Notes pour le cours de “L2: Groupes et géométrie”

Reda Chhaibi [1]

2 février 2016

1. reda.chhaibi@math.univ-toulouse.fr

Table des matières

1 Eléments de théorie des groupes (30h) 5
1.1 Groupes, sous-groupes . . . 5
1.1.1 Lois internes, associativité et commutativité . . . 5
1.1.2 Groupes . . . 6
1.1.3 Sous-groupes . . . 8
1.2 Morphismes . . . 8
1.2.1 Noyaux et injectivité . . . 9
1.2.2 Exemples . . . 10
1.3 Une excursion en arithmétique . . . 10
1.3.1 PGCD, PPCM . . . 11
1.3.2 Bézout et lemme de Gauss reformulés . . . 11
1.3.3 Congruences . . . 12
1.4 Parties génératrices . . . 13
1.5 Le groupe symétrique . . . 13

2 Géométrie du plan (30h) 15

Préambule

Il s'agit simplement d'un document de résumé des notions abordées en cours. Il ne s'agit aucunement d'un polycopié. Une référence complète utilisée en cours est le livre de CALVI.

Au programme, nous ne sommes pas supposés aborder la notion de groupe quotient ainsi que la relation d'équivalence qui lui est associée. Pourtant ce choix me forcerai à un certain nombre de contorsions. J'irai donc à l'encontre de ce choix de programme.

Chapitre 1

Eléments de théorie des groupes (30h)

1.1 Groupes, sous-groupes

1.1.1 Lois internes, associativité et commutativité

Afin de définir la notion de groupe, il est nécessaire de se placer dans un cadre abstrait qui formalise bon nombre des opérations que vous connaissez déjà.

Définition 1.1.1 (Loi interne)**.** *Soit E un ensemble. Une loi interne $*$ sur E est une application $* : E \times E \to E$. L'image de $(a, b) \in E \times E$ par E sera notée $a * b$.*

De façon générale, un ensemble E muni d'une opération interne $*$ sera noté $(E, *)$.

Comme l'indique cette dénomination, une loi interne permet de fabriquer un élément de E à partir de deux autres éléments donnés. Dans le but de généraliser les opérations d'addition $+$, de multiplication $\times$ ou de produit extérieur $\wedge$, la notation classique $*(a, b)$ parait très inadaptée et peu pratique pour les calculs. L'utilisation de parenthèse permet d'indiquer l'ordre dans lequel se font les calculs. Par exemple, l'écriture $(a * (b * c)) * d$ signifie que l'on commence par composer b et c dans la loi interne $*$. Le résultat est alors composé avec a *à gauche*. Ce dernier est lui-même composé *à droite* par d.

Deux propriétés clés peuvent être vérifiées par une loi interne :

(i) Associativité : $*$ est dite associative lorsque :

$$\forall a, b, c \in E \times E \times E,\ (a * b) * c = a * (b * c)$$

(ii) Commutativité : $*$ est dite commutative lorsque :

$$\forall a, b \in E \times E,\ a * b = b * a$$

Ainsi, pour une loi associative, les parenthèses peuvent être déplacées et donnent toujours le même résultat. Ainsi $a * b * c$ donne un résultat sans ambiguité. Pour reprendre l'exemple précédent, si $*$ est associative, il est possible d'oublier les parenthèses et simplement écrire

$$(a * (b * c)) * d = a * b * c * d\ .$$

Dans le cadre de ce cours, toutes les lois internes que nous rencontrerons seront associatives. Cette hypothèse n'est à affaiblir que dans le cas improbable où nous

étudierons les octonions. A contrario, l'hypothèse de commutativité fera souvent défaut. Un exemple non-commutatif connu est celui des matrices $(M_n(\mathbb{R}), \times)$. Par exemple :

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Définition 1.1.2 (Elément neutre)**.** *Soit $*$ une loi interne sur un ensemble E. Nous dirons qu'un élément $e \in E$ est un élément neutre lorsque pour tout $a \in E$, $a * e = e * a = a$.*

Par exemple 0 est neutre pour la lois additive dans $(\mathbb{R}, +)$ (ou $(\mathbb{C}, +)$), alors que 1 est neutre pour la loi multiplicative dans $(\mathbb{R}^*, \times)$. Remarquez l'utilisation de l'article indéfini dans la désignation d'"un élément neutre". En fait, nous pouvons utiliser l'article défini et parler de **l'élément neutre** d'une loi interne :

Théorème 1.1.3 (Unicité de l'élément neutre)**.** *Une loi interne admet au plus un élément neutre.*

Démonstration. Supposons que e et e' soient des éléments neutres. En utilisant la définition d'être un élément neutre pour e, on a d'une part $e * e' = e$. D'autre part, la définition appliquée à e' donne $e * e' = e'$. La conjonction des deux égalités donne $e = e'$. □

1.1.2 Groupes

La notion de groupe est une notion essentielle en mathématiques. Il a fallu cependant beaucoup de temps pour qu'elle se dégage comme une notion permettant de formuler des problèmes mathématiques dans tous les domaines.

Définition 1.1.4 (Groupe)**.** *Un ensemble $(G, *)$ muni d'une loi interne est un groupe lorsque*

- *La loi $*$ est associative et admet un élément neutre e_G. S'il n'y a pas d'ambiguité sur le choix de neutre, ce dernier sera simplement désigné par la lettre e.*
- *Pour tout $x \in G$, il existe un élément $y \in G$, dit symétrique ou inverse, tel que*

$$x * y = y * x = e_G$$

- *Si le groupe est commutatif, il est alors dit abélien.*

De la même façon que pour l'unicité de l'élément neutre, nous avons :

Théorème 1.1.5 (Unicité de l'inverse)**.** *Dans un groupe, tout élément admet un unique inverse.*

Démonstration. Supposons que y et y' soient inverse d'un élément $x \in G$. Nous avons alors la quadruple égalité :

$$x * y = y * x = x * y' = y' * x = e \ .$$

Ainsi :

$$\begin{array}{lcc} \Rightarrow & y' * (x * y) = y' & \text{(Multiplication à gauche par } y') \\ \Rightarrow & (y' * x) * y = y' & \text{(Associativité)} \\ \Rightarrow & e * y = y' & \text{(4e égalité)} \\ \Rightarrow & y = y' & \text{(Définition du neutre)} \end{array}$$

□

Maintenant que nous sommes certains de l'unicité de l'inverse dans un groupe, une notation spécifique peut lui être associée. L'unique élément symétrique de $x \in G$ sera noté x^{-1} en général.

Propriétés 1.1.6. *1. L'élément neutre est son propre symétrique.* $e = e^{-1}$.

2. *L'inverse à gauche est l'inverse à droite. Si* $x * y = e$ *alors* $y * x = e$ *et donc* $y = x^{-1}$. *(Et vice-versa).*
3. $\left(x^{-1}\right)^{-1} = x$ *pour tout* $x \in G$.
4. *L'inverse d'un produit est le produit inverse des inverses. Pour tout* x, x' *dans* G, *on a :*
$$\left(x * x'\right)^{-1} = x'^{-1} * x^{-1}$$
5. *Plus généralement, pour* $g_1, g_2, \ldots, g_m$ *éléments dans le groupe :*
$$(g_1 * g_2 * \cdots * g_m)^{-1} = g_m^{-1} * \cdots * g_1^{-1}$$

Il est très utile de démontrer ses propriétés afin de s'habituer aux manipulations formelles des groupes.

Exercice 1.1.7. *Démontrer ces propriétés.*

Exemples 1.1.8. *1. L'ensemble des entiers relatifs* $(\mathbb{Z}, +)$ *est un groupe muni de l'addition habituelle. L'élément neutre est le* 0. *L'inverse au sens de l'opération de groupe est l'opposé habituel. Il en est de même pour* $(\mathbb{R}, +)$ *ou* $(\mathbb{R}, +)$. *Il s'agit de groupes abéliens infinis.*

2. *Le cercle unité* $(U, \times)$. *Vu comme sous-ensemble de* $\mathbb{C}$ *des nombres complexes de module* 1, *le cercle unité est muni de l'opération de multiplication. L'élément neutre est l'unité* 1. *L'inverse d'un élément est son inverse au sens habituel de la multiplication sur* $\mathbb{C}$. *Remarquons que le fait d'avoir une loi interne repose sur l'identité* $|zz'| = |z||z'|$ *pour deux nombres complexes* z *et* z'. *Ainsi, le produit de deux nombres de modules* 1 *est de module* 1. *Il s'agit d'un groupe abélien infini.*
3. *Les racines n-ièmes de l'unité* $(U_n, \times)$. *Ici :*
$$U_n := \left\{ e^{\frac{i2\pi}{n}},\ k = 0, 1, 2, \ldots, n-1 \right\}$$
L'élément neutre est toujours l'unité. Il s'agit d'un groupe abélien. Dans ce cas, de la même façon que nous dressions des tableaux de multiplication en école élémentaire, il est possible de donner une description complète de la loi de groupe.
4. *Le groupe linéaire* $GL_n(\mathbb{K})$ *pour* $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$ *ou* $\mathbb{Q}$.
$$GL_n(\mathbb{K}) := \{A \in M_n(\mathbb{K}) \mid \det A \neq 0\}$$
L'élément neutre est la matrice identité id. *Rappelons que le produit de matrices est associatif et que le calcul ne saute pas aux yeux ! Aussi la formule de Laplace donne une expression de l'inverse d'une matrice* $x \in M_n(\mathbb{K})$ *dès que* $\det x \neq 0$. *Elle stipule que :*
$$A^{-1} = \frac{{}^t com(A)}{\det A}$$

où $com(A)$ est la comatrice de A i.e la matrice des cofacteurs. Si la formule de Laplace n'est que d'un intérêt pratique très limité, elle a l'avantage de prouver que l'inverse existe bien et qu'il s'agit d'une matrice à coefficients dans $\mathbb{K}$. Enfin, notons que le groupe linéaire est un groupe infini non-abélien dès que $n > 1$.

5. *Produit direct de deux groupes. Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. Une loi interne $*$ est définie sur le produit ensembliste $G_1 \times G_2$ par :*

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1,\ x_2 *_2 y_2)$$

pour tout $(x_1, y_1, x_2, y_2) \in G_1 \times G_1 \times G_2 \times G_2$. L'élément neutre est $e_{G_1 \times G_2} = (e_{G_1}, e_{G_2})$. On peut vérifier que le produit direct de deux groupes abéliens est abéliens.

1.1.3 Sous-groupes

Il sera fréquent de construire des groupes à partir d'autres groupes. Dans ce cas, il y a moins d'axiomes à vérifier.

Définition 1.1.9 (Sous-groupes)**.** *Soit $(G, *)$ un groupe. Un sous-ensemble $H \subset G$ non-vide est dit, sous-groupe de G, lorsque :*
- *Pour tout $x, y \in H$, $x * y \in H$.*
- *Pour tout $x \in H$, $x^{-1} \in H$.*

Naturellement, comme nous pourrions nous en douter :

Théorème 1.1.10. *Un sous-groupe est un groupe.*

Démonstration. Soit G un groupe et H un sous-groupe. Grâce au premier axiome de la définition 1.1.9, H est laissé stable par la loi $*$. Ainsi la loi interne de G restreinte à H est une loi interne pour H. Par restriction, le neutre de G est neutre pour H. Le deuxième axiome de la définition 1.1.9 permet de s'assurer que l'inverse d'un $x \in G$ est dans H. □

Seulement, les axiomes formant la définition d'un sous-groupe peuvent être rassemblés en un seul, ce qui donne une caractérisation plus rapidement vérifiable.

Proposition 1.1.11. *Soit $H \subset G$ non-vide. H est un sous-groupe de G si et seulement si pour toute paire $(x, y) \in H \times H$, $x * y^{-1} \in H$.*

Démonstration. ($\Rightarrow$) Il suffit d'appliquer le premier axiome de la définition 1.1.9 avec y^{-1} à la place de y. Le deuxième axiome nous assure que $y^{-1} \in H$.

($\Leftarrow$) Comme H est non-vide, il existe au moins un élément $h \in H$. Par application de l'hypothèse de départ, $e_G = h * h^{-1} \in H$. Ainsi pour tout $y \in H$, $y^{-1} = e_G * y^{-1} \in G$. Le deuxième axiome est vérifié. Le premier suit. □

1.2 Morphismes

Un homomorphisme de groupes, ou plus simplement un morphisme de groupes est une application qui préserve la structure de groupe. Plus formellement :

Définition 1.2.1 (Homomorphisme de groupes)**.** *Soient $(G, *)$ et $(G', \circ)$ deux groupes. Une application $f : G \to G'$ est qualifiée de morphisme de groupe lorsque*

$$\forall a, b \in G \times G,\ f(a * b) = f(a) \circ f(b)\ .$$

L'ensemble des morphismes de G dans G' est noté $\mathrm{Hom}(G, G')$*.*

On parle d'endomorphisme si le groupe d'arrivée est identique à celui de départ et on note $\mathrm{End}(G) = \mathrm{Hom}(G, G')$. Un morphisme de groupes bijectif est qualifié d'isomorphisme. Un isomorphisme de G dans lui-même est appelé un automorphisme. On a $\mathrm{Aut}(G) \subset \mathrm{End}(G)$.

Exercice 1.2.2.
- $\mathrm{Hom}(G, G')$ *n'est jamais vide.*
- *Si $f \in \mathrm{Hom}(G, G')$ et $g \in \mathrm{Hom}(G', G'')$ alors $g \circ f \in \mathrm{Hom}(G, G'')$.*
- *Si $f \in \mathrm{Hom}(G, G')$ est un isomorphisme, alors l'application réciproque f^{-1} est aussi un isomorphisme de groupes.*

Quelques résultats structurels viennent comme application de la définition. On dit communément que les morphismes "respectent les lois de groupe".

Théorème 1.2.3. *Soient $(G, *)$ et $(G', \circ)$ deux groupes. Considérons un morphisme $f \in \mathrm{Hom}(G, G')$.*
- *L'image de l'élément neutre par un morphisme est nécessairement l'élément neutre du groupe d'arrivée.*
$$f(e_G) = e_{G'}$$
- *L'image de l'inverse d'un élément par un morphisme est nécessairement l'inverse de l'image de cet élément :*
$$\forall x \in G,\ f(x^{-1}) = f(x)^{-1}$$

Démonstration. Pour le premier point, le fait que $e_G = e_G * e_G$ combiné au fait que f respecte la loi de groupe dans la définition entraîne que :

$$e_{G'} = f(e_G) \circ f(e_G)^{-1} = f(e_G * e_G) \circ f(e_G)^{-1} = f(e_G) \circ f(e_G) \circ f(e_G)^{-1} = f(e_G)\ .$$

Pour le second point, nous avons un calcul similaire :

$$e_{G'} = f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1})\ ,$$

à l'issue duquel nous reconnaissons la caractérisation de l'inverse de $f(x)$. □

1.2.1 Noyaux et injectivité

Grâce à la structure de groupe, la propriété d'injectivité est particulièrement liée à une nouvelle notion.

Définition 1.2.4 (Noyau)**.** *Le noyau d'un morphisme de groupes $\varphi : (G, *) \to (G', \circ)$ est l'ensemble*

$$\ker \varphi = \{g \in G,\ \varphi(g) = e_{G'}\}$$

Théorème 1.2.5. *Le noyau est un sous-groupe du groupe de départ.*

Démonstration. Puisque $\ker\varphi \neq \emptyset$, il suffit de vérifier que pour tout $x, y \in \ker\varphi$, on a $x * y^{-1} \in \ker\varphi$. Celà se vérifie aisément :

$$\varphi\left(x * y^{-1}\right) = \varphi(x) \circ \varphi(y^{-1}) = \varphi(x) \circ \varphi(y)^{-1} = e_{G'} \circ e_{G'}^{-1} = e_{G'}$$

□

Une propriété importante du noyau est la suivante. Si $g \in G$ et $x \in \ker\varphi$ alors le conjugué de x par g est dans le noyau : $g * x * g^{-1} \in \ker\varphi$.

Démonstration.

$$\begin{aligned}\varphi\left(g * x * g^{-1}\right) &= \varphi(g) \circ \varphi(x) \circ \varphi\left(g^{-1}\right) \\ &= \varphi(g) \circ \varphi(x) \circ \varphi(g)^{-1} \\ &= \varphi(g) \circ e_{G'} \circ \varphi(g)^{-1} \\ &= \varphi(g) \circ \varphi(g)^{-1} \\ &= e_{G'}\end{aligned}$$

□

Si H est un sous-groupe de G vérifiant cette propriété, on parle de sous-groupe distingué ou normal, ce qui est noté $H \triangleleft G$.

1.2.2 Exemples

— Exponentielle et logarithme.
— Exponentielle imaginaire.
— Le déterminant.
— Les automorphismes intérieurs.
— L'application puissance.

1.3 Une excursion en arithmétique

Avant de reprendre étude théorique et systématique de concepts de théorie de groupes, prenons le temps de revisiter des notions connues. L'arithmétique peut être décrite comme l'étude des intéractions entre la structure additive des entiers et leur structure multiplicative. De ce point de vue, il s'agit de comprendre comment les deux groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}^*, \times)$ dialoguent, ainsi que leurs sous-groupes. Nous allons maintenant formaliser certaines notions d'arithmétique, connues au niveau L2, dans un langage de théorie des groupes.

Remarquons d'abord que la relation de divisibilité "a divise b" s'exprime comme "$b \in a\mathbb{Z}$". De plus, les ensembles de la forme $a\mathbb{Z}$ jouent un rôle particulier. Celà apparait dans le lemme suivant.

Lemme 1.3.1 (Structure des sous-groupes de $(\mathbb{Z}, +)$)**.** *Un sous-groupe de $(\mathbb{Z}, +)$ est nécessairement de la forme $n\mathbb{Z}$ où a est un entier naturel.*

Démonstration. Cf. Feuille de TD1. □

Exercice 1.3.2. *Sous quelle condition $a\mathbb{Z}$ est-il un sous-groupe de $b\mathbb{Z}$?*

Ce lemme indique qu'un sous-groupe de $\mathbb{Z}$ est engendré par un seul élément. On parle de groupe *monogène* . Notons qu'à la fois a et $-a$ sont générateurs, et qu'il n'y a pas unicité des générateurs. Une écriture possible est $a\mathbb{Z} = \langle a \rangle$, que nous revisiterons plus tard.

1.3.1 PGCD, PPCM

Le plus grand diviseur commun de deux entiers relatifs est noté $a \wedge b$, alors que le plus petit commun multiple est noté $a \vee b$.

Théorème 1.3.3 (Théorème et définition PGCD/PPCM)**.** *Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Alors $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$. En fait :*

$$a\mathbb{Z} + b\mathbb{Z} = a \wedge b\mathbb{Z}$$

$$a\mathbb{Z} \cap b\mathbb{Z} = a \vee b\mathbb{Z}$$

Démonstration. D'abord il est facile de se convaincre qu'il s'agit bien de sous-groupes : Les stabilités par somme et par inverse (au sens du groupe) sont immédiates. Ensuite, le lemme 1.3.1 sur la structure des sous-groupes de $\mathbb{Z}$ nous indique $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont monogènes et donc nécessairement de la forme $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Il ne reste plus qu'à reconnaitre les deux entiers naturels d et m.

- D'une part, $d = au + bv$ pour un certain couple (u, v) d'entiers relatifs. Or $a \wedge b$ divise toute combinaison linéaire de a et de b donc $a \wedge b$ divise d et $a \wedge b \leq d$. De la même façon, par l'identité de Bezout, il existe un autre couple (w, z) tel que $a \wedge b = aw + bz \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Ainsi d divise $a \wedge b$ et $d \leq a \wedge b$. Nous déduisons de la double inégalité que $d = a \wedge b$.

- D'autre part, les éléments de $a\mathbb{Z} \cap b\mathbb{Z}$ sont exactement les multiples communs de a et b. Cet ensemble est un groupe, et le plus petit entier non nul au sens de la valeur absolue est le générateur m mais aussi le PPCM ! □

Le théorème précédent est la "bonne définition" de la notion de PGCD et PPCM. Il permet de plus d'intuiter assez facilement les "bonnes définitions" pour le PGCD et le PPCM de n entiers $a_1, \dots a_n$.

Exercice 1.3.4. *Prouver que le PGCD et le PPCM de n entiers $a_1, \dots a_n$ au sens usuel sont les entiers naturels générateurs des groupes :*

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$$

$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} \ .$$

1.3.2 Bézout et lemme de Gauss reformulés

La partie du théorème 1.3.3 concernant le PGCD est en fait une reformulation de l'identité de Bézout. Rappelons que l'identité de Bézout affirme que si $(a, b) \in \mathbb{Z}^2$, alors il existe $(u, v) \in \mathbb{Z}^2$:

$$au + bv = a \wedge b \ .$$

Pour obtenir cette identité, il suffit de remarquer que dans le théorème 1.3.3 donne $a \wedge b \in a\mathbb{Z} + b\mathbb{Z}$.

Un autre lemme classique est le lemme de Gauss :

Lemme 1.3.5 (Lemme de Gauss classique)**.** *Soient a, b et c trois entiers naturels non nuls. Si a divise bc et $a \wedge b = 1$ alors a divise c.*

Si nous prenons la peine de le reformuler dans la même logique que précédemment, nous obtenons :

Lemme 1.3.6 (Lemme de Gauss reformulé)**.** *Si $bc \in a\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ alors $c \in a\mathbb{Z}$.*

Démonstration.

$$c \in c\mathbb{Z} = c\,(a\mathbb{Z} + b\mathbb{Z}) = ac\mathbb{Z} + bc\mathbb{Z} \subset ac\mathbb{Z} + a\mathbb{Z} = a\mathbb{Z}$$

□

Exercice 1.3.7. *Reconnaitre en filigrane une preuve plus conventionnelle du lemme de Gauss, qui utilise l'identité de Bézout.*

1.3.3 Congruences

Soit $m \in \mathbb{N}$ un entier naturel. Deux entiers a et b sont congrus modulo m lorsque m divise $a - b$ ou, de façon équivalente, $a - b \in m\mathbb{Z}$. Nous notons $a \equiv b \mod m$.

Rappelons que la relation de congruence modulo m est une relation d'équivalence sur les entiers $\mathbb{Z}$. Afin de vérifier qu'il s'agit d'une relation d'équivalence, il faut vérifier les axiomes :

(R) Réflexivité :

$$a \equiv a \mod m$$

(S) Symétrie :

$$a \equiv b \mod m \Leftrightarrow b \equiv a \mod m$$

(T) Transitivité :

$$(a \equiv b \mod m, b \equiv c \mod m) \Rightarrow b \equiv a \mod m$$

Si en général, les relations d'équivalence ne sont pas reliées à des groupes, la relation de congruence l'est. Il suffit de se souvenir que la congruence s'exprime comme l'appartenance à $m\mathbb{Z}$, qui est un groupe. Aussi, les axiomes RST qui font de la relation de congruence une relation d'équivalence sont les axiomes de groupe de $m\mathbb{Z}$ déguisés. En effet, (R) découle de $0 \in m\mathbb{Z}$, (S) découle de la stabilité de $m\mathbb{Z}$ par passage à l'opposé alors que (T) est une reformulation de la stabilité par somme de m. Nous reviendrons plus en détail sur de telles relations d'équivalences issues d'un sous-groupe.

Pour le moment, contentons nous de remarquer qu'en identifiant les entiers modulo m, c'est-à-dire qu'en ne travaillant qu'avec les restes $\{0, 1, \ldots, m-1\}$, nous avons un groupe muni de la loi $+$. Ce groupe est noté $\mathbb{Z}/m\mathbb{Z}$ - lire $\mathbb{Z}$ quotienté par la relation d'équivalence définie par $n\mathbb{Z}$. Ce groupe n'est autre que le groupe des racines m-ièmes de l'unité déjà rencontré en auparavant, avec une loi notée multiplicativement.

1.4 Parties génératrices

Nous avons déjà rencontré en TD des groupes monogènes ou encore, des groupes cycliques. Rappelons qu'un groupe est dit monogène s'il est engendré par un seul élément, et cyclique s'il est de plus fini. Dans cette section, nous nous intéresserons à une étude plus systématique de ce que "être engendré par" signifie.

Un premier théorème général :

Théorème 1.4.1. *Soit $(G, *)$ un groupe et $\mathcal{F}$ une famille non-vide de sous-groupes de G. Si*

$$I = \cap_{H \in \mathcal{F}} H$$

est un sous-groupe de G. Autrement dit, une intersection quelconque de sous-groupes est un groupe.

Démonstration. Il suffit de vérifier le critère de sous-groupe. I est bien stable par inverse et bien stable par produit. □

Ce dernier permet de définir abstraitement un sous-groupe engendré par une partie $A \subset G$ *non-vide.*

Définition 1.4.2 (Groupe engendré)**.** *Le sous-groupe engendré par A est*

$$\langle A \rangle = \cap_{A \subset H, H \text{ sous-groupe de } G} H \ .$$

De plus, c'est le plus petit sous-groupe de G (au sens de l'inclusion) contenant A

Démonstration. Par le théorème 1.4.1, $\langle A \rangle$ est bien un sous-groupe de G comme intersection d'une famille quelconque de sous-groupes. Cette famille est non-vide car contenant au moins le groupe G tout entier.

Afin de voir qu'il s'agit du plus petit, il suffit de constater que tout sous-groupe I contenant A apparaîtra dans l'intersection et donc $\langle A \rangle \subset I$. □

Exercice 1.4.3. *Illustrer le théorème dans le cas de $\mathbb{Z}$ tout en listant les sous-groupes apparaissant dans l'intersection :*

$$\langle m \rangle = \cap_{m \in H, H \text{ sous-groupe de } \mathbb{Z}} H$$

Définition 1.4.4. *Un sous-groupe H de G est dit monogène s'il est engendré par un seul élément i.e $H = \langle a \rangle$.*

Si de plus H est fini, on dit que H est cyclique.

1.5 Le groupe symétrique

Le groupe symétrique (définition, cardinal, cycles, décomposition en produit de cycles, signature). Définition du groupe alterné. En exercice, recherche de diverses familles de générateurs.

Chapitre 2

Géométrie du plan (30h)

1. Le plan affine euclidien / le plan complexe. Objets géométriques fondamentaux (points droites, segment, polygones, cercles, repères, barycentres, coordonnées barycentriques convexité). Pas de définition d'un espace affine abstrait. Le plan affine euclidien est $\mathbb{R}^2$ muni de la norme euclidienne usuelle. Dans tous les cas, on fera une double présentation réel / complexe en insistant particulièrement sur la présentation complexe. 4h 2. Transformations affines. Effets sur les objets géométriques fondamentaux. Applications. Groupe des homothéties-translations. Inversions, homographies. 6H 3. Isométries, classifications des isométries, générateurs des groupes d'isométries, applications (dont le groupe diédral). 10h. 4. Formes quadratiques et coniques 10h