Groupes diédraux

Table des matières

Dans cette partie, nous allons étudier un type particulier de groupes : les groupes diédraux.

1 Définition

Soit n un entier supérieur ou égal à 3.

On se place dans le plan complexe et on considère le polygone régulier à n côtés P_n formé par les racines n^{ièmes} de l'unité $e^{\frac{2ik\pi}{n}}$, k=0, ... , n-1.

Proposition 1.0.1 *L'ensemble des isométries affines de $\mathbb{C} \cong \mathbb{R}^2$ opère sur $\mathbb{C}^n$ via l'opération f.(x_1, ... ,x_n)=(f(x_1), ... ,f(x_n)).*

Démonstration *Immédiate.* $\diamondsuit$

Définition *On appelle groupe diédral de degré n et on note D_n, le stabilisateur de $\{e^{\frac{2ik\pi}{n}}$, k=0, ... , n-1$\}$ pour l'opération définie dans la Proposition précédente.*

Le groupe diédral de degré n n'est autre que l'ensemble des isométries affines telles que l'image de P_n est P_n.

Toute isométrie conservant P_n fixe le point O par conservation des distances.
Il suffit donc de considérer les isométries vectorielles autrement dit $O_2(\mathbb{R})$.

2 Caractérisation de D_n

Soit n un entier supérieur ou égal à 3.

Proposition 2.0.2 *D_n contient un sous-groupe cyclique d'ordre 2.*

Démonstration *On vérifie facilement que la réflexion s d'axe (OI) avec I d'affixe 1 appartient à D_n. s est d'ordre 2 donc <s> est un sous-groupe cyclique d'ordre 2 de D_n.* $\diamondsuit$

Proposition 2.0.3 *D_n contient un sous-groupe cyclique d'ordre n.*

Démonstration *Les rotations r(O,$\frac{2ik\pi}{n}$) de centre O et de rayon $\frac{2k\pi}{n}$, k=0, ... , n-1, appartiennent à D_n.*
Ces rotations auxquelles on ajoute l'identité, forment un sous-groupe cyclique de D_n d'ordre n, engendré par la rotation r(O,$\frac{2\pi}{n}$). $\diamondsuit$

On pose s=s(OI), la réflexion d'axe (OI) avec I d'affixe 1 et r=r(O,$\frac{2\pi}{n}$), la rotation de centre O et d'angle $\frac{2\pi}{n}$.
On a montré que s et r appartiennent à D_n.

Proposition 2.0.4 *s∘r∘s∘r=Id.*

Démonstration *Montrons que s∘r∘s=r^{-1} :*
r^{-1} est la rotation de centre O et de rayon $\frac{-2\pi}{n}$.
det s∘r∘s=det r=1 donc s∘r∘s est une isométrie directe de $\mathbb{R}^2$ c'est à dire une rotation.
s∘r∘s(O)=O donc s∘r∘s est de centre O.
s∘r∘s(I)=s(r(I)) est le point d'affixe $e^{-2\pi n}$ donc s∘r∘s est une rotation de centre O et d'angle $\frac{-2\pi}{n}$ c'est à dire s∘r∘s=r^{-1}. ♢

Proposition 2.0.5 *D_n est engendré par s et r.*

Démonstration *On pose A_0=I et pour k compris entre 1 et n-1, on définit A_k comme le point d'affixe $e^{\frac{2k\pi}{n}}$.*
Soit f appartenant à D_n.
f étant une isométrie de $\mathbb{R}^2$ ayant au moins un point fixe (le point O), f est soit une rotation soit une réflexion.
Si il existe k compris entre 0 et n-1 tel que f(A_k)=A_k alors O et A_k sont des points fixes pour f donc f est la réflexion d'axe (OA_k).
s∘r^{n-2k}(A_k)=s(A_{n-k})=A_k donc O et A_k sont des points fixes pour s∘r^{n-2k}.
D'où, s∘r^{n-2k}=f et f∈<$\{s, r\}$>.
Supposons que f(A_k)≠ A_k pour tout k compris entre 0 et n-1.
Supposons que f est une rotation.
Soient k et m compris entre 0 et n-1 tels que f(A_k)=A_m.
Alors, l'angle de f est égal à $(\overrightarrow{OA}_k,\overrightarrow{OA}_m)=\arg \frac{e^{\frac{2ik\pi}{n}}}{e^{\frac{2im\pi}{n}}}=\frac{2i(k-m)\pi}{n}$.
D'où, f=r^{k-m} ∈<$\{s, r\}$>.
Supposons maintenant que f est une réflexion d'axe Δ. O appartient à Δ.
f appartenant à D_n, il existe k compris entre 0 et n-1 tel que Δ coupe [A_k,A_{k+1}] en son milieu (où on pose $A_n = A_0$ si k=n).
Montrons que f=s∘r^{n-2k-1} :
det(s∘r^{n-2k-1})=det(s)det(r^{n-2k-1})=-1.1=-1 donc s∘r^{n-2k-1} est une réflexion.
s∘r^{n-2k-1}(A_k)=s(A_{n-k-1})=A_{k+1} donc l'axe de s∘r^{n-2k-1} passe par le milieu de [A_k,A_{k+1}].
Puisque s∘r^{n-2k-1} appartient à D_n, O appartient à l'axe de s∘r^{n-2k-1}.
D'où, l'axe de s∘r^{n-2k-1} est Δ et f=s∘r^{n-2k-1} ∈<$\{s, r\}$>.
Tout élément de D_n appartient à <$\{s, r\}$> donc D_n ⊂<$\{s, r\}$>.
Puisque s et r appartiennent à D_n, <$\{s, r\}$>⊂ D_n et par conséquent, D_n=<$\{s, r\}$>.
♢

D_n est donc un groupe engendré par deux éléments s et r vérifiant : s est d'ordre 2, r est d'ordre n et s∘r∘s∘r=Id.

3 Etude de D_n

Soit n un entier supérieur ou égal à 3.

D'après les résultats de la Section précédente, on a la proposition suivante :

Proposition 3.0.6 *Tout groupe engendré par deux éléments a et b tels que :*
1)a est d'ordre 2,
2)b est d'ordre n et
3)abab=1,
est isomorphe à D_n.

Pour étudier D_n, on va donc se placer dans le cadre défini par la Proposition précédente.

3.1 Eléments de D_n

Propriété 3.1.1 D_n *n'est pas abélien.*

Démonstration *Puisque abab=1, on a $abab^{-1}=b^{-2}$.*
b^{-2} est différent de 1 car b est d'ordre n>2 donc $abab^{-1}$ est différent de 1.
D'où, a étant d'ordre 2, $(ab)(ba)^{-1}=abab^{-1}$ est différent de 1 et par conséquent, ab est différent de ba. D_n n'est ainsi pas abélien. $\diamondsuit$

La propriété suivante nous sera très utile :

Propriété 3.1.2 *Pour tout entier k compris entre 1 et n-1, $ab^ka = b^{-k}$.*

Démonstration *Nous allons procéder par récurrence sur k (compris entre 1 et n) :*
Cas k=1 : abab=1 donc $aba=b^{-1}$.
Supposons que la propriété est vraie pour jusqu'à l'entier k-1.
Alors,

$$\begin{aligned}
ab^ka &= ab^{k-1}ba \\
&= ab^{k-1}aaba \text{ car a est d'ordre 2} \\
&= b^{1-k}b^{-1} \text{ par hypothse de rcurrence} \\
&= b^{-k}.
\end{aligned}$$

$\diamondsuit$

Proposition 3.1.3 *a n'est pas une puissance de b.*

Démonstration *Supposons qu'il existe un entier k compris entre 1 et n-1 tel que* $a=b^k$. *Alors,* $abab=b^{2k+2}=b^{2k}b^2$.
Comme $a=b^k$ *est d'ordre 2,* $b^{2k}=1$. *D'où,* $abab=b^2$.
Comme $abab=1$, *on en déduit que* $b^2=1$.
Par conséquent, b est d'ordre au plus 2 ce qui est impossible puisque b est d'ordre $n>2$.
$\diamondsuit$

Proposition 3.1.4 $D_n = \{1,\ a,\ b,\ \ldots\ ,b^{n-1},\ ab,\ \ldots\ ,\ ab^{n-1}\}$.

Démonstration *Comme a n'est pas une puissance de b,* D_n *contient les éléments distincts :* $1,\ a,\ b,\ \ldots\ ,\ b^{n-1}$.
Si k et m sont deux entiers distincts compris entre 1 et n-1 alors $ab^k \neq ab^m$.
D'où, puisque b est d'ordre n et comme a n'est pas une puissance de b, D_n *contient les éléments* $1,\ a,\ b,\ \ldots\ ,\ b^{n-1},\ ab,\ \ldots\ ,\ ab^{n-1}$.
Soit x un élément de D_n.
Comme D_n *est engendré par a et b, x s'écrit sous la forme* $a^{m_1}b^{k_1}\ \ldots\ a^{m_r}b^{k_r}$ *avec, pour tout i compris entre 1 et r,* $m_i=0$ *ou 1 et* k_i *compris entre 0 et n-1.*
D'après la Propriété 3.1.2 et puisque $a=a^{-1}$ *(a d'ordre 2),* $b^k a = ab^{-k}$ *pour tout entier k compris entre 1 et n-1.*
D'où, on peut ramener l'écriture de x à une écriture de la forme $a^k b^m$ *avec k=0 ou 1 et m compris entre 0 et n-1.*
Par suite, $D_n = \{1,\ a,\ b,\ \ldots\ ,b^{n-1},\ ab,\ \ldots\ ,\ ab^{n-1}\}$. $\diamondsuit$

Corollaire 3.1.5 D_n *est d'ordre 2n.*

3.2 Sous-groupe normaux de D_n

Proposition 3.2.1 $<b>$ *est un sous-groupe normal de* D_n.

Démonstration *L'ordre de* $<b>$ *est n donc l'indice de* $<b>$ *dans* D_n *est* $[D_n :<b>] = \frac{|D_n|}{|<b>|}=2$. *On en déduit que* $<b>$ *est normal dans* D_n
(cf Cours Sous-groupes normaux*).* $\diamondsuit$

Proposition 3.2.2 D_n *est le produit semi-direct de* $<b>$ *par* $<a>$.

Démonstration *On a montré dans la Proposition précédente que* $<b>$ *est normal dans* D_n *et on a montré dans la Proposition 3.1.3 que* $<b>\cap<a>=\{1\}$.
Comme l'ordre de $<b><a>$ *est* $\frac{|<b><a>|}{|<b>\cap<a>|}$ *(cf Cours* Produit semi-direct*), on a* $|<b><a>| = \frac{2n}{1} = 2n = |D_n|$ *et par conséquent,* $<b><a>=D_n$.
D'où, D_n *est le produit semi-direct de* $<b>$ *par* $<a>$ $\diamondsuit$

D'après la Propriété 3.1.2, on définit un homomorphisme α du groupe <a> dans le groupe Aut(<b>) en posant $\alpha(1)$=Id et $\alpha(a)(b^k)=ab^ka^{-1}=ab^ka=b^{-k}$.

Proposition 3.2.3 *D_n est isomorphe au produit semi-direct $<b>\rtimes_\alpha<a>$.*

Démonstration *Si on pose $N=<b>\times\{1\}$ et $H=<a>\times\{1\}$ alors $<b>\rtimes_\alpha<a>$ est le produit semi-direct de N par H (cf Cours* Produit semi-direct*).*
Montrons que le produit semi-direct de <b> par <a> dans D_n est isomorphe au produit semi-direct de N par H dans $<b>\rtimes_\alpha<a>$: à b^ka^m on associe $f(b^ka^m)=(b^k,1)(1,a^m)$, $0\leq k\leq n-1$, $m\in\{0, 1\}$. f est clairement bijective.
Soient $0\leq k,r\leq n-1$, $m,s\in\{0, 1\}$.
<b> étant normal dans D_n, on a $a^mb^ra^{-m}\in<b>$ donc
$f(b^ma^kb^ra^s)=f((b^ka^mb^ra^{-m})(a^ma^s))=(b^ka^mb^ra^{-m},1)(1,a^ma^s)$.
Puisqu'on utilise la loi du produit semi-direct (cf Cours Produit semi-direct*), on a*
$f(b^ka^m)f(b^ra^s)=(b^k,1)(1,a^m)(b^r,1)(1,a^s)=(b^k\alpha(1)(1),1a^m)\ (b^r\alpha(1)(1),1a^s)=(b^k,a^m)(b^r,a^s)$
$=(b^k\alpha(a^m)(b^r),a^ma^s)=\ (b^ka^mb^ra^{-m},a^ma^s)$.
D'où, f est un isomorphisme entre les produits directs de sous-groupes $<b>\rtimes<a>$ et $H\rtimes K$.
Or d'après la Proposition précédente, le produit semi-direct $<b>\rtimes<a>$ est égal à D_n donc D_n est isomorphe à $<b>\rtimes_\alpha<a>$. ♢

Corollaire 3.2.4 *D_n est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes_\gamma\mathbb{Z}/2\mathbb{Z}$.*

Démonstration *<b> est un groupe cyclique d'ordre n donc <b> est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De même, <a> est un groupe cyclique d'ordre 2 donc <a> est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. D'où, le produit semi-direct $<b>\rtimes_\alpha<a>$ est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes_\gamma\mathbb{Z}/2\mathbb{Z}$ où γ est défini de $\mathbb{Z}/2\mathbb{Z}$ dans Aut($\mathbb{Z}/n\mathbb{Z}$) par $\gamma(\overline{0})$=Id et $\gamma(\overline{1})(\widetilde{m})=-\widetilde{m}$ (cf Cours* Produit semi-direct*).*
Puisque D_n est isomorphe au produit semi-direct $<b>\rtimes_\alpha<a>$, D_n est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes_\gamma\mathbb{Z}/2\mathbb{Z}$. ♢

Propriété 3.2.5 *Quel que soit k compris entre 0 et n-1, $bab^kb^{-1}=ab^{k-2}$.*

Démonstration *Puisque abab=1 et a est d'ordre 2, on a $ba=ab^{-1}$.*
D'où, $bab^kb^{-1}=ab^{-1}b^{k-1}=ab^{k-2}$. ♢

Proposition 3.2.6 *1)Si n est impair alors les sous-groupes normaux de D_n sont D_n et les sous-groupes de <b>.*
2)Si n est pair alors les sous-groupes normaux de D_n sont D_n, les sous-groupes de <b>, le sous-groupe engendré par b^2 et a et le sous-groupe engendré par b^2 et ab.

Démonstration *$<b>$ étant cyclique, les sous-groupes de $<b>$ sont des groupes cycliques. Soit k compris entre 1 et n-1.*
Montrons que $<b^k>$ est un sous-groupe normal de D_n :
$<b^k>$ est un sous-groupe normal de $<b>$. Soit i compris entre 0 et n-1.
D'après la Propriété 3.1.2, $ab^ib^k(ab^i)^{-1}=ab^ka=b^{-k} \in <b^k>$.
D'où, $<b^k>$ est un sous-groupe normal de D_n pour tout k compris entre 1 et n-1.
Soit N un sous-groupe normal de D_n non inclus dans $<b>$.
Il existe alors, d'après la Proposition 3.1.4, un entier k compris entre 0 et n-1 tel que $ab^k \in N$. Alors, d'après la Propriété précédente, N contient ab^{k-2}, élément différent de 1 d'après la Proposition 3.1.3. D'où, N contient l'élément $ab^{k-2}ab^k=b^2$ et par conséquent, N contient le groupe $<b^2>$.
1)Si n est impair alors pgcd(2,n)=1 et par conséquent, $<b^2>=<b>$ (cf Cours Congruence*)*
N est ainsi d'ordre au moins égal à n+1. Or $|N|$ divise $|D_n|$ c'est à dire 2n donc $|N|$=2n et par suite, $N=D_n$.
Les seuls sous-groupes normaux de D_n, lorsque n est impair, sont D_n et les sous-groupes de $<b>$.
2)Supposons n pair.
Pour tout i compris entre 1 et $\frac{n}{2}$-1, $ab^kb^{2i}=ab^{k+2i}$ et d'après la Propriété 3.1.2,
$b^{2i}ab^k=aab^{2i}ab^k=ab^{k-2i}=ab^{k+n-2i}=ab^{k+2(\frac{n}{2}-i)}$ donc $<\{b^2, ab^k\}>$ est constitué des éléments b^{2i} et ab^{k+2i}, i=0, ... , $\frac{n}{2}$-1.
Ainsi, $<\{b^2, ab^k\}>$ est d'ordre n et donc $<\{b^2, ab^k\}>$ est d'indice 2 dans D_n.
On en déduit que $<\{b^2, ab^k\}>$ est un sous-groupe normal de D_n (cf Cours Sous-groupes normaux*).*
Comme ab^k et b^2 appartiennent à N, N contient $<\{b^2, ab^k\}>$.
D'où, N possède au moins n éléments.
Or $|N|$ divise D_n=2n donc $|N|$=n c'est à dire $<\{ab^k, b^2\}>$ ou $|N|$=2n c'est à dire $N=D_n$.
Il reste à déterminer l'ensemble des groupes de la forme $<\{b^2, ab^k\}>$.
On a vu que $<\{b^2, ab^k\}>$ est constitué des éléments b^{2i} et ab^{k+2i}, i=0, ... , $\frac{n}{2}$-1 donc $<\{b^2, ab^k\}>=<\{b^2, ab^m\}>$ dès que m-k est pair.
On en déduit qu'il y a deux sous-groupes de la forme $<\{b^2, ab^k\}>$: $<\{b^2, a\}>$ et $<\{b^2, ab\}>$.
Les sous-groupes normaux de D_n, lorsque n est pair, sont D_n, les sous-groupes de $<b>$, le sous-groupe $<\{b^2, a\}>$ et le sous-groupe $<\{b^2, ab\}>$. $\diamondsuit$

Etudions maintenant deux sous-groupes associés à un groupe donné : le centre et le groupe dérivé.

3.3 Centre et groupe dérivé de D_n

Proposition 3.3.1 *1)Si n est impair alors $Z(D_n)=\{Id\}$.*
2)Si n est pair alors $Z(D_n)=\{Id, b^{\frac{n}{2}}\}$.

Démonstration *Soit k compris entre 1 et n-1.*
D'après la Propriété 3.1.2, $ab^k(b^ka)^{-1}=ab^kab^{-k}=b^{-2k}$

Si n est impair ou si n est pair et k est différent de $\frac{n}{2}$ alors b^{-2k} est différent de 1. On a alors $ab^k \neq b^k a$ et donc $b^k \notin Z(D_n)$.
1)Si n est impair alors, puisque $Z(D_n)$ est un sous-groupe normal de D_n, $Z(D_n)$ est un sous-groupe de $<b>$ d'après la Proposition 3.2.6.
Or chacun de ces sous-groupes, hormis $\{1\}$, possède une puissance non nulle de b donc il ne peut être inclus dans $Z(D_n)$ d'après ce qui précède. D'où, $Z(D_n)=\{Id\}$.
2)Il est clair que $b^{\frac{n}{2}}$ commute avec toute puissance de b.
De plus, $(b^{\frac{n}{2}})^2=b^n=1$ donc $b^{\frac{n}{2}}=b^{-\frac{n}{2}}$.
Pour tout k compris entre 0 et n-1, $ab^k b^{\frac{n}{2}}=ab^{\frac{n}{2}+k}$ et d'après la Propriété 3.1.2, $b^{\frac{n}{2}}ab^k=aab^{\frac{n}{2}}ab^k=ab^{-\frac{n}{2}}b^k=ab^{\frac{n}{2}}b^k=\ ab^{\frac{n}{2}+k}$. D'où, $b^{\frac{n}{2}}$ appartient à $Z(D_n)$.
On a vu que si k est différent de $\frac{n}{2}$ alors b^k n'appartient pas à $Z(D_n)$.
Comme $abab=1$, on a $ab=b^{-1}a\neq ba$ donc a n'appartient pas à $Z(D_n)$.
De plus, $aab=b$ et $aba=b^{-}1 \neq b$ donc ab n'appartient pas non plus à D_n.
D'où, puisque $Z(D_n)$ est un sous-groupe normal de D_n, $Z(D_n)=\{1,\ b^{\frac{n}{2}}\}$ d'après la Proposition 3.2.6. $\diamondsuit$

Proposition 3.3.2 *1)Si n est impair alors $D(D_n)=<b>$.*
2)Si n est pair alors $D(D_n)=<b^2>$.

Démonstration *Pour tout couple (i,j) d'entiers compris entre 0 et n-1, on a, en utilisant la Propriété 3.1.2, $[b^i,b^j]=b^ib^jb^{-i}b^{-j}=1$, $[ab^i,b^j]=ab^ib^jb^{-i}ab^{-j}=ab^jab^{-j}=b^{-2j}$, $[b^j,ab^i]=([ab^i,b^j])^{-1}=b^{2j}$ et $[ab^i,ab^j]=ab^iab^jb^{-i}ab^{-j}a=b^{-i}b^jb^{-i}b^j=1$.*
D'où, puisque $D(D_n)$ est engendré par les commutateurs, $D(D_n)$ est inclus dans $<b^2>$.
Comme $[a,b^{-1}]=ab^{-1}ab=b^2$, $<b^2>$ est inclus dans $D(D_n)$. D'où, $D(D_n)=<b^2>$.
Lorsque n est impair, pgcd(2,n)=1 donc $<b^2>=<b>$ (cf Cours Congruence*).* $\diamondsuit$

Corollaire 3.3.3 *Le groupe D_n est résoluble.*

Démonstration *$<b>$ et $<b^2>$ étant cycliques donc abéliens, on a $D(<b>)=D(<b^2>)=\{1\}$.*
D'où, $D^2(D_n)=D(D(D_n))=\{1\}$ et D_n est donc résoluble. $\diamondsuit$