Semaine 6

Pomme Bleue

24 janvier 2022

Pierre-Gabriel Berlureau

Congruences modulo un sous-groupe et Théorème de Lagrange

On a

i) L'application $f : h \in H \mapsto xh$ est une bijection. En effet, il est clair que $\mathrm{Ker} f = \{e\}$, donc f est injective ; la surjectivité est claire, d'où que f est bijective, donc $|H| = |xH|$.

ii) On montre que la relation $\mathcal{R}$ définie par

$$x\mathcal{R}y \Leftrightarrow y \in xH$$

est une relation d'équivalence et que la classe d'équivalence de $x \in H$ est xH.

$G/\mathcal{R}$ est une partition de G de parts toutes égales, donc on a

$$G = \bigcup_{H \in G/\mathcal{R}} H$$

d'où que, en passant au cardinal, $G = \sum_{H \in G/\mathcal{R}} |H| = |G/\mathcal{R}| \times |H|$.

Matteo Delfour

Morphismes de $\mathbb{Q}$ dans $\mathbb{Z}$

Analyse Soit $f \in \mathrm{Hom}(\mathbb{Q}, \mathbb{Z})$, alors $f(\mathbb{Z})$ est un sous-groupe de $(\mathbb{Z}, +)$, ainsi il existe $n \in \mathbb{N}$ tel que $f(\mathbb{Z}) = n\mathbb{Z}$. Il en découle qu'il existe $x \in Q$ tel que $f(x) = n$, d'où que $2f(\frac{x}{2}) = n$ donc $f(\frac{x}{2}) = \frac{n}{2}$ donc $\frac{n}{2} \in n\mathbb{Z}$, ceci n'est possible que si $n = 0$, donc f est la fonction nulle.

Syntèse Bla bla...

Yanis Grigy

Petit Lemme

Méthode 1 : la récurrence bizarre.

On que tout élément de G est égal à son inverse, donc, lorsque $x, y \in G$, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

On montre à présent par récurrence sur $|G|$ que $|G|$ est une puissance de 2.

Lorsque $|G| = 1$, il n'y a rien à vérifier. Lorsque $|G| \geq 2$, on note H le sous-groupe de G maximal pour l'inclusion tel que $G \neq H$. Soit $a \in G \backslash H$, alors $H \cup aH$ est un groupe, mais $H \cap aH = \emptyset$. D'autre part $|H \cup aH| = 2|H|$ d'après la propriété de Pierre-Gabriel, ainsi $H \cup aH$ est un sous-groupe de G ayant un cardinal strictement plus grand que celui de H, donc $H \cup aH = G$, d'où que $|G| = 2|H|$. D'après notre hypothèse de récurrence, $|G|$ est une puissance de 2 puisque $|H|$ est une puissance de 2.

Méthode 2 : la méthode élégante qui utilise de l'algèbre linéaire.

On remarque que G est un $\mathbb{Z}/2\mathbb{Z}$-ev lorsque que l'on définit la loi de composition externe $\cdot$ telle que $0 \cdot x = 1_G$ et $1 \cdot x = x$; on laissera le soin au lecteur de vérifier les axiomes. On a directement, avec $\dim G$ fini,

$$G \simeq (\mathbb{Z}/2\mathbb{Z})^{\dim G}$$

Ce qui conclut.

Louis Marchal

Groupes dont l'ensemble des sous-groupes est fini

Soit G un groupe. On note E l'ensemble de ses sous-groupes, on suppose qu'il est fini.

Les éléments de G sont tous d'ordre fini : en effet, si $g \in G$ est tel que $\text{ord}(g) = +\infty$, alors on a que $< g > \simeq \mathbb{Z}$ donc $< g >$ a une infinité de sous-groupes, ce qui ne peut arriver puisque E est fini. On note E' l'ensemble des sous-groupes monogènes de G, alors $\bigcup_{H \in E'} H = G$. Ainsi, G est fini puisqu'il est une union finie de groupes finis.

Remarques : $< g >$ désigne le plus petit sous-groupe de G contenant g, qui est égal à $g\mathbb{Z}$ lorsque la loi de G est notée additivement; on appelle le plus petit sous-groupe de G contenant une partie X de G, et on note $\text{Gr}(X)$, l'intersection de tous les sous-groupes de G contenant X : $\text{Gr}(X)$ est le sous-groupe monogène engendré par X. Un sous-groupe est dit homogène s'il est un sous-groupe homogène de lui-même.

Louis Thevenet

Cas particulier du Lemme de Cauchy

D'après le théorème de Lagrange, les éléments de G sont soit d'ordre 1, 2, p ou $2p$. On suppose par l'absurde qu'il n'existe pas d'éléments d'ordre p : il en découle assez rapidement qu'il n'existe pas non plus d'éléments d'ordre $2p$ (en effet, si $x \in G$ est d'ordre $2p$, x^2 est d'ordre p). On en déduit que tous les éléments sont d'ordre soit 1 ou 2 et $p \geq 3$, d'où

$$\forall g \in G,\ g^2 = 1_G$$

D'après le Lemme de Yanis, G est une puissance de 2. Or, $|G| = 2p$, qui n'est pas une puissance de 2. Voilà l'absurdité.

Armand sans nom de famille

Existence d'un idempotent

Soit $a \in G$, l'application $f : n \in \mathbb{N} \mapsto a^{2^n}$ ne saurait être injective, puisque E est fini; ainsi, il en découle qu'il existe $p, q \in \mathbb{N}$ deux entiers différents tels que $a^{2^p} = a^{2^q}$, ce qui peut être réécrit : $a^{2^{m+n}} = a^{2^m}$. On pose $b = a^{2^m}$, on a alors $b^{2^n} = b$, ainsi b^{2^n-1} est idempotent : en effet, $(b^{2^n-1})^2 = b^{2^n+2^n-2} = bb^{2^n-2} = b^{2^n-1}$.

Shems

Neutre à droite et inverse à droite

On montre que tout élément est inversible : soit $g \in G$, alors g admet un inverse à droite g' qui admet un inverse à droite g'' : ainsi, $gg'g'' = eg''$ donc $g'gg'g'' = g'eg''$ donc $g'ge = g'g''$ donc $g'g = e$ donc g' est inversible à gauche et e est un neutre à gauche ce qui conclut.