Développement : Théorème de Wedderburn - Méthode de Witt

Théorème : K est un corps fini : il sera prouvé qu'il est nécessairement commutatif.

1. Historique. — *Ce résultat important a été démontré par de nombreux mathématiciens avec des approches différentes. On peut citer Artin, , Bourbaki, Zassenhaus, Witt et, le premier chronologiquement, MacLadgan Wedderburn qui produisit 3 méthodes différentes. On choisit ici la méthode très élégante due à Witt en 1931*

2. Première moitié du chemin : algèbre générale et linéaire. —

- Extension des corps :
  - Pro : Si on a une tour de corps finis $M \subset L \subset K$, si M est commutatif, L et K peuvent être considérés comme des M-espaces vectoriels de dimension finie, dimensions que l'on note $[K : M]$ et $[K : M]$. De même, si L est commutatif, K est un L-espace vectoriel de dimension $[K : L]$.
  - *Bases Télescopiques* - nous avons $[K : M] = [K : L] \times [K : M]$.
  - *Corps premier* P : image du morphisme d'anneaux $g : \mathbb{Z} \to K$, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ où p est la caractéristique de K. On note $card(P) = p$ et p est premier. P est *commutatif.*
  - Le Centre de K, noté Z est un sous-corps *commutatif* de K contenant P. Le cardinal de Z est donc une puissance de p que l'on notera q. On note n la Z-dimension de K, de sorte que $card(K) = q^n$.
  - Pro : $\forall x \in K$, le Centralisateur C_x de élément x est un sous-corps de K contenant Z. On note n_x sa Z-dimension, de sorte que $card(C_x) = q^{n_x}$.
  - Comme C_x est un sous-groupe de K, on a *pour tout* x : (Eq:*) q^{n_x}/q^n.
  - Comme $(C_x^*, .)$ est un sous-groupe de $(K^*, .)$, *pour tout* x : $(q^{n_x} - 1)/(q^n - 1)$.
- Action de groupe :
  - Considérons sur le groupe $(K^*, .)$ l'action par conjugaison du groupe sur lui-même, $(K^*, .) \times (K^*, .) \to (K^*, .)$ avec $(y, x) \mapsto y \odot x = yxy^{-1}$.
  - On a alors que $Stab(x) = C_x$.
  - L'orbite de s sera notée A_s et on notera Θ l'ensemble des orbites.
  - L'équation des classes nous donne alors : $Card(K^*) = \Sigma_\Theta Card(A_s) = \Sigma_\Theta \frac{Card(K^*)}{Card(C_s)} = \Sigma_\Theta \frac{q^n - 1}{q^{n_s} - 1}$.
  - Rem : K est commutatif ssi $Z = K$ auquel cas chaque orbite est un singleton et la seule classe de conjugaison est K^*.
- Nous avons enfin :
  - Si K est commutatif : $q^n - 1 = q - 1$ et $n = 1$
  - Si K n'est pas commutatif on aura des orbites singleton pour les $q-1$ éléments de Z et les autres orbites, de sorte que nous aurons l'équation (Eq:**) : $q^n - 1 = (q - 1) + \Sigma_{\Theta - Z} \frac{p^n - 1}{p^{n_s} - 1}$

3. Deuxième moitié : racines n-ièmes de l'unité dans $\mathbb{C}$. —

- L'équation (Eq:**) fait intervenir un polynôme $X^n - 1$. Or, $\forall n \in \mathbb{N}, X^n - 1 = \Pi_{d|n} \phi_d(X)$
- Pro : les coefficients des différents $\phi_d(X)$ sont entiers.
- En considérant que K n'est pas commutatif, il existe au moins un s (et son n_s associé) pour lequel $Card(A_s) > 1$ et n_s divise n (Eq:*).
- on a alors : $X^n - 1 = (\phi_n(X))\Pi_{d|n_s} \phi_d(X) \Pi_{d|n, d \neq n, d \dagger n_s} \phi_d(X) = (\phi_n(X))(X^{n_s} - 1)\Pi_{d|n, d \neq n, d \dagger n_s} \phi_d(X)$
- Si on l'applique à q : $\phi_n(q)$ divise $q^n - 1$ et $\phi_n(q)$ divise $\frac{q^n - 1}{q^{n_s} - 1}$
- En revenant à l'équation (Eq:**) on voit alors que $\phi_n(q)$ doit diviser $q - 1$.
- Or, $\phi_n(X) = \Pi(X - \lambda)$ et chaque racine de l'unité λ autre que 1 ou -1 vérifie que $|q - \lambda > q - 1$ et donc, puisque on fait l'hypothèse que $n > 1$, $|\phi_n(q)| > q - 1$ et ne peut le diviser. Ceci confirme le caractère absurde de l'hypothèse de non-commutativité.

.

Sources :Proofs from THE BOOK

December 10, 2017

Bruno Nitrosso, EPP et candidat libre