

Chapitre 5

Compléments : groupes, polynômes

5.1 Produits semi-directs

Soient G' et G deux groupes notés multiplicativement, et $\gamma : G \rightarrow \text{Aut}(G')$ un morphisme de groupe. L'image par γ de $x \in G$ est notée γ_x .

On définit sur le produit cartésien $G \times G'$ une opération :

$$(x', x)(y', y) = (x'\gamma_x(y'), xy) .$$

Proposition 5.1.1. *L'opération précédente définit une structure de groupe.*

Définition 5.1.2. On appelle produit semi-direct de G' et G au dessus de γ le groupe précédent. On le note $G' \times_{\gamma} G$.

Remarque 5.1.3. Lorsque γ est constante : $\forall x \in G, \gamma_x = \text{Id}_{G'}$, on retrouve le produit direct.

Exemple 5.1.4. Soient $G' = \langle a \rangle$, $G = \langle b \rangle$ des groupes cycliques d'ordres respectifs $n \geq 2$ et 2, et $\gamma : G \rightarrow \text{Aut}(G')$ défini par $\gamma_b(a^k) = a^{-k}$.

Le produit semi-direct $G' \times_{\gamma} G$ est appelé *groupe diédral* à $2n$ éléments, et noté D_n . Il est engendré par $\alpha = (a, b^0)$ et $\beta = (a^0, b)$ qui satisfont les relations (ici $e = (a^0, b^0)$ est le neutre) : $\alpha^n = e = \beta^2$, $\beta\alpha = \alpha^{-1}\beta$. Notons que les éléments $\alpha^k\beta$ qui ne sont pas dans le groupe cyclique $\langle \alpha \rangle$ sont d'ordre 2 et pour $n > 2$ engendrent un sous-groupe qui n'est pas distingué.

19/10/2011

Théorème 5.1.5 (Décomposition en produit semi-direct). *Soient H et K des sous-groupes d'un groupe G noté multiplicativement. Si H est un sous-groupe distingué et $H \cap K = \{e\}$, alors HK est un sous-groupe de G isomorphe au produit semi direct $H \times_{\gamma} K$, où $\gamma_k(h) = khk^{-1}$.*

Remarque 5.1.6. Dans le cas de groupes finis, le cardinal de HK est le produit des cardinaux de H et de K , il est facile de voir si HK est égal à G !

5.2 Groupes libres et présentations

Etant donné deux symboles a et b , on considère l'ensemble des mots (suites finies) en $a, b, \bar{a}$ et $\bar{b}$ (le mot vide est admis). Un mot est réduit si et seulement s'il ne contient aucune occurrence d'un symbole suivi de son *inverse* : $a\bar{a}$, $\bar{a}a$, $b\bar{b}$ ou $\bar{b}b$,

Le groupe libre à deux éléments $L(a, b)$ est l'ensemble des mots réduits en $a, b, \bar{a}$ et $\bar{b}$ (y compris le mot vide), muni de l'opération obtenue avec la concaténation suivie de la réduction : on itère l'enlèvement de l'occurrence d'un symbole suivi de son inverse, tant qu'on en trouve.

Proposition 5.2.1. *a) $L(a, b)$ est un groupe.*

b) Pour tout groupe G , et tout $x \in G$, and $y \in G$, il existe un unique morphisme de groupe $\phi : L(a, b) \rightarrow G$ tel que $\phi(a) = x$, $\phi(b) = y$.

On définit de même plus généralement le groupe libre à n générateurs : $L(a_1, \dots, a_n)$, voire le groupe libre $L(E)$ avec un ensemble quelconque de générateurs.

Etant donné un ensemble $R \subset L(E)$, on note :

$$\langle E; R \rangle ,$$

le quotient du groupe libre $L(E)$ par le sous-groupe normal engendré par R .

Définition 5.2.2. Une présentation d'un groupe G est un ensemble E de générateurs et un ensemble $R \subset L(E)$ qui engendre, comme sous-groupe normal, le noyau du morphisme $L(E) \rightarrow G$ qui étend l'inclusion des générateurs :

$$\langle E; R \rangle \simeq G .$$

5.3 Action de groupe

Définition 5.3.1. Une action d'un groupe G sur un ensemble X est un morphisme du groupe G dans les bijections de X , $\gamma : G \rightarrow \mathcal{B}(X)$.

On note habituellement $g.x$ pour $\gamma_g(x)$. On peut aussi définir une action comme l'opération externe : $(g, x) \mapsto g.x$, avec $e.x = x$ et $g.(g'.x) = (gg').x$ pour tout x, g, g' .

Exemple 5.3.2. Un sous-groupe H d'un groupe G opère sur G par translation à gauche.

5.3.1 Orbites et stabilisateur

Une action d'un groupe G sur un ensemble X définit une partition de G en orbites $Gx = \{g.x, g \in G\}$. Le stabilisateur d'un élément x est le sous-groupe $\text{Stab}(x) = \{g, g.x = x\}$.

Dans le cas de l'action par translation à gauche de l'exemple précédent les orbites sont les classes à gauche Hx et le stabilisateur est trivial.

Lemme 5.3.3. *Etant donnée une action du groupe G sur X , le cardinal de l'orbite de $x \in X$ est égal à l'indice du stabilisateur $[G : \text{Stab}(x)]$.*

Théorème 5.3.4 (Formule des classes). *Etant donnée une action du groupe G sur un ensemble fini X , on a :*

$$\text{card}(X) = \sum_{x \in R} \#Gx = \sum_{x \in R} [G : \text{Stab}(x)] ,$$

où $R \subset X$ est un ensemble représentatif des classes.

Action de conjugaison

Un groupe G agit sur lui-même par conjugaison : $(g, h) \mapsto ghg^{-1}$. Le stabilisateur de h , noté C_h , s'appelle alors le centralisateur de h .

Un groupe G agit sur ses sous-groupes par conjugaison : $(g, H) \mapsto gHg^{-1}$. Le stabilisateur de H ; noté N_H s'appelle alors le normalisateur de H .

Proposition 5.3.5. *Dans un groupe G de cardinal p^α avec p premier, le centre est non trivial.*

24/10/2011

5.4 Groupes résolubles

Définition 5.4.1. Un groupe G est résoluble si et seulement s'il existe une suite :

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1} , et G_{i+1}/G_i abélien.

Théorème 5.4.2. *Tout groupe G de cardinal p^α avec p premier est résoluble.*

5.5 Théorèmes de Sylow

Définition 5.5.1. Dans un groupe G de cardinal mp^α , p premier qui ne divise pas m , on appelle p -sous-groupe de Sylow (ou simplement p -Sylow) tout sous-groupe de cardinal p^α .

Théorème 5.5.2. Soit G un groupe de cardinal mp^α , p premier qui ne divise pas m , alors le nombre n_p de p -sous-groupes de Sylow est congru à 1 modulo p .

Théorème 5.5.3. Soit G un groupe de cardinal mp^α , p premier qui ne divise pas m , alors tous les p -sous-groupes de Sylow sont conjugués et leur nombre n_p divise m .

5.6 Polynômes à n variables

Soit A un anneau commutatif et $X_1, \dots, X_n$ des *indéterminées*. On note $A[X_1, \dots, X_n]$ l'ensemble des familles d'éléments de A indexées par $\mathbb{N}^n$, avec un nombre fini de termes non nuls, notées comme combinaisons linéaires des $X_1^{k_1} \dots X_n^{k_n}$, $k_j \geq 0$: les éléments de $A[X_1, \dots, X_n]$ s'écrivent sous la forme :

$$P = \sum_{k_1, \dots, k_n} a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n} = \sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \dots X_n^{k_n} .$$

$A[X_1, \dots, X_n]$ est muni des opérations :

$$\left(\sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \dots X_n^{k_n} \right) + \left(\sum_{\underline{k}} b_{\underline{k}} X_1^{k_1} \dots X_n^{k_n} \right) = \sum_{\underline{k}} (a_{\underline{k}} + b_{\underline{k}}) X_1^{k_1} \dots X_n^{k_n} .$$

$$\left(\sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \dots X_n^{k_n} \right) \left(\sum_{\underline{l}} b_{\underline{l}} X_1^{l_1} \dots X_n^{l_n} \right) = \sum_{\underline{\nu}} c_{\underline{\nu}} X_1^{\nu_1} \dots X_n^{\nu_n} ,$$

$$\text{avec } c_{\underline{\nu}} = \sum_{\underline{k} + \underline{l} = \underline{\nu}} a_{\underline{k}} b_{\underline{l}} ,$$

et de l'application de structure :

$$\begin{aligned} \eta : A &\rightarrow A[X_1, \dots, X_n] \\ a &\mapsto aX^0 = a \end{aligned}$$

Proposition 5.6.1. $A[X_1, \dots, X_n]$ est une algèbre sur A .

Remarque 5.6.2. L'application qui définit la structure d'algèbre est injective, d'image les polynômes constants; A est identifié au sous-anneau de $A[X_1, \dots, X_n]$ formé par les polynômes *constants*.

Proposition 5.6.3 (Propriété universelle). *Soit B une algèbre sur l'anneau commutatif A , et $b_1, \dots, b_n$ des éléments de B , alors il existe un unique morphisme d'algèbre $E_{(b_1, \dots, b_n)} : A[X_1, \dots, X_n] \rightarrow B$ qui envoie chaque X_i sur b_i .*

Proposition 5.6.4. *Les anneaux $A[X_1, \dots, X_{n-1}, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes.*

Corollaire 5.6.5. *Si l'anneau A est factoriel, alors $A[X_1, \dots, X_n]$ est factoriel.*

Définition 5.6.6. Le multidegré d'un monôme $a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n}$ est la suite des exposants $(k_1, \dots, k_n)$; son degré total ou simplement son degré est la somme des exposants : $|k| = \sum_i k_i$.

Le degré d'un polynôme non nul est le maximum des degrés (totaux) de ses monômes.

5.7 Polynômes symétriques

Le groupe symétrique $\mathcal{S}_n$ agit à gauche sur $A[X_1, \dots, X_n]$ par permutation des variables : pour $\sigma \in \mathcal{S}_n$,

$$\sigma.P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) .$$

Définition 5.7.1. Les polynômes invariants sous l'action du groupe symétrique forme un sous-anneau de $A[X_1, \dots, X_n]$: le sous-anneau des polynômes symétriques, noté $A[X_1, \dots, X_n]^{sym}$.

Polynômes symétriques élémentaires

Définition 5.7.2. Pour $1 \leq k \leq n$ le polynôme symétrique élémentaire $\sigma_k \in A[X_1, \dots, X_n]^{sym}$ est le coefficient de degré $n - k$ du polynôme :

$$\prod_i (T + X_i) \in A[X_1, \dots, X_n][T] .$$

Remarques 5.7.3. 1. On a : $\sigma_k = \sum_{i_1 < i_2 < \dots < i_k} X_{i_1} \dots X_{i_k}$.

2. Relations entre coefficients et racines :

$$\prod_{i=1}^n (X - \alpha_i) = X^n + \sum_{k=1}^n (-1)^k \sigma_k(a_1, \dots, a_n) X^{n-k} .$$

Théorème 5.7.4. *Tout polynôme symétrique s'écrit de manière unique comme un polynôme dans les polynômes symétriques élémentaires : le morphisme d'algèbre de $A[Y_1, \dots, Y_n]$ dans $A[X_1, \dots, X_n]^{sym}$ qui envoie Y_k sur σ_k est un isomorphisme d'algèbre.*

5.8 Résultant et discriminant

Définition 5.8.1. Soient K un corps, $P \in K[X]$ un polynôme unitaire et pour $Q \in K[X]$, ψ_Q la multiplication par Q modulo P :

$$\begin{aligned} \psi_Q : \mathbb{K}[X]/(P) &\rightarrow \mathbb{K}[X]/(P) \\ \overline{U} &\mapsto \overline{UP} \end{aligned}$$

On définit le résultant :

$$\text{Res}(Q, P) = \det(\psi_Q) .$$

Théorème 5.8.2. *Le résultant $\text{Res}(Q, P)$ est non nul si et seulement si P et Q sont premiers entres eux.*

Remarque 5.8.3. Le résultant ne change pas par extension du corps des coefficients.

Proposition 5.8.4. a) $\text{Res}(Q_1 Q_2, P) = \text{Res}(Q_1, P) \text{Res}(Q_2, P)$.

b) $\text{Res}((Q, X - \alpha)^k) = Q(\alpha)^k$.

c) $\text{Res}(Q, P_1 P_2) = \text{Res}(Q, P_1) \text{Res}(Q, P_2)$.

d) Si P est scindé : $P = \prod_{i=1}^n (X - \alpha_i)$, alors :

$$\text{Res}(Q, P) = \prod_{i=1}^n Q(\alpha_i).$$

Discriminant

Soit $P = a_0 + \dots + a_{n-1}X^{n-1} + X^n$ un polynôme unitaire de degré n à coefficients dans un corps K .

Définition 5.8.5. Le discriminant de P est :

$$\text{Disc}(P) = (-1)^{\frac{n(n-1)}{2}} \text{Res}(P', P) .$$

Théorème 5.8.6. Si le polynôme unitaire P est scindé : $P = \prod_{i=1}^n (X - x_i)$, alors :

$$\text{Disc}(P) = \prod_{i < j} (x_j - x_i)^2 .$$

Corollaire 5.8.7. *Le polynôme unitaire P a une racine double si et seulement si son discriminant est nul.*