110 : Structure et dualité des groupes abéliens finis.

Rombaldi :
Peyré :
Ulmer :

I Structure des groupes abéliens finis [Rom]

• Groupes cycliques :

- **Def 1 :** Un groupe G est dit cyclique s'il est fini et s'il est engendré par un élément.
- **Def 2 :** Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ et à $(\mathbb{U}_n, \times)$.
- **Prop 3 :** $\forall d \mid |G|$, G admet un unique sous-groupe d'ordre d, c'est : $H_d := \{x \in G \text{ tq } x^d = 1\} = \{\omega^k, k \in [\![1 : d]\!]\}$, où ω est d'ordre d.
- **Prop 4 :** $\forall d \mid |G|$, G possède $\varphi(d)$ éléments d'ordre d, où $\varphi(d)$ est le nombre d'entiers premiers avec d dans $[\![1 : d]\!]$.
  - **Application 5 :** $\forall n \in \mathbb{N}^*$, $\sum_{d \mid n} \varphi(d) = n$
  - **Application 6 :** Si k est un corps, tout sous-groupe fini de k^* est cyclique.
- **Thm 7 : (Chinois)** $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ssi $m \wedge n = 1$.
- **Ex :** $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- **Prop 8 :** $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}$. Les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les : $\overline{k} \mapsto \overline{lk}$, où $k \wedge l = 1$.

• Groupes abéliens :

- **Def 9 :** L'exposant d'un groupe abélien est le ppcm des ordres des éléments du groupe.
- **Prop 10 :** $\forall x, y \in G$, $\exists z \in G$ tq $o(z) = \mathrm{ppcm}(o(x), o(y))$.
- **Contre-exemple** si G n'est pas abélien : $G = S_3$, $x = (1,2)$, $y = (1,2,3)$
  - **Corollaire 11 :** Il existe $a \in G$ tq $o(a) = \exp(G)$.
  - **Application 12 :** 2ème démo de : Tout sous-groupe fini de k^* est cyclique.

II Dualité des groupes abéliens finis [Pey]

• Caractères et groupe dual :

- **Def 13 :** Un caractère χ de G est un morphisme de G dans $\mathbb{C}^*$. L'ensemble des caractères de G forme un groupe : le groupe dual, noté $\hat{G}$.
- **Prop 14 :** Si $n := |G|$, tout caractère χ de G est à valeurs dans $\mathbb{U}_n$.

DEV

- **Prop 15:** Soit ω une racine primitive n-ième de l'unité, ~~et soit g_0 un générateur de G~~. Les caractères de $\mathbb{Z}/n\mathbb{Z}$ sont les $\chi_k : \bar{j} \mapsto \omega^{jk}$, pour $k \in [\![0; n-1]\!]$.

- **Cor 16:** Si G est cyclique, $G \simeq \hat{G}$.

- **Rq 17:** Un tel isomorph n'est pas canonique, il dépend du choix de ω.

- **Lemme 18:** Si H est un sous-groupe de G, tout caractère de H se prolonge en un caractère de G.

- **Cor 19:** Pour tout groupe abélien fini G, il existe $d_1 \dots d_s \in \mathbb{N}$ tq $d_1 \geq 2$, $d_1 | \dots | d_s$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$

- **Prop 20:** Une telle famille $d_1 \dots d_s$ est unique ainsi que les d_i près.

- **Cor 20:** $G \simeq \hat{G}$, pour G gaf.

- **Rq 21:** Un tel isomorphisme n'est toujours pas canonique.

- **Def 22:** Le bidual de G est $\hat{\hat{G}}$.

- **Prop 23:** On a un isomorphisme canonique de G sur $\hat{\hat{G}}$ donné par : $g \mapsto ev_g : \chi \mapsto \chi(g)$.

- **Orthogonalité des caractères :**

- **Def 24:** On note $\mathbb{C}[G] := \mathcal{F}(G; \mathbb{C})$. C'est un espace hermitien muni de $\langle f : g \rangle := \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$

- **Lemme 25:** Pour $\chi \in \hat{G}$, $\sum_{g \in G} \chi(g) = \begin{cases} 0 \text{ si } \chi \neq 1 \\ |G| \text{ si } \chi = 1 \end{cases}$

- **Prop 26:** Les caractères forment une base orthonormée de $\mathbb{C}[G]$: Pour $\chi_1, \chi_2 \in \hat{G}$ $\langle \chi_1 : \chi_2 \rangle = \begin{cases} 1 \text{ si } \chi_1 = \chi_2 \\ 0 \text{ sinon} \end{cases}$

- **Prop 27:** Pour $g, h \in G$: $\sum_{\chi \in \hat{G}} \chi(g) \overline{\chi(h)} = \begin{cases} 0 \text{ si } g \neq h \\ |G| \text{ si } g = h \end{cases}$

III. Représentations des groupes abéliens finis [Ulm]

- **Définition et exemples:**

- **Def 28:** Une représentation de G est (E, ρ), où E est un G-EV de dim finie, et ρ est un morphisme de G dans $GL(E)$.
Le degré de (E, ρ) est la dimension de E.

- **Prop 29:** Les représentations de degré 1 de G sont les caractères (les morphismes de $G \to \mathbb{C}^\times$).

- **Def 30:** (E, ρ) est fidèle si ρ est injectif.

• Def 31 : La représentation régulière de G est la représentation par permutations de G associée à l'action de G sur lui-même par translations à gauche, ie : $E := \mathbb{C}^G$, dont une base est $(e_g)_{g\in G}$, définie par $e_g(h) = 0$ si $g \neq h$, $= 1$ si $g = h$.
• $\forall g, h \in G$, $g \cdot e_h := e_{gh}$
On la note $R(G)$.

• Prop 32 : $R(G)$ est fidèle. $\deg(R(G)) = |G|$.

Morphismes et sous-représentations :

• Def 33 : Un morphisme de (E_1, ρ_1) dans (E_2, ρ_2) est $\varphi \in \mathcal{L}(E_1, E_2)$ tq $\forall v \in E_1$, $\forall g \in G$, $g \cdot \varphi(v) = \varphi(g \cdot v)$.
L'ensemble des morphismes de E_1 dans E_2 est noté $\mathcal{L}_G(E_1 : E_2)$.

• Def 34 : Une sous-représentation de (E, ρ) est un sev F de E tq $\forall g \in G$, $\forall v \in V$, $g \cdot v \in V$.

• Prop 35 : Pour $\varphi \in \mathcal{L}_G(E_1 : E_2)$, $\ker(\varphi)$ et $\mathrm{Im}(\varphi)$ sont des sous-représentations de (E_1, ρ_1) et (E_2, ρ_2)

• Thm 36 : (Maschke) : Toute sous-rep de (E, ρ) admet un supplémentaire stable par G.

• Def 37 : Une sous-rep de (E, ρ) est dite irréductible si $E \neq \{0\}$ et si E n'a pas de sous-représentation non triviale.

• Cor 38 : Toute représentation se décompose en somme directe de rep irréductibles.

• Prop 39 : Toute représentation irréductible est isomorphe à une sous-rep de la régulière.

• Cor 40 : G est abélien ssi toutes ses représentations irréductibles sont de degré 1 (ie les morphismes de G dans $\mathbb{C}^*$).

IV Corps finis [Peg]

• Def 41 : Soit p un nombre premier.
Le symbole de Legendre de $x \in \mathbb{F}_p^*$ est :
$$\left(\frac{x}{p}\right) := \begin{cases} 1 \text{ si } x \text{ est un carré} \\ -1 \text{ sinon} \end{cases}$$

• Prop 42 : $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$

• Cor 43 : Le symbole de Legendre est un caractère de $\mathbb{F}_p^*$.