Corrigé devoir

Exercice 1 (Preuve élémentaire du petit théorème de Fermat (exo 15 feuille 1))

1. Montrer que pour tout couple d'entiers a et b et tout p premier, on a :

$$(a+b)^p \equiv a^p + b^p \pmod p.$$

Soient $a, b \in \mathbb{Z}$ alors

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p.$$

Pour tout $0 < i < p$, $i!\binom{p}{i} = p!/(p-i)!$ est divisible par p. De plus p est premier avec $i!$ donc par Gauss, $\binom{p}{i}$ est divisble par p. D'où $(a+b)^p \equiv a^p + b^p \pmod p$.

2. En déduire le petit théorème de Fermat :

$$n^p \equiv n \pmod p.$$

Le résultat est évident pour $n = 0$. Supposons que $n^p \equiv n \pmod p$ pour un entier $n \in \mathbb{N}$. Alors par (1.) $(n+1)^p \equiv n^p + 1^p \pmod p$ d'où $(n+1)^p \equiv n+1 \pmod p$. Il suit par récurrence que le résultat est vérifié pour tout $n \in \mathbb{N}$. On en déduit le résultat pour $n \in \mathbb{Z}$ en remarquant que pour tout entier m, $(-m)^p \equiv -m^p \pmod p$.

3. A quelle condition a-t-on $n^{p-1} \equiv 1 \pmod p$?
$n^{p-1} \equiv 1 \pmod p$ *si et seulement si n est premier avec p. En effet par (2.), p divise $n(n^{p-1}-1)$. Ou bien p divise n et $n^{p-1} \equiv 0 \pmod p$ ou bien p est premier avec n et alors p divise $n^{p-1} - 1$, c'est-à-dire $n^{p-1} \equiv 1 \pmod p$.*

Exercice 2 Soit $n \geq 1$. Vérifier que A_n est un sous-groupe normal de S_n.

A_n est un sous-groupe normal de S_n car c'est le noyau d'un morphisme (le morphsime signature). En effet si ϕ est un morphisme de G vers G', considérons $\sigma \in \ker \phi$ et $\tau \in G$. Alors

$$\phi(\tau\sigma\tau^{-1}) = \phi(\tau)\phi(\sigma)\phi(\tau^{-1}) = \phi(\tau)\phi(\tau^{-1}) = 1.$$

D'où $\tau\sigma\tau^{-1} \in \ker \phi$. On a vérifié que le noyau d'un morphisme était normal.

Exercice 3

1. Lister toutes les permutations dans A_4.
A_4 est constitué de l'identité, des produits de deux transpositions à supports disjoints et des 3-cycles, c'est-à-dire

$$A_4 = \{id, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

2. Soit $H = \{\sigma \in A_4 | \sigma^2 = id\}$

(a) Lister les permutations dans H.
Les éléments d'ordre 2 de A_4 sont les produits de deux transpositions à supports disjoints donc

$$H = \{id, (12)(34), (13)(24), (14)(23)\}.$$

(b) Montrer que H est un sous-groupe de A_4.
Remarquons tout d'abord que tout élément de H est son propre inverse. Remarquons de plus que

$$(12)(34)(13)(24) = (14)(23).$$

Il suit (quitte à permuter l'ensemble $\{1, 2, 3, 4\}$) que le produit de deux éléments non triviaux de H est égal au troisième. L'ensemble H est non vide, stable par produit et par passage à l'inverse, c'est donc un sous-groupe de A_4.

(c) Montrer que H est normal dans A_4.
Soit $\sigma \in H$ et $\tau \in A_4$. Alors

$$(\tau\sigma\tau^{-1})^2 = \tau\sigma^2\tau^{-1} = \tau\tau^{-1} = id.$$

Donc $\tau\sigma\tau^{-1} \in H$.

(d) H est-il normal dans S_4 ?
Soit $\sigma \in H$ et $\tau \in S_4$. Alors comme A_4 est normal dans S_4, $\tau\sigma\tau^{-1} \in A_4$. Le même calcul qu'à la question précédente montre que $(\tau\sigma\tau^{-1})^2 = id$. Donc $\tau\sigma\tau^{-1} \in H$.

3. Donner un exemple de sous-groupe propre non trivial K de H.
K est nécessairement le sous-groupe engendré par l'un des éléments non trivial de H. On peut prendre par exemple $K = \langle (12)(34) \rangle$.
   - Le sous-groupe K est-il normal dans H ?
   On a remarqué précédemment que le produit de deux éléments de H non trivial était égal au troisème élément non trivial de H. Donc si on prend $\tau \in \{(13)(24), (14)(23)\}$, il suit que

   $$\tau(12)(34)\tau^{-1} = (\tau(12)(34))\tau = (12)(34).$$

   On en déduit immédiatement que K est normal dans H.
   - Le sous-groupe K est-il normal dans A_4 ?
   K n'est pas normal dans A_4 car

   $$(123)(12)(34)(132) = (14)(23).$$

   Notons que cet exemple montre que la relation être "un sous-groupe normale dans" n'est pas transitive : en effet H est normal dans K, K est normal dans A_4 mais H n'est pas normal dans A_4.