S. Lang Algèbre p35 108.2
F. Ulmer Théorie des groupes p 69 108.3 108.4

Lemme de Cauchy

Soit G un groupe fini d'ordre n.
Le lemme de Cauchy assure l'existence d'élément de G d'ordre p, pour tout nombre premier p divisant n. Dans les cas où G est cyclique ou abélien le résultat est évidemment vrai, mais surtout plus facile à démontrer, c'est pourquoi on commence par énoncer ces propriétés plus faibles.

108.1 **Pté** Si G est cyclique d'ordre n,
alors pour tout d divisant n, il existe $g \in G$ d'ordre d

Preuve Soit g un générateur de G. g est donc d'ordre n.
Soit d un diviseur de n. On pose $g' = g^{n/d}$.
On a $(g')^d = g^{n/d \times d} = g^n = 1$ donc $o(g') \mid d$.
De plus pour $i \in [1..d-1]$ $(g')^i = g^{n/d \times i} \neq 1_G$ car $\frac{n}{d} \times i < n = o(g)$.
Donc $o(g') = d$.

Rq Cela montre aussi que si G est cyclique, pour tout $d \mid n$, il existe un sous-groupe de G d'ordre d. On peut de plus montrer qu'il est unique.

108.2 **Pté** Si G est abélien fini d'ordre n,
alors pour p premier divisant n, il existe $g \in G$ d'ordre p

Preuve 1) MQ SI t EST UN EXPOSANT DE G, IL EXISTE k TQ $|G| \mid t^k$
On rappelle qu'un exposant de G est un entier t tel que tous les éléments de G élevés à la puissance t valent 1_G.
On montre ce résultat par récurrence sur l'ordre de G
→ Si $|G| = 1$, alors pour tout t (exposant de G) $1 = |G| \mid t = t^1$.
→ Si $|G| > 1$ et si la propriété est vérifiée pour tout groupe d'ordre plus petit.

On suppose que t est un exposant de G.
Puisque $|G| \neq 1$, il existe $b \in G \setminus \{1\}$. On considère $H = \langle b \rangle$.
Puisque G est abélien on a automatiquement $H \trianglelefteq G$ et alors G/H est un groupe d'ordre plus petit (car $H \neq \{1_G\}$) et qui a aussi pour exposant t puisque $\forall \bar{g} \in G/H \quad \bar{g}^t = \overline{g^t} = \overline{1_G} = 1_{G/H}$. Donc par hypothèse de rec. il existe $k \in \mathbb{N}^*$ tel que $|G/H| \mid t^k$.
De plus comme $b \in G$, $b^t = 1_G$ donc $o(b) \mid t$, c-à-d $|H| \mid t$.
Donc $|G| = |H| \times |G/H| \mid t^k \times t = t^{k+1}$. D'où la propriété au rg $|G|$.

2) EN DÉDUIRE LE RÉSULTAT

Soit p un diviseur premier de $n = |G|$.
Puisque G est fini on a facilement un exposant en prenant $t = \text{PPCM}\{o(g) \mid g \in G\}$
Il existe donc $k \in \mathbb{N}^*$ tel que $n \mid t^k$, donc $p \mid t^k$.
Comme p est premier cela implique nécessairement qu'il existe $g \in G$ tel que $p \mid o(g)$, disons $o(g) = p \times s$. On considère alors $g' = g^s$.
$g'^p = (g^s)^p = g^{sp} = g^{o(g)} = 1_G$ donc $o(g') \mid p$ et $\forall i \in [1 \dots p-1] \quad g'^i = g^{si} \neq 1_G$ car $si < sp = o(g)$.
Donc g' est d'ordre exactement p.

Démontrons maintenant ce lemme utile pour le lemme de Cauchy.

108.3 **lemme** Si H est un groupe fini d'ordre p^m avec p premier et $m \in \mathbb{N}^*$, agissant sur X un ensemble fini
alors $\#\text{Fix}(H) \equiv \#X \ [p]$ où $\text{Fix}(H) = \{x \in X \mid \forall h \in H \ h.x = x\}$.

Preuve. Considérons $(x_i)_{i \in [1..n]}$ un système de représentants de X sous l'action de H. Comme les orbites sous l'action de H forment une partition on a $\#X = \sum_{i=1}^{n} \#\Omega_H(x_i) = \sum_{i=1}^{n} [H : \text{Stab}_H(x_i)]$
(car on rappelle que $\left(H/\text{Stab}_H(x) \to \Omega_H(x) \right.$ est une bijection$)$
$\left. \bar{h} \longmapsto h.x \right)$

$x \in \text{Fix}(H) \Leftrightarrow \forall h \in H, \ h.x = x \Leftrightarrow \Omega_H(x) = \{x\} \Leftrightarrow |\Omega_H(x)| = 1$.
Les orbites de cardinal 1 sont exactement celles des points H-fixes.

Sinon, $|Stab_H(x)|$ est un diviseur strict de $|H| = p^m$. c-à-d qu'il existe $\beta < m$ tel que $|Stab_H(x)| = p$ et alors $|\Omega_H(x)| = [H : Stab_H(x)] = p^{m-\beta}$ est divisible par p car $m-\beta > 0$.

Finalement $\#X = \sum_{\substack{i=1 \\ x_i \in Fix(H)}}^{n} \underbrace{|\Omega_H(x_i)|}_{=1} + \sum_{\substack{i=1 \\ x_i \notin Fix(H)}}^{\hat{n}} \underbrace{|\Omega_H(x)|}_{\text{divisible par } p} \equiv \#Fix(H) + 0 \ [p]$.

108.4 **Lemme de Cauchy.** [Si G est fini d'ordre n alors pour p diviseur premier de n, il existe $g \in G$ d'ordre p.]

Preuve Pour appliquer le lemme ci-dessus, on cherche une action d'un groupe d'ordre une puissance de p dont les points fixes sont en bijection avec les élém^t d'ordre p de G.

Précisément l'idée ici est de faire agir $\mathbb{Z}/p\mathbb{Z}$, un gpe cyclique d'ordre p, sur $X = \{(x_i)_{i\in[1..p]} \in G^p \mid \prod_{i=1}^{p} x_i = 1_G\} \subset G^p$.

On sait déjà que $\mathfrak{S}_p$ agit sur G^p par $\sigma . (x_i)_{i\in[1..p]} = (x_{\sigma(i)})_{i\in[1..p]}$.

En particulier $c = (1, 2, \dots p) \in \mathfrak{S}_p$ agit sur G^p, de plus si $(x_i)_{i\in[1..p]} \in X$, alors $\prod_{i=1}^{p} x_{c(i)} = x_2 x_3 \cdots x_p x_1 = x_1^{-1} \underbrace{x_1 x_2 \cdots x_p}_{=1_G} x_1 = x_1^{-1} x_1 = 1_G$.

donc $c.(x_i) \in X$.

Donc $\langle c \rangle$ agit sur X, et comme c est d'ordre p on a bien un groupe cyclique d'ordre p qui agit sur X.

Soit $(x_i)_{i\in[1..p]} \in X$. $(x_i)_{i\in[1..p]}$ est $\langle c \rangle$-fixe ssi $x_1 = x_2 = \dots = x_p$.

Et comme il est donc x, ——— ssi il existe $x \in G$ tq $\forall i \in [1..p]\ x_i = x$ et $x^p = 1$

On a donc autant de points $\langle c \rangle$ fixes que d'élém^t d'exposant p, et puisque p est premier il y en a un de plus que d'élém^t d'ordre exactem^t p ($x^p = 1 \Leftrightarrow x$ est d'ordre p ou $x = 1$).

Donc le lemme se réécrit $\#$élém^t d'ordre p $+ 1 \equiv \#X \ [p]$.

Or comme étant donné $(x_i)_{i\in[1..p-1]} \in G^{p-1}$ il existe un unique $x_p \in G$ tq $(x_i)_{i\in[1..p]} \in X$ (c'est $(x_1 \cdots x_{p-1})^{-1}$), $\#X = \#(G^{p-1}) = n^{p-1}$. Or $p \mid n$ donc $p \mid \#X$.

D'où finalem^t $\#$élém^t d'ordre $p + 1 \equiv 0 \ [p]$ et donc $\#$élém^t d'ordre $p \neq 0$.

Il existe donc bien un élém^t d'ordre p.