Semaine 7
Exercices

Amar AHMANE

30 janvier 2022

Je m'en allais, les poings dans mes poches crevées ;
Mon paletot aussi devenait idéal ;
J'allais sous le ciel, Muse ! et j'étais ton féal ;
Oh ! là ! là ! que d'amours splendides j'ai rêvées !

Ma bohème, Arthur Rimbaud

Les rappels :

Définition 1 Lorsque G est un groupe fini, on appelle ordre de G son cardinal.

Définition 2 Soit G un groupe multiplicatif. Soit $g \in G$, alors on définit

$$\text{ord}(g) = \min\{n \in \mathbb{N}^* \mid g^n = 1\}$$

Par convention, cette quantité est $+\infty$ si l'ensemble considéré ci-dessus est vide.

Définition 3 Soit $n \in \mathbb{N}^*$. On note $\mathbb{P}$ l'ensemble des nombres premiers. Cet entier admet une décomposition nombres premiers (résultat admis) que l'on choisit de noter de la sorte :

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

où $v_p(n)$ est l'exposant de p dans la décomposition en nombre premiers de n. Dans ce cas, le pgcd de deux entiers m et n non nuls est l'entier

$$n \wedge m = \prod_{p \in \mathbb{P}} p^{\min(v_p(n), v_p(m))}$$

Définition 4 On dit que deux entiers sont premiers entre eux si leur pgcd est égal à 1.

Quelques résultats utiles :

— Théorème de Lagrange : l'ordre de chaque sous-groupe d'un groupe G divise l'ordre de G.

— Lemme de Gauss : lorsque p et q sont deux entiers premiers entre eux, et lorsque $p|mq$ où m est un entier, on a que $p|m$.

Exercice : ordre du produit de deux éléments dont les ordres sont premiers entre eux (source : Oraux X-ENS, Algèbre 1, Cassini)

Évidemment, l'ordre de y^m est n, et l'ordre de x^m est n. Or, on a $y^m \in < xy >$ et $x^n \in < xy >$ donc, d'après Lagrange, $O(x^n) = O(x)|O(xy)$ et $O(y^m) = O(y)|O(xy)$, mais il est aussi clair que $(xy)^{mn} = 1$ donc $O(xy)|O(x)O(y)$ et $O(x)O(y)|O(xy)$; or, tous les entiers avec lesquels ont travaille ici sont dans $\mathbb{N}$, mais $|$ est une relation d'ordre sur $\mathbb{N}$, donc par antisymétrie $O(xy) = O(x)O(y) = mn$.

Exercice : quelques exemples de sous-groupes (source : Les maths en tête, Xavier Gourdon)

Soit G un groupe, H_1 et H_2 deux sous-groupes de G.

1. On suppose que $H_1 \cup H_2$ est un sous-groupe de G et on suppose par l'absurde que que $H_1 \not\subset H_2$ et $H_2 \not\subset H_1$. Il existe alors $h_1 \in H_1$ tel que $h_1 \notin H_2$ et $h_2 \in H_2$ tel que $h_2 \notin H_2$. Alors $h_1h_2 \in H_1 \cup H_2$ puisque $H_1 \cup H_2$ est un sous-groupe : si $h_1h2 \in H_1$, alors $h_2 = h_1^{-1}(h_1h_2) \in H_1$ ce qui est absurde, sinon on a que $h_1h_2 \in H_2$ et $h_1 = (h_1h_2)h_2^{-1} \in H_2$ ce qui est aussi absurde.
2. $H_1 \cap H_2$ est un sous-groupe de H_1, donc son ordre divise celui de H_1, de même, c'est un sous-groupe de H_2 donc son ordre divise celui de H_2. Ainsi, l'ordre de $H_1 \cap H_2$ est un diviseur commun de l'ordre de H_1 et celui de H_2, donc l'ordre de $H_1 \cap H_2$ est fatalement 1, donc $H_1 \cap H_2 = \{1_G\}$.

Exercice : cardinal d'un groupe fini et Im et Ker. (source : Oraux X-ENS, Algèbre 1, Cassini)

Soit G un groupe fini, et f un morphisme de G dans lui-même.

1. C'est du cours.
2. Il y a autant de classes d'équivalences que d'images par le morphisme f.
3. Vérifications faciles, le neutre est évidemment $\bar{1}$.
4. Découle directement de l'équivalence $f(x) = f(y) \Leftrightarrow x^{-1}y \in \mathrm{Ker} f$.
5. Conséquence de ce que PG a du démontrer la semaine dernière : les classes d'équivalences sont deux à deux disjontes et de même cardinal et leur union disjointe est égale à G, il suffit alors de passer au cardinal.
6. C'était la question la plus difficile de la semaine : il fallait se convaincre que $(\mathrm{Ker} f = \mathrm{Ker} f^2 \Leftrightarrow \operatorname{Im} f = \operatorname{Im} f^2) \Leftrightarrow (|\mathrm{Ker} f| = |\mathrm{Ker} f^2| \Leftrightarrow |\operatorname{Im} f| = |\operatorname{Im} f^2|)$; en effet, si $x \in \mathrm{Ker} f$, on a $f \circ f(x) = f(e) = e$ donc $x \in \mathrm{Ker} f^2$ donc $\mathrm{Ker} f \subset \mathrm{Ker} f^2$, d'autre part si $y \in \operatorname{Im} f^2$, alors il existe $x \in G$ tel que $y = f \circ f(x) \in \operatorname{Im} f$ donc $\operatorname{Im} f^2 \subset \operatorname{Im} f$. Comme tous ces ensembles sont finis, il est clair que $\operatorname{Im} f = \operatorname{Im} f^2 \Leftrightarrow |\operatorname{Im} f| = |\operatorname{Im} f^2|$, et de même $\mathrm{Ker} f = \mathrm{Ker} f^2 \Leftrightarrow |\mathrm{Ker} f| = |\mathrm{Ker} f^2|$. L'exercice devient très simple puisque l'on sait que $|G| = |\mathrm{Ker} f| \times |\operatorname{Im} f|$, et comme f^2 est aussi un homomorphisme, $|G| = |\mathrm{Ker} f^2| \times |\operatorname{Im} f^2|$, je vous laisse conclure...