105 - Groupes des permutations d'un ensemble fini. Applications.

Motivation: Le groupe symétrique a été introduit pour étudier les racines d'un polynôme (début de la théorie de Galois). Le groupe des permutations permet également d'introduire la notion d'action de groupe. Enfin le théorème de Cayley qui dit que tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique justifie le fait que l'étude des groupes des permutations est très étudié.

I Généralités sur le groupe symétrique

Définition et action de groupe

Def Le groupe $\mathfrak{S}(E)$ est le groupe des permutations de E. [Rom01]

Prop Si E te F sont deux ensembles non vides en bijection alors $\mathfrak{S}(E)$ et $\mathfrak{S}(F)$ sont en bijection. [Rom01]

Rq On note $\mathfrak{S}_n := \mathfrak{S}([1,n])$ et on peut donc se restreindre à cet ensemble.

Prop $\mathfrak{S}_n := \mathfrak{S}([1,n])$ est de cardinal $n!$ [Rom01].

Thme De Cayley [Per04] (+ rq disant que ça ne sert pas à grand chose).

Def Action de groupe et le lien avec le groupe symétrique [Per04].

Ex Action de $\mathfrak{S}_3$ sur les sommets d'un triangle

Ex L'ensemble des permutations laissant stable un point est isomorphe à $\mathfrak{S}_{n-1}$.

Support et orbites d'une permutation

Def D'un cycle et d'une transposition (+ un exemple) [Rom01]

Lem La formule $\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \cdots, \tau(x_r))$ [Rom01].

App On en déduit que deux cycles sont conjugués entre eux SSI ils sont de même longueur.

Def Orbite d'une permutation et d'un élément [Rom01]

Rq Les orbites sont deux à deux distinctes et forment une partition de E. Ce sont donc des classes d'équivalence pour la relation d'équivalence $x\mathcal{R}y \Leftrightarrow (\exists k \in \mathbb{Z},\ y = \sigma^k(x))$ [Rom01].

Def Support d'une permutation [Rom01].

Prop $\sigma(Supp(\sigma)) = Supp(\sigma)$; $Supp(\sigma)) = Supp(\sigma^{-1})$, $Supp(\sigma^r)) \subset Supp(\sigma)$ et que deux cycles à support disjoints commutent. [Rom01]

CE La réciproque du dernier point est fausse (σ, σ^{-1})

App L'odre d'une permutation (sous forme de produit de cycles à support disjoints) et le ppcm des longueurs des cycles. [Rom01].

Générateurs

Thme Toute permutation se décompose en produit de cycle à support disjoint [Rom01] + donner un exemple

App On peut en déduire les classes de conjugaison de $\mathfrak{S}_n := \mathfrak{S}([1,n])$.

Prop Les transpositions engendrent $\mathfrak{S}_n$ [Rom01]

Prop $\mathfrak{S}_n$ est engendré par les transpositions $(1,k)$, les transpositions $(k,k+1)$ et par $(1,2)$ avec $(1,2,\cdots,n$ [Rom01]

Rq Pour connaitre un morphisme de $\mathfrak{S}_n$, il suffit de connaitre ses valeurs sur les transpositions.

Rq Le générateur $(1,2)$ avec $(1,2,\cdots,n)$ est utile en informatique.

App Si $n \geq 3$ alors $Z(\mathfrak{S}_n) = \{id\}$.

II Le groupe alterné

Signature

Def La signature notée ϵ est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\{-1,1\}$. [Rom01]

Coro $\epsilon(\tau) = -1$ et $\epsilon(r-cycle) = (-1)^{r-1}$ + cas général pour une décomposition. [Rom01]

Prop Le cardinal du noyau de ϵ est $\frac{n!}{2}$.

Prop $\epsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{j-i}$. [Rom01]

Ex Terminer par un exemple, celui du [Rom01] par exemple.

Groupe alterné

Def Le groupe alterné est l'ensemble des permutations paires, i.e. le noyau de ϵ. On le note $\mathfrak{A}(E)$ [Rom01].

Prop Comme $\mathfrak{A}_n$ est d'indice 2 alors il est distingué dans $\mathfrak{S}_n$.

Prop Pour $n \geq 3$ le groupe $\mathfrak{A}(E)$ est engendré par les produits de deux transpositions; les 3-cycles. [Rom01].

Prop Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$ [Per04].

CE C'est faux si $n \leq 4$. [Per04].

DEV Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$ et $n = 3$. [Rom01].

App Pour $n \geq 5$ les sous-groupes distingué de $\mathfrak{S}_n$ sont $\{id\}, \mathfrak{S}_n$ et $\mathfrak{A}_n$.

III Application

Déterminant

Def Forme n-linéaire antisymétrique + forme n-linéaire alternée [Rom01]

Prop Si $car(\mathbb{K}) \neq 2$ alors forme antisymétrique = forme alternée [Rom01]

Def Du déterminant comme l'unique forme n-linéaire alternée. Et def/lien avec la grosse formule du déterminant. [Rom01]

Ex $\det(P_\sigma) = \epsilon(\sigma)$ [Rom01]

Polynômes symétrique

Def Polynôme symétrique, polynôme symétrique élémentaire [QQ17]

Thme Théorème de décomposition des polynômes symétriques [QQ17]

App Formules de Vietes [QQ17]

Def Définition et propriétés sur les polynômes cyclotomiques (pour le dev) [QQ17] (démo dans [Per04])

DEV Théorème de Kronecker. [QQ17]

Isomorphismes execptionnels

- Les isomorphismes de la forme $PSL(2, \mathbb{F}_3) \simeq \mathfrak{A}_4$, $PGL(2, \mathbb{F}_4) \simeq PSL(2, \mathbb{F}_4) \simeq \mathfrak{A}_5$, [Per04] et [CG13].