Groupes et Anneaux

Johannes Huisman

Plan

I Groupes

§1 Rappels

§2 Théorèmes de Sylow

§3 Groupes abéliens de type fini

II Anneaux

§1 Rappels

§2 Modules

§3 Anneaux de polynômes

Bibliographie

S. Lang : Algebra

M.P Malliavin : Algèbre commutative

P. Tauvel : Cours d'algèbre

(notes de cours sur ma page web)

I Groupes

§1 Rappels

Actions de groupes

Déf. Soit $(G, \cdot)$ un groupe. Soit E un ensemble. Une action (à gauche) de G sur E est une loi de composition externe $*$ ayant les propriétés suivantes :

1) $\forall x \in E : \quad 1 * x = x$
2) $\forall g, h \in G : \forall x \in E :$
$$(gh) * x = g * (h * x)$$

On dit alors que E est un G-ensemble

Exemples

1. Soit S_n le groupe symétrique sur $\{1, 2, 3, \ldots, n\}$, i.e, S_n est le groupe des bijections de $\{1, \ldots, n\}$ dans lui-même. On sait que $|S_n| = n!$

On définit une loi de composition externe de S_n sur $\{1, \dots n\}$ par

$$\sigma * i := \sigma(i)$$

où $\sigma \in S_n$ et $i \in \{1, \dots n\}$.
C'est une action de S_n sur $\{1, \dots n\}$

2. Soit $G = S_n$ et $E = \mathcal{P}(\{1, \dots n\})$ l'ensemble des parties de $\{1, \dots n\}$. $|E| = 2^n$ Considérons la loi externe de S_n sur E définie par

$$\sigma * A = \sigma(A)$$

où $\sigma \in S_n$ et $A \in \mathcal{P}(\{1, \dots n\})$ c-à-d $A \subseteq \{1, \dots n\}$ Ceci définit une action de S_n sur $\mathcal{P}(\{1, \dots n\})$.

3. Soit G un groupe agissant sur un ensemble E. Supposons que H est un sous-groupe de G. Définissons une loi externe
$\circledast : H \times E \to E$ par $h \circledast x := h * x$

C'est une loi obtenue par restriction.

l'action de G sur E

C'est une action de H sur E

Soit G un groupe et E un G-ensemble.

<u>Déf.</u>: Soit $x \in E$. Soit

$$G_x = \{ g \in G \mid g * x = x \}$$

G_x est le <u>stabilisateur de x</u>

<u>Prop.</u> G_x est un sous-groupe de G.

<u>Démo.</u> (exo).

<u>Exemple</u> Considérons l'action de S_n sur $\{1, \ldots n\}$

$$(S_n)_n = \{ id, (1\,2) \text{ si } n > 2, \ldots \}$$
$$= S_{n-1} \text{ vu comme sous-groupe de } S_n$$

Plus explicitement

$$(S_3)_3 = \{ \sigma \in S_3 \mid \sigma(3) = 3 \}$$
$$= \{ id, (1,2) \} = S_2$$

<u>Déf.</u> Soit $g \in G$ et $x \in E$. On dit que x est un <u>point fixe</u> de g si $g * x = x$ i.e. si $g \in G_x$. On dit que x est un <u>point fixe</u> de G si $\forall g \in G : g * x = x$ i.e. si $G_x = G$

Si x est point fixe de G on dit encore que G agit trivialement sur x !

G agit librement sur x si $G_x = \{1\}$. G agit librement sur E si G agit librement sur tous les éléments de E. G agit fidèlement sur E si

$$\forall x \in E \quad g * x = x \Rightarrow g = 1$$

i.e. seul $1 \in G$ agit trivialement sur tous les éléments de E

Ou encore, l'action est fidèle si

$$\bigcap_{x \in E} G_x = \{1\}$$

Exemple. S_n n'agit pas librement sur $\{1, .., n\}$ $(n \geq 3)$

En effet, $(1\ 2)(3) = 3$.

L'action de S_n sur $\{1, .., n\}$ est fidèle : si $\sigma \in S_n \setminus \{id\}$ alors $\exists\, x \in \{1, .., n\}$ tq $\underbrace{\sigma(x)}_{= \sigma * x} \neq x$

Déf. Soit $x \in E$. L'orbite de x est le sous-ensemble

$$Gx = G * x = \{g * x \mid g \in G\} \subseteq E$$

Déf. L'action de G sur E est transitive s'il existe $x \in E$ tq $Gx = E$.

<u>Exemple</u>. S_n agit transitivement sur $\{1, \dots, n\}$. On a même

$$S_n 1 = \{1, \dots, n\}$$

S_n n'agit pas transitivement sur $\mathcal{P}(\{1, \dots, n\})$

$$S_n \emptyset = \{\emptyset\} \neq \mathcal{P}(\{1, \dots, n\})$$
(si $n \neq 0$)

<u>Déf</u> Si $F \subseteq E$, F est G-<u>stable</u> si $\forall g \in G \ \forall x \in F \ \ gx \in F$
si on note

$$GF = \{ gx \mid g \in G, x \in F\} \subseteq E,$$

F est G-stable si $GF \subseteq F$

<u>Prop</u>. Toute orbite est stable

<u>Démo</u>. (exo)

<u>Exo</u> Mq un sous-ensemble stable est une réunion d'orbites

<u>Prop</u>. Soit $x \in E$ et $g \in G$

$$G_{gx} = g G_x g^{-1}$$

<u>Démo</u> $\supseteq$: Soit $h \in G_x$ i.e. $hx = x$.
On a alors

$$(ghg^{-1})(gx) = g(h(g^{-1}g))x$$
$$= g(hx) = gx, \text{ i.e. } ghg^{-1} \in G_{gx}.$$

$\subseteq$: Soit $h \in G_{gx}$

On montre que $h \in gG_x g^{-1}$

c-à-d, $h = gkg^{-1}$ où $k \in G_x$.

Soit $k = g^{-1}hg \in G$

On a bien $gkg^{-1} = gg^{-1}hgg^{-1} = h$.

Montrons que $k \in G_x$:

$$kx = g^{-1}hgx = g^{-1}gx = x$$

D'où $k \in G_x$ $\boxed{}$

Exo Obtenir la deuxième inclusion à partir de la première en utilisant que $x = g^{-1}(gx)$.

<u>Remarque</u>. si x et $y \in E$ appartiennent à une même orbite de E, leurs stabilisateurs sont conjugués dans G.

<u>Rappel</u> $H, K \leq G$

H et K sont <u>conjugués</u> dans G s'il existe $g \in G$ tq $H = gKg^{-1}$

<u>Prop</u> Soit E un G-ensemble. E est réunion disjointe de ses orbites, i.e.

$\forall x, y \in E$ si $Gx \neq Gy$ alors
$$Gx \cap Gy = \emptyset$$

<u>Démo</u>. (exo)

La proposition précédente dit que l'ensemble des orbites de E constituent une partition de E. Elles donnent donc lieu à une relation d'équivalence sur E :

$$x \sim y \iff Gx = Gy$$

le quotient $E/_\sim$ est noté $E/_G$ (ou plutôt ${}_G\backslash E$ car l'action est à gauche).

$${}_G\backslash E = \{ Gx \mid x \in E \}$$

On note souvent par

$$\begin{aligned} \pi : E &\longrightarrow {}_G\backslash E \\ x &\longmapsto Gx \end{aligned}$$

l'application quotient.

<u>Prop.</u> Si G agit librement sur E alors

$$|E| = |G| \times |{}_G\backslash E| .$$

<u>Démo</u> (exo dans le cas $|G|$ et $|E|$ finis. Indication : si $x \in E$ l'application ensembliste

$$\begin{aligned} f : G &\longrightarrow Gx \\ g &\longmapsto gx \end{aligned}$$

est une bijection)

Théorème (la formule des orbites)

Soit E un G-ensemble fini, où G est un groupe fini. Soient $X_1, \dots, X_r$ les orbites de E. Soit $x_i \in X_i$, $i = 1, \dots, r$. Alors

$$|E| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}.$$

Démo. La seule chose à démontrer est que

$$|Gx| = \frac{|G|}{|G_x|}.$$

Soit
$$\begin{aligned} f : G &\longrightarrow Gx \\ g &\longmapsto gx \end{aligned}$$

On a

$$\begin{aligned} f(g) = f(h) &\iff gx = hx \\ &\iff h^{-1}gx = x \\ &\iff h^{-1}g \in G_x \\ &\iff g \in hG_x \end{aligned}$$

f induit donc une bijection

$$\begin{aligned} \bar{f} : G/G_x &\longrightarrow Gx \\ \bar{g} &\longmapsto gx \end{aligned}$$

Or, $|G/G_x| = |G|/|G_x|$ ☒