

TD 3 – Groupes, anneaux, corps

Exercice 1.

Appliquer la définition : groupes

1. Montrer que $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont des groupes additifs.
2. Montrer que (\mathbb{R}^*, \times) et (\mathbb{Q}^*, \times) sont des groupes multiplicatifs.
3. Montrer que $(\mathbb{N}, +)$, (\mathbb{Z}, \times) et (\mathbb{R}, \times) ne sont pas des groupes.
4. Montrer que les couples suivants sont des groupes, et préciser s'ils sont abéliens :
 - i. $(n\mathbb{Z}, +)$ où $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$;
 - ii. $(\{-1, 1\}, \times)$;
 - iii. $(\{0, 1\}^n, \otimes)$ (ensemble des mots binaires de longueur n fixée, avec l'opération « ou exclusif bit-à-bit ») ;
 - iv. (S_n, \circ) (ensemble des permutations de $\{1, \dots, n\}$ avec l'opération de composition).
5. Le couple $(\{0, 1\}^*, \cdot)$ de l'ensemble des mots binaires avec l'opération de concaténation est-il un groupe ?

Exercice 2.

Appliquer la définition : anneaux et corps

1. Montrer que $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$ et $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont des anneaux.
2. Montrer que $(\mathbb{R}, +, \times)$ et $(\mathbb{Q}, +, \times)$ sont des corps, mais pas $(\mathbb{Z}, +, \times)$.
3. Montrer que $(n\mathbb{Z}, +, \times)$ n'est pas un anneau.
4. Montrer que $((\mathbb{Z}/n\mathbb{Z})^\times, +, \times)$ n'est pas un anneau.

Exercice 3.

Indicatrice d'Euler

1. Rappeler comment on calcule $\varphi(n)$ à partir de la décomposition de n en facteurs premiers.
2. Calculer $\varphi(7)$, $\varphi(8)$ et $\varphi(21)$.
3.
 - i. Soit $k = \varphi(n)$. Montrer que les facteurs premiers de n sont $\leq k + 1$.
 - ii. Soit $k = \varphi(n)$. Montrer que les exposants de la décomposition en facteurs premiers de n sont tous $\leq \log k$.
 - iii. En déduire que $\{n : \varphi(n) = k\}$ est fini.
 - iv. En déduire que $\lim_{+\infty} \varphi(n) = +\infty$.

Exercice 4.*Les maths de RSA*

Dans cet exercice on présente quelques résultats mathématiques sur lesquels le cryptosystème RSA est basé. *Attention, ce qu'on décrit n'est pas le cryptosystème RSA.*

Soit $n = p \times q$ où p et q sont deux nombres premiers. On définit deux clefs e et d de la manière suivante : e est un entier $< \varphi(n)$, premier avec $\varphi(n)$; d est l'inverse modulo $\varphi(n)$ de e , c'est-à-dire que $de \equiv_{\varphi(n)} 1$. Étant donné un entier m entre 1 et $n - 1$, son chiffré est $c = m^e \pmod n$.

L'objectif de l'exercice est d'une part de montrer qu'étant donné c et la clef d , il est possible de retrouver m , et d'autre part de déterminer les algorithmes nécessaires pour produire les clefs e et d et pour effectuer les calculs de c à partir de m , et de m à partir de c .

1.
 - i. Combien vaut $\varphi(n)$?
 - ii. Étant donné e , comment peut-on calculer d ?
 - iii. Étant donné m et e , comment calculer c ? *Vu dans un autre cours !*
 - iv. Si on connaît la factorisation $n = pq$, il est facile de calculer $\varphi(n)$. Montrer l'inverse : si on connaît $\varphi(n)$, et qu'on sait que n est un produit de deux nombres premiers, alors on peut retrouver p et q . *Indication. On peut calculer les coefficients du polynôme $(X - p)(X - q)$ en connaissant n et $\varphi(n)$.*
2.
 - i. Soit $a \in \{1, \dots, n\}$ tel que $\text{PGCD}(a, n) = 1$. Montrer que $a^{\varphi(n)} \equiv_n 1$ où φ est l'indicatrice d'Euler. *Indication : traduire cette question dans le langage de $(\mathbb{Z}/n\mathbb{Z})^\times$.*
 - ii. Soit $a \in \{1, \dots, n\}$ tel que $\text{PGCD}(a, n) \neq 1$. Montrer que a est multiple de p , ou de q .
 - iii. On suppose que $\text{PGCD}(a, n)$ est un multiple de p . Montrer que $a^{\varphi(n)} \equiv_p 1$.
 - iv. En déduire que $a^{\varphi(n)} \equiv_n 1$. *Utiliser le théorème chinois.*
3. Soit m un entier entre 1 et $n - 1$, et $c = m^e \pmod n$. Si on connaît c , d et n , montrer qu'on peut calculer m .