercice 1.0.24. Montrer que se donner un morphisme, f, de groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est équivalent à se donner un entier k tel que $f(\bar{1}) = \tilde{k}$ et $n\tilde{k} = \tilde{0}$, en notant, si x est un entier, par $\bar{x}$ la classe de x modulo n et par $\tilde{x}$ la classe de x modulo m.

Exercice 1.0.25. Existe t'il un morphisme de $\frac{\mathbb{Z}}{12\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{20\mathbb{Z}}$ tel que $f(\bar{3}) = \tilde{10}$? Si oui donner $f(\bar{1})$.

Exercice 1.0.26. Soit f un morphisme de $\frac{\mathbb{Z}}{12\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{30\mathbb{Z}}$

Cet exercice fera intervenir plusieurs quotients. Pour savoir, à tout moment, à quels espaces appartiennent les objets que l'on manipule , nous noterons si x est un entier par $\bar{x}$ la classe de x modulo 12 et par $\tilde{x}$ la classe de x modulo 30.
a) Donner les valeurs possibles de $f(\bar{1})$.
On suppose désormais que $f(\bar{1}) = \tilde{5}$.
b) Décrire les éléments de $\ker(f)$ et ceux de $\mathrm{Im}(f)$.
c) Décrire les éléments de $\frac{\frac{\mathbb{Z}}{12\mathbb{Z}}}{ker(f)}$.
d)Vérifier que $\frac{\frac{\mathbb{Z}}{12\mathbb{Z}}}{ker(f)}$ est isomorphe à $\mathrm{Im}(f)$. On exhibera un isomorphisme.
e) Retrouver d) en utilisant les théorèmes du cours.

Exercice 1.0.27. Pour chacun des morphismes possibles de $\frac{\mathbb{Z}}{12\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{20\mathbb{Z}}$
explicitez le noyau et l'image et vérifier le premier théorème d'isomorphisme.

Exercice 1.0.28. $\frac{\mathbb{Q}}{\mathbb{Z}}$ est-il un groupe fini ? Ses éléments sont-ils tous d'ordre fini ?

Exercice 1.0.29. On sait (cf le cours) que si G est un groupe à 4 éléments ne contenant aucun élément d'orde 4 alors G est isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. Donner le nombre d'isomorphismes possibles.

Exercice 1.0.30. Montrer que se donner un morphisme $\alpha : \frac{\mathbb{Z}}{n\mathbb{Z}} \to Aut(\frac{\mathbb{Z}}{m\mathbb{Z}})$ est équivalent à se donner $\bar{a}$ de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ tel que pgcd(a,m) =1 et $a^n \equiv 1$ (mod m) .

Exercice 1.0.31. Soit p un entier premier impair. On note $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ le groupe des éléments inversibles de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ pour la multiplication et par $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times 2}$ l'ensemble des carrés de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ donc l'ensemble des y de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ tels qu'il existe x de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ et $y = x^2$.

1)Montrer que $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times 2}$ est un groupe.

2) Soit $f : (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times \longrightarrow (\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times 2}$ définie par $f(x) = x^2$.

Montrer que f est un homomorphisme.

3) Soit x élément de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$. Montrer que $x \neq -x$ et que pour tout y de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ on a $f(y) = f(x) \iff y = x$ ou $y = -x$.

4) Montrer qu'il y a exactement $\frac{p-1}{2}$ carrés dans $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$.

Exercice 1.0.32. Soit p un entier premier impair et $g : (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times \longrightarrow (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ définie par $g(x) = x^{\frac{p-1}{2}}$.

1) Montrer que g est un morphisme et que pour tout x $g(x) = 1$ ou $g(x) = -1$

2)On pose $H = \{x \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times \ / g(x) = 1\}$.

2-1) Montrer que H est un sous-groupe de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ et que H contient $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times 2}$.

2-2) Montrer qu'il y a au plus $\frac{p-1}{2}$ éléments dans H.

Exercice 1.0.33. Soit p un entier premier congru à 3 modulo 4.

1) Montrer que $\frac{p+1}{4}$ est un entier.

2) Soit x élément de $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$. Montrer que si x est un carré alors $x^{\frac{p+1}{4}}$ est une racine carrée de x.

3) Existe-il un entier x tel que $x^2 \equiv 5$ modulo 19 ?

4) Existe-il un entier x tel que $x^2 \equiv 14$ modulo 19 ?

Exercice 1.0.34. Soit p un entier premier impair. Montrer qu'il existe un entier a tel que $a^2 \equiv -1$ modulo $p \iff p \equiv 1$ modulo 4.