Rappelons où on en était :

G groupe fini d'ordre $n = m p^r$
où p premier et $(m,p) = 1$

Soit

$$X_s = \{ H \subseteq G \mid H \text{ sous-groupe de } G \text{ de cardinal } p^s \}$$

la seule chose qui restait à montrer c'est

$$|X_s| \equiv 1 \mod p \quad , s = 0, \dots, r$$

On considère pour ce faire

$$E_s = \{ A \subseteq G \mid |A| = p^s \}$$

l'ensemble des parties de G de cardinal p^s.
On fait agir G sur E_s en définissant

$$g * A = gA = \{ ga \mid a \in A \}$$

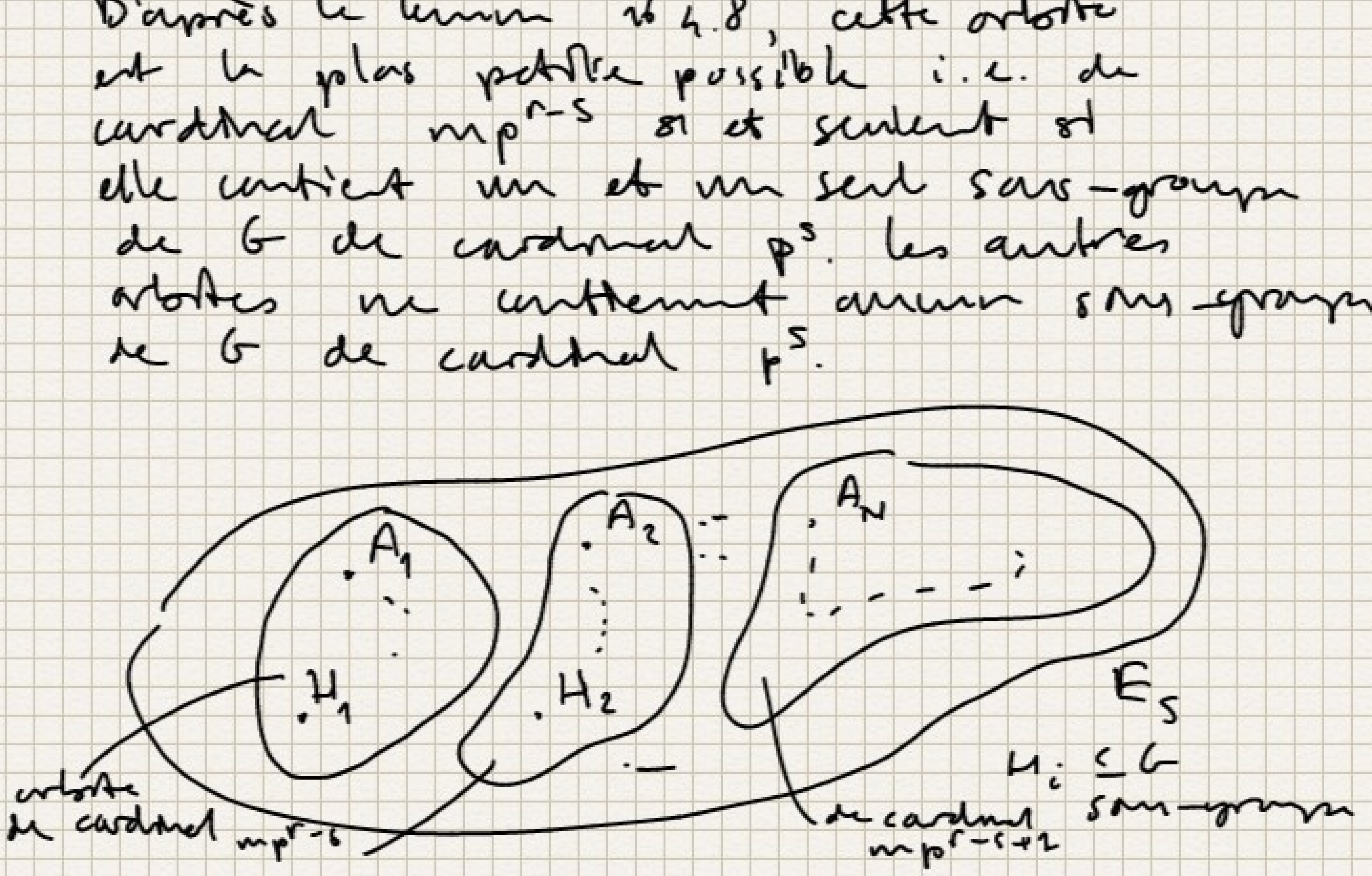
On a $X_s \subseteq E_s$. L'orbite de $A \in E_s$ est notée

$$O(A) = \{ gA \mid g \in G \}.$$

Le lemme 16.4.7 dit que

$$|O(A)| = m p^{r-i}$$

pour un certain $i = 0, \dots, s$
D'après le lemme 16.4.8, cette orbite est la plus petite possible i.e. de cardinal mp^{r-s} si et seulement si elle contient un et un seul sous-groupe de G de cardinal p^s. Les autres orbites ne contiennent aucun sous-groupe de G de cardinal p^s.



On était en train de démontrer :

<u>Lemme</u> 16.4.9

$$\binom{n}{p^s} \equiv |X_s| m p^{r-s} \mod m p^{r-s+1}$$

De plus, $|X_s| \mod p$ ne dépend pas de G mais seulement des entiers n, p, s.

<u>Démo.</u> Soient $A_1, \dots, A_N \in E_s$ des représentants des orbites de E_s :

$$E_s = \dot{\bigcup_{i=1}^{N}} O(A_i)$$

On suppose que

$$|O(A_i)| \begin{cases} = mp^{r-s} & i = 1, \dots, M \\ > mp^{r-s} & i = M+1, \dots, N \end{cases}$$

D'après le lemme 16.4.8 $O(A_i)$ contient un sous-groupe de G de cardinal p^s si et seulement si $i \leq M$, et dans ce cas elle n'en contient qu'un seul. Du coup

$\Rightarrow M = |X_s|$

$$\binom{n}{p^s} = |E_s| = \sum_{i=1}^{N} |O(A_i)| = \sum_{i=1}^{M} |O(A_i)| + \sum_{i=M+1}^{N} |O(A_i)| \equiv$$

$$\equiv \sum_{i=1}^{M} mp^{r-s} + \sum_{i=M+1}^{M} 0 \qquad \mod mp^{r-s} \times p$$

$$\equiv |X_s| \, m p^{r-s} \qquad \mod m p^{r-s+1}$$

Montrons que $|X_s| \mod p$ ne dépend que des entiers n, p, s : Soit G' un autre groupe de cardinal n. Notons X'_s l'ensemble des sous-groupes de G' de cardinal p^s. On doit montrer que

$$|X_s| \equiv |X'_s| \mod p$$

En effet, d'après ce qui précède

$$|X_s|\, mp^{r-s} \equiv \binom{n}{p^s} \equiv |X'_s|\, mp^{r-s} \mod mp^{r-s+1}$$

c-à-d

$$|X_s|\, mp^{r-s} - |X'_s|\, mp^{r-s} = k \cdot mp^{r-s+1}$$

où $k \in \mathbb{Z}$. Diviser par mp^{r-s} :

$$|X_s| - |X'_s| = kp$$

où $k \in \mathbb{Z}$, i.e., $|X_s| \equiv |X'_s| \mod p$ ☒

Montrons maintenant que

$$|X_s| \equiv 1 \mod p$$

Soit $G' = \mathbb{Z}/n\mathbb{Z}$, et X'_s l'ensemble des sous-groupes de G' de cardinal p^s.

D'après le lemme précédent,

$$|X_s| \equiv |X'_s| \mod p.$$

Or, d'après un exemple ci-dessus,

$$X'_s = \left\{ \tfrac{n}{p^s}\mathbb{Z}/n\mathbb{Z} \right\}$$

En particulier $|X'_s| = 1$. Du coup

$$|X_s| \equiv |X'_s| \equiv 1 \mod p$$ ☒

<u>Remarque</u> On aurait pu montrer plus directement que

$$|X_s| \equiv 1 \mod p$$

en montrant que

$$\binom{n}{p^s} \equiv mp^{r-s} \mod mp^{r-s+1}$$

Car, dans ce cas, la congruence

$$\binom{n}{p^s} \equiv |X_s|\, mp^{r-s} \mod mp^{r-s+1}$$

impliquerait que $|X_s| \equiv 1 \mod p$.

Corollaire (Th. de Cauchy)
Soit G un groupe fini de cardinal n et p premier divisant n. Alors G contient un élt d'ordre p.

Démo. Comme $p|n$, il existe un sous-groupe de G de cardinal p^1, d'après les Théorèmes de Sylow. Un tel sous-groupe est cyclique car p est premier. Un générateur d'un tel sous-groupe est d'ordre p. $\square$

Exemples illustrant les Théorèmes de Sylow

1) $G = A_4 \qquad n = |G| = 12$

Soit $K = \{(1), (12)(34), (13)(24), (14)(23)\}$

le sous-groupe de A_4 des doubles transpositions. On a vu que K est distingué dans A_4. K est un 2-sylow. Comme il est distingué, G ne contient qu'un seul 2-sylow. Du coup, K est le seul 2-sylow de A_4.
Observons que la partie arithmétique des Théorèmes de Sylow nous disent seulement que le nombre s_2 de 2-sylows de A_4 est $\equiv 1 \mod 2$, et divise 3,

Qu'en est-il des 3-sylows de A_4 ?

$\langle (i\,j\,k) \rangle$ est un 3-sylow de A_4 si $\{i, j, k\} \subseteq \{1,2,3,4\}$ de cardinal 3. On en déduit que A_4 contient $\binom{4}{3} = 4$ 3-sylows.

2) $G = S_4$. $n = 24$

Déterminons les 2-sylows de S_4

Soit $K \subseteq S_4$ des doubles transpositions. K est même distingué dans S_4. Soit $L = \langle (1\,2) \rangle$

Comme K est distingué

$$KL = \{ \sigma\tau \mid \sigma \in K, \tau \in L \}$$

est un sous-groupe de S_4.

(exo. Soit G un groupe et $K, L \leq G$ des sous-groupes

1) donner un exemple où KL n'est pas un sous-groupe de G.

2) Mq si K est distingué, alors KL est un sous-groupe de G)

$|KL| = 4 \times 2 = 8$ car $K \cap L = \{1\}$

(exo : Soit G un groupe et $K, L \leq G$ des sous-groupes

Soit f l'application ensembliste

$$f : K \times L \longrightarrow G$$
$$(k, l) \longmapsto kl$$

1) Mq. $f(K \times L) = KL$
En particulier, f est surjective
ssi $KL = G$
2) Mq. f est injective ssi
$K \cap L = \{1\}$)

Cela montre alors que
$$|KL| = |K| \times |L| = 4 \times 2 = 8.$$
Du coup KL est un 2-sylow de S_4. Soit s_2 le nombre de 2-sylow de S_4. D'après Sylow.
$s_2 \equiv 1 \mod 2$ et $s_2 | 3$ i.e
$s_2 = 1$ ou $s_2 = 3$.
Soit $L' = \langle (13) \rangle$ on peut vérifier que $KL \neq KL'$
Or KL' est encore un 2-sylow de S_4. Du coup, $s_2 \geq 2$
et donc $s_2 = 3$.

Déterminons les 3-sylows de S_4. Comme A_4 est d'indice 2 dans S_4 et $(2,3) = 1$, les 3-sylows de A_4 sont des 3-sylows de S_4. Comme A_4 est distingué dans S_4, il n'y en a pas d'autre, c-à-d, le nombre de 3-sylows de S_4 est égal à 4.

Les théorèmes de Sylow sont très utiles dans la classification des groupes finis. Avant de voir des exemples, rappelons les faits suivants :

<u>Prop.</u> Soit G un groupe et $H, K \leq G$ des sous-groupes. Supposons que H et K sont distingués et que $H \cap K = \{1\}$. Alors $\forall h \in H\ \forall k \in K$,

$$hk = kh.$$

<u>Démo.</u> Considérons le commutateur de h et k, où $h \in H$ et $k \in K$:

$$\begin{aligned} [h,k] &= hkh^{-1}k^{-1} \\ &= (hkh^{-1})k^{-1} \in K \\ &= h(kh^{-1}k^{-1}) \in H \end{aligned}$$

i.e. $[h,k] \in H \cap K = \{1\}$

et $hkh^{-1}k^{-1} = 1$

d'où $hkh^{-1} = k$

et $hk = kh$ $\square$

<u>Corollaire.</u> Soit G un groupe, $H, K \leq G$ sous-groupes distingués avec $H \cap K = \{1\}$ et $HK = G$. Alors l'application ensembliste

$$f : H \times K \longrightarrow G$$
$$(h,k) \longmapsto hk$$

est un isomorphisme de groupes où $H \times K$ est le groupe produit.

<u>Dém</u> On sait que f est surjective car $HK = G$ et que f est injective car $H \cap K = \{1\}$. Par conséquent, f est une bijection. Mq f est un morphisme : Soient (h,k) et $(h',k') \in H \times K$. On a

$$f\big((h,k)\cdot(h',k')\big) = f\big((hh', kk')\big) =$$
$$= hh'kk' \underset{\uparrow}{=} hkh'k' = f(h,k)\cdot f(h',k')$$

la prop. précédent

☒

<u>Exemple</u> Soit G un groupe de cardinal $15 = 3 \times 5$. Soit s_3 (resp^t s_5) le nombre de 3-sylow (resp^t 5-sylows) de G. D'après Sylow,

$$s_3 \equiv 1 \mod 3 \quad , \quad s_3 \mid 5 \quad \Rightarrow s_3 = 1$$
$$s_5 \equiv 1 \mod 5 \quad , \quad s_5 \mid 3 \quad \Rightarrow s_5 = 1$$

Soit $H \leq G$ <u>le</u> 3-sylow de G et $K \leq G$ <u>le</u> 5-sylow de G. H et K sont distingués !

$H \cap K$ est un sous-groupe de H. D'après Lagrange $|H \cap K|$ divise $|H| = 3$. De même, $|H \cap K|$ divise $|K| = 5$. Or $(3,5) = 1$, i.e, $H \cap K = \{1\}$. Du coup $|HK| = |H \times K| = |H| \times |K| = 15$ et $HK = G$.

D'après le corollaire précédent, l'application

$$f : H \times K \longrightarrow G$$
$$(h,k) \longmapsto hk$$

est un isomorphisme de groupes. Or, $H \cong \mathbb{Z}/3\mathbb{Z}$, $K \cong \mathbb{Z}/5\mathbb{Z}$.
D'après le Th. chinois :

$$H \times K \cong \mathbb{Z}/15\mathbb{Z}$$

Au final, $G \cong \mathbb{Z}/15\mathbb{Z}$!
c-à-d tout groupe de cardinal 15 est cyclique, en particulier commutatif.

Plus généralement

<u>Théorème</u>. Soit G un groupe de cardinal pq où p et q sont des nombres premiers distincts. On suppose que $p \not\equiv 1 \mod q$ et que $q \not\equiv 1 \mod p$. Alors, G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ i.e. G est cyclique et commutatif en particulier.

<u>Démo</u>. (exo.)

Que se passe-t-il si $p \equiv 1 \mod q$ ou $q \equiv 1 \mod p$? En supposant $p<q$, on a $p \not\equiv 1 \mod q$ et le q-sylow

sera distingué, mais non forcément le p-sylow.

Soit G un groupe et $H, K \leq G$ deux sous-groupes. Supposons que H est distingué dans G, et non forcément K. On suppose encore que

$$H \cap K = \{1\} \text{ et que } HK = G$$

Soit

$$f : H \times K \to G$$
$$(h,k) \mapsto hk$$

En général, f n'est pas un morphisme de groupe.

Comme f est bijective, il existe une unique loi $*$ sur $H \times K$ telle que

$$(h,k) * (h',k') = f^{-1}(f(h,k) \cdot f(h',k'))$$

$*$ est une loi de groupe sur $H \times K$ qui ne coïncide pas forcément avec la loi de groupe produit sur $H \times K$.

Explicitons $*$:

$$(h,k) * (h',k') = f^{-1}(f(h,k) \cdot f(h',k')) =$$
$$= f^{-1}(hkh'k') = f^{-1}(h(kh'k^{-1})kk')$$
$$= (h(kh'k^{-1}), kk')$$

Donc la loi $*$ sur $H \times K$ est

$$(h,k) * (h',k') = (h(kh'k^{-1}), kk')$$

Le produit kh', par exemple, fait intervenir la loi de G.

En fait, il faut comprendre le produit $kh'k^{-1}$ comme une action de K sur H. De manière générale, si H et K sont des groupes et

$$\varphi : K \times H \longrightarrow H$$

une action de K sur H par morphismes de groupes, alors l'ensemble $H \times K$ acquiert une structure de groupe si on définit

$$(h,k) * (h',k') = (h\,\varphi(k,h'),\ kk')$$

Le groupe est noté $H \rtimes K$ et est le produit semi-direct de H et K.