

3. Simplicité de A_n [Perrin, Cours d'algèbre, chap. I, §8]

Th Si $n \geq 5$, le groupe A_n est simple.

Nous donnons la démonstration du livre de Perrin. Lors de la lecture, nous invitons la lectrice / le lecteur à apprécier l'importance des propriétés ① et ② mises en valeur dans la section précédente :

- ① les 3-cycles ont beaucoup de points fixes
- ② les 3-cycles sont conjugués dans A_n .

Nous allons en donner une démonstration en deux temps : pour $n = 5$ d'abord, par une méthode très élémentaire qui mettra en évidence l'intérêt de la connaissance des classes de conjugaison dans les questions de simplicité ; pour $n > 5$ ensuite, par réduction au cas $n = 5$.

1) Le théorème pour $n = 5$.

Le groupe \mathfrak{A}_5 a 60 éléments : le neutre, 15 éléments d'ordre 2 (produit de deux transpositions disjointes), 20 d'ordre 3 (3-cycles), 24 d'ordre 5 (5-cycles).

On a vu que les cycles d'ordre 3 sont conjugués dans \mathfrak{A}_5 . Les éléments d'ordre 2 le sont aussi : si $\tau = (ab)(cd)(e)$ et $\tau' = (a'b')(c'd')(e')$ il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a) = a', \sigma(b) = b', \sigma(e) = e'$ et on a alors $\tau' = \sigma\tau\sigma^{-1}$.

Soit alors $H \triangleleft \mathfrak{A}_5, H \neq \{1\}$. Si H contient un élément d'ordre 3 (resp. 2) il les contient tous d'après ce qui précède. S'il contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc tous les 5-sous groupes de Sylow puisqu'ils sont conjugués, donc tous les éléments d'ordre 5.

Mais H ne peut contenir un seul des trois types d'éléments précédents (en plus du neutre) car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (n'oublions pas que le cardinal de H divise $|\mathfrak{A}_5| = 60$). Donc H contient au moins deux des trois types, d'où $|H| \geq 15 + 20 + 1 = 36$ et donc $|H| = 60, H = \mathfrak{A}_5$.

Remarque 8.3. Les 24 éléments d'ordre 5 ne sont pas conjugués dans \mathfrak{A}_5 (sinon ils formeraient une orbite et 24 diviserait 60). On peut cependant éviter le recours à Sylow dans la démonstration précédente en remarquant que si a et b sont d'ordre 5, b est conjugué dans \mathfrak{A}_5 de a ou de a^2 .

Rappelons la formule-clé ★★★ qui donne le conjugué d'un cycle par une permutation σ : $\sigma (i_1, \dots, i_k) \sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_k))$

2) Le cas $n > 5$.

Posons $E = \{1, \dots, n\}$. Soit $H \triangleleft \mathfrak{A}_n$, $H \neq \{1\}$ et soit $\sigma \in H$, $\sigma \neq 1$. On va se ramener au cas $n = 5$ et, pour ceci, fabriquer à partir de σ un élément non trivial de H qui n'agisse, en fait, que sur un ensemble à 5 éléments, donc qui ait $n - 5$ points fixes. ①

Vu les remarques ci-dessus, la méthode naturelle à notre disposition est de prendre un commutateur $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$, avec $\tau \in \mathfrak{A}_n$. Ecrivant $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$, on a vu que ρ est dans H . Mais si on regarde ρ par l'autre bout : $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$ on constate que ρ est produit de deux éléments du type de τ de sorte que si τ a beaucoup de points fixes, il en sera de même de ρ . ①

Il ne reste plus qu'à mettre ces remarques en forme :

Comme $\sigma \neq 1$, il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \neq a, b, \sigma(b)$, soit τ le 3-cycle $\tau = (acb)$, de sorte que $\tau^{-1} = (abc)$ et soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (acb)(\sigma a, \sigma b, \sigma c)$. Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma a, \sigma b, \sigma c\}$ a au plus 5 éléments et on a $\rho(F) = F$, $\rho|_{E-F} = \text{Id}_{E-F}$. ①

Quitte à rajouter, au besoin, des éléments à F , on peut supposer $|F| = 5$. On note enfin que ρ est distinct de 1, car $\rho(b) = \tau\sigma(b) \neq b$ puisque $\sigma(b) \neq \tau^{-1}(b) = c$.

Soit alors $\mathfrak{A}(F)$ l'ensemble des permutations paires de F , $\mathfrak{A}(F)$ est isomorphe à \mathfrak{A}_5 et $\mathfrak{A}(F)$ se plonge dans \mathfrak{A}_n par $u \mapsto \bar{u}$ avec :

$$\bar{u}|_F = u \quad ; \quad \bar{u}|_{E-F} = \text{Id}_{E-F}.$$

Posons $H_0 = \{u \in \mathfrak{A}(F) \mid \bar{u} \in H\} = H \cap \mathfrak{A}(F)$. Il est clair que H_0 est distingué dans $\mathfrak{A}(F)$ et qu'on a $\rho|_F \in H_0$ et $\rho|_F \neq \text{Id}_F$. Comme $\mathfrak{A}(F) \simeq \mathfrak{A}_5$ est simple, on a $H_0 = \mathfrak{A}(F)$. Soit alors u un cycle d'ordre 3 de $\mathfrak{A}(F)$, il est dans H_0 , donc \bar{u} qui est encore un cycle d'ordre 3 est dans H .

Mais, comme les 3-cycles sont conjugués dans \mathfrak{A}_n , ils sont tous dans H , et comme ils engendrent \mathfrak{A}_n , on a montré $H = \mathfrak{A}_n$, ce qui achève la démonstration. ②