

## 10 Counting the elements of a finite group

May 24, 2015

### 10.5

1.  $G$  tel que  $o(G) = 8$
2.  $G$  n'est pas cyclique

$$\diamond a \in G \Rightarrow a^4 = e$$

Car soit  $a \in G$ . Alors  $o(a) | o(G)$ . Donc  $o(a) \in \{1, 2, 4, 8\}$ . Or  $o(a) \neq 8$ , car alors  $a$  serait un générateur et donc  $G$  serait cyclique.

Donc soit  $o(a) = 1$ , auquel cas il s'agit de l'identité et donc  $a^4 = e^4 = e$ , soit  $o(a) \in \{2, 4\}$ . Or,  $a^4 = e$  dans un cas comme dans l'autre.

### 10.6

1.  $H, K$  des sous-groupes de  $G$  tel que  $|H| = 12$  et  $|K| = 5$

$$\diamond H \cap K = \{e\}$$

Car supposons le contraire. Soit  $a \in H \cap K$ . Alors  $o(a) = o(\langle a \rangle) \neq 1$  divise  $|H|$  et  $|K|$ .

Alors  $\text{pgdc}(12, 5) \neq 1$ , ce qui est absurde.

### 10.7

1.  $p, q$  des nombres premiers et  $G$  un groupe d'ordre  $pq$

**$\diamond$  Tout sous-groupe de  $G$  est cyclique.**

Car soit  $H$  un sous-groupe de  $G$ . Alors  $o(H) | o(G)$  ie.  $o(H) | pq$ . On les cas où  $o(H)$  est 1,  $p$  ou  $q$ .

Si  $o(H) = 1$ ,  $H$  est trivialement cyclique. Sinon, spd,  $o(H) = q$ . Alors soit  $a \in H - \{e\}$ . Alors l'ordre de  $a$  doit diviser l'ordre de  $H$  et n'est pas 1. Alors il doit être  $q$ . Mais alors il s'agit d'un générateur.

## 10.8

1.  $p$  premier et  $G$  un groupe d'ordre  $p^2$

◇ Il existe  $H$  un sous group de  $G$  d'ordre  $p$

Soit  $a \in G - \{e\}$ . Alors  $o(a) | p^2$ . Si  $o(a) | p$ , on a finit. Sinon,  $o(a) = p^2$  et donc  $G$  est cyclique. Soit alors  $b = a^p$ . Alors  $b \neq e$ . Aussi,  $b^p = (a^p)^p = a^{p^2} = e$ .

Or, il doit bien s'agir de l'ordre de  $b$ , car sinon l'ordre de  $a$  serait différent. Donc  $\langle b \rangle$  est un sous-groupe d'ordre  $p$ .

## 10.9

1.  $H, K$  des sous groupes de  $G$  tel que  $|H| = 39$  et  $|K| = 65$

◇  $H \cap K$  est cyclique

**TODO Faire avec des cosets**

Si  $|H \cap K| = 1$ , la chose est triviale. Soit alors  $|H \cap K| \neq 1$ . Alors il existe  $a \in H \cap K$  tel que  $a$  divise 39 et 65. Or 13 est le seul diviseur commun de ces nombres. Donc  $o(a) = 13 \forall a \in H \cap K$ .

On a alors que  $H \cap K$  est d'ordre 26 ou 39.

Supposons l'ordre 26. Alors  $\langle a \rangle$  est un sous-groupe de  $H \cap K$  d'ordre 13 et il existe  $b \in H \cap K$  tel que  $b \notin \langle a \rangle$ . Alors  $\langle b \rangle \cap \langle a \rangle = \{e\}$ , car tous leurs éléments sont des générateurs (tous d'ordre 13).

Mais alors il existe  $c \notin \langle a \rangle$ ,  $c \notin \langle b \rangle$  car  $\langle a \rangle$ ,  $\langle b \rangle$  ont un élément en commun, notamment  $e$ , et donc représentent 25 des 26 éléments de  $H \cap K$ . Or  $c$  est d'ordre 13 et donc  $\langle c \rangle$  est également un sous-groupe contenant 13 éléments distincts de ceux se trouvant dans  $\langle a \rangle$  et  $\langle b \rangle$ . Alors la cardinalité de  $H \cap K$  est d'au moins 38, ce qui est absurde.

L'argument est le même dans le cas où la cardinalité serait 39. Donc la cardinalité est 13 et il s'agit d'un groupe cyclique.

## 10.10

◇ **Donnez une autre preuve du théorème de Lagrange.**