TD 3 (suite)
Lois de composition internes
Groupes

Polytech Marseille - IRM 1ère année
Alexandra Bac

Méthodologie du raisonnement

(***) Exercices de base à préparer impérativement pour le TD.
($\mathfrak{E}$) Exercices d'entraînement pour assimiler les exercices de base.
($\mathfrak{Ch}$) Exercice challenge à cherche en groupe après le TD.

1 Sous-groupes, sous-groupes engendrés, groupes quotient

Exercice 1 (***)**.** En travaillant dans $\mathbb{Z}/2\mathbb{Z}$, retrouver la règle de divisibilité par 2 (i.e. un nombre est divisible par 2 s'il se termine par un chiffre pair).

Exercice 2 (***)**.** En travaillant dans $\mathbb{Z}/5\mathbb{Z}$, retrouver la règle de divisibilité par 5 (i.e. un nombre est divisible par 5 s'il se termine par 0 ou 5).

Exercice 3 (***)**.** En travaillant dans $\mathbb{Z}/3\mathbb{Z}$, retrouver la règle de divisibilité par 3 (i.e. un nombre est divisible par 3 si la somme de ses chiffres est divisible par 2).

De même pour la divisibilité par 9.

Exercice 4 (***)**.** Déterminer le sous-groupe de $\mathbb{Z}$ engendré, pour l'opération $+$, par :

(i) $\{3, 5\}$

(ii) $\{6, 10\}$

Exercice 5 (***)**.** Soit G le sous-groupe de $(\mathbb{C}^*, \times)$ engendré par $\{i, j\}$ où j est une racine cubique de l'unité distincte de 1.

(i) Montrer que G est le sous-groupe engendré par ij.

(ii) Quel est l'ordre de G ?

Exercice 6 (***)**.** On considère $\mathbb{U}_n$ le groupe des racines n-èmes de l'unité de $\mathbb{C}$, c'est-à-dire :

$$\mathbb{U}_n = \{z \in \mathbb{C} \,;\, z^n = 1\}$$

Par ailleurs, on considèrera dans la suite l'application :

$$f : \begin{array}{ccc} \mathbb{U}_n & \to & \mathbb{C}^* \\ z & \mapsto & z^3 \end{array}$$

Montrer que :

(i) $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$

(ii) Résoudre l'équation dans $\mathbb{C}$ pour en déduire les éléments de $\mathbb{U}_n$.

(iii) Montrer que f est un morphisme de groupes

(iv) Calculer son noyau et son image

(v) En déduire que $\mathbb{U}_3$ est un sous-groupe de $\mathbb{U}_{15}$

(vi) Puis, plus difficile, que $\mathbb{U}_{15}/\mathbb{U}_3$ est isomorphe à $\mathbb{U}_5$

Exercice 7 ($\mathfrak{E}$). Soient H et K deux sous-groupes de G. Démontrez l'équivalence :

$$H \cup K \text{ sous-groupe de } G \;\Leftrightarrow\; H \subseteq K \text{ ou } K \subseteq H$$

Indication : par l'absurde ...

Exercice 8 ($\mathfrak{E}$). Montrer que si n et m sont premiers entre eux :

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$$

i.e. qu'il existe un morphisme bijectif (isomorphisme) entre ces deux groupes.

Indication : on considèrera

$$\begin{array}{rccc} f : & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & \dot{x}^{[nm]} & \mapsto & (\dot{x}^{[n]}, \dot{x}^{[m]}) \end{array}$$

Exercice 9 ($\mathfrak{E}$). Soient $\mathbb{R}[X]$ et $\mathbb{R}_n[X]$ l'ensemble des polynômes à coefficients réels et celui des polynômes de degré au plus n.

(i) Montrer que $\mathbb{R}[X]$ est un groupe pour l'addition.

(ii) Montrer que $\mathbb{R}_n[X]$ en est un sous-groupe.

(iii) Quel est le sous-groupe engendré dans $\mathbb{R}[X]$ par $X^2 + 2X + 1$?

(iv) Arrivez-vous à déterminer celui engendré par $\{X^2 + 2X + 1, X^2 - 1\}$?

Exercice 10 ($\mathfrak{Ch}$). Dans cet exercice, on va utiliser et étudier certaines propriétés des groupes pour décrire un protocole de cryptage asymétrique (à clé publique / clé privée) appelé ElGamal.

Pour cela, nous aurons besoin des deux résultats suivants (admis) :

Rappel - théorème de Bezout *Soient $a, b \in \mathbb{N}$, a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{N}$ tels que $1 = au + bv$.*

Ordre d'un élément - ordre d'un groupe *Lorsqu'un groupe est fini, différentes propriétés apparaissent. Commençons par une définition :*

- *On appelle ordre d'un groupe fini $(G, \star)$ son nombre d'éléments.*
- *Par ailleurs, pour tout $x \in G$, on peut montrer qu'il existre une puissance $k \in N$ telle que $x^{(k)} = e$. Soit k le plus petit entier non nul vérifiant cette propriété, on dit que k est l'ordre de l'élément x. On a alors :*

$$\mathrm{Gr}(\{x\}) = \{e, x, x^2, \ldots, x^{k-1}\} \text{ avec } x^k = e$$

On peut alors prouver une proposition important :

Dans un groupe fini $(G, \star)$ l'ordre de tout élément divise l'ordre du groupe.

(i) Montrer que pour $n \in \mathbb{N}^*$ donné, les éléments inversibles pour $\otimes$ dans $\mathbb{Z}/n\mathbb{Z}$ sont les $\dot{k}$ tels que $\mathrm{pgcd}(n, k) = 1$.

(ii) En déduire que si p est premier, alors $(\mathbb{Z}/p\mathbb{Z}\backslash\{\dot{0}\}, \times)$ est une groupe. On notera $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z}\backslash\{\dot{0}\}$. Son ordre est $p-1$.

(iii) A titre d'exemple, on considère $p = 11$. Déterminez quels sont les ordres des éléments de $\mathbb{Z}/11\mathbb{Z}^*$ (attention, d'après ce qui précède, quels sont les ordres possibles pour les éléments ? et donc avez-vous besoin de tester toutes les puissances $x^{(k)}$ pour trouver l'ordre de x ?). Y a-t-il un/des générateur(s), un/des élément(s) d'ordre strictement inférieur à $p-1$?

(iv) Soit g un générateur de $\mathbb{Z}/11\mathbb{Z}^*$. Montrez que :

$$\forall \dot{x} \in \mathbb{Z}/11\mathbb{Z}^*, \exists k \in \{0, \dots 10\} \quad \dot{x} = g^k \text{ on appelle logarithme discret de } x \text{ cet indice } k.$$

(v) Choisissez un générateur g et calculez les logarithmes discrets des éléments de $\mathbb{Z}/11\mathbb{Z}^*$.

(vi) Le calcul du logarithme discret est réputé complexe (donc sûr d'un point de vue cryptographique) car on ne peut pas faire grand chose d'autre que d'énumérer toutes les puissance de g, ce qui est long ... On l'utilise pour définir l'algorithme de cryptage suivant (appelé ElGamal) :

Soit g un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ et soit $x \in \{1 \dots p-1\}$ (dans un “vrai cas”, on choisira p un grand nombre premier, pas seulement 11 ...).
- La clé secrète est x.
- La clé publique corresondante est $(g, h = g^x)$.
- Un message M est un élément un élément de $\mathbb{Z}/p\mathbb{Z}^*$.
- Encodage (utilise la clé publique exclusivement) :
  - Soit $y \in \{1 \dots p-1\}$ un élément tiré aléatoirement.
  - Le message codé correspondant est (c_1, c_2) où $c_1 = g^y$ et $c_2 = M.h^y$.
- Décodage (nécessite la clé secrète) :
  - Etant donné un message (c_1, c_2) reçu
  - Soit $s = c_1^x$, le message décodé est $m = c_2 \times s^{-1}$

(a) Prouvez que le décodage marche bien.

(b) Quel est la faiblesse de cet algorithme, réputé sûr, en terme de complexité en espace ?

(Bonus) A titre d'exemple, on va utiliser notre “prototype” de $\mathbb{Z}/11\mathbb{Z}^*$. Pour cela, il faut en amont coder l'alphabet dans $\mathbb{Z}/11\mathbb{Z}^*$ (qui contient 10 éléments ...). On va donc utiliser un codage très simple :
- un texte est une suite de caractères qui peut être vue comme une suite de bits 0/1 grâce à la table ASCII
- on les regroupe 3 bits par 3 bits (c'est le mieux que l'on puisse faire car $2^3 = 8$ est la plus grand puissance de 2 “entrant" dans les 10 éléments dont nous disposons).
- On envoie alors chaque entier i codé sur 3 bits ainsi créé sur $\dot{\overline{i+1}} \in \mathbb{Z}/11\mathbb{Z}^*$.

Ainsi par exemple : ABC correspond, via la table ASCII à “1000001.1000010.1000011”. Cette suite de bits est alors découpée 3 bits par 3 bits :

100	000	110	000	101	000	011

Qui correspondent donc à la suite d'entiers :

4	0	6	0	5	0	3

Puis à la suite d'éléments de $\mathbb{Z}/11\mathbb{Z}^*$ à coder :

$\dot{5}$	$\dot{1}$	$\dot{7}$	$\dot{1}$	$\dot{6}$	$\dot{1}$	$\dot{4}$

Vous utiliserez le générateur que vous aviez trouvé à la question 5 et choisirez une clé secrète.

i. Quelle est la clé publique correspondante ?

ii. Quel est le message codé correspondant à la chaîne “MRS" (vous devriez avoir 14 éléments de $\mathbb{Z}/11\mathbb{Z}^*$) ?

Exercice 11 (***)**.** On s'intéresse ici à $\mathbb{Z}/16\mathbb{Z}$ pour l'opération de multiplication.

(i) Montrer que le groupe $(\mathbb{Z}/16\mathbb{Z}, +)$ admet plusieurs générateurs (ie. plusieurs éléments a tels que $\mathrm{Gr}\{a\} = \mathbb{Z}/16\mathbb{Z}$.

(ii) Dans la suite de l'exercice, on s'intéressera à l'opération de **multiplication**

  (a) Montrer que pour la **multiplication**, il existe des éléments de $\mathbb{Z}/16\mathbb{Z}$ non symétrisables. Donner des exemples.

  (b) Si $\mathrm{pgcd}(a, b) = 1$ le théorème de Bezout implique qu'il existe u, v tels que $1 = au + bv$. Ces entiers sont calculés par algorithme d'Euclide étendu.

    i. Rappeler cet algorithme et l'appliquer à 16 et 3.

    ii. En déduire que si $\mathrm{pgcd}(a, 16) = 1$ alors a est symétrisable pour $\times$ et expliquer comment calculer son symétrique $\tilde{a}$.

    iii. En déduire qu'il existe 8 éléments symétrisables pour $\times$ (on notera $(\mathbb{Z}/16\mathbb{Z})^*$ ces éléments symétrisables). $\left((\mathbb{Z}/16\mathbb{Z})^*, \times\right)$ est-il un groupe (vous calculerez les symétriques des éléments en utilisant 2(b)ii) ?

(Bonus) $(\mathbb{Z}/16\mathbb{Z})^*$ a-t-il des générateurs pour $\times$? En déduire que $(\mathbb{Z}/16\mathbb{Z})^*$ n'est pas isomorphe à $Z/8Z$.