NOTES D'ALGÈBRE ABSTRAITE

enseigné par

meral tosun

département de mathématiques
l'université galatasaray

rédigé par
abdullah uyu
oneofvalts@sdf.org

le 23 février 2022

table des matières

chapitre 1

introduction

1.1 comprendre les groupes intuitivement

lecture 1, february 23[rd] 2022

un petit peu d'histoire. une motivation pour géométrie algébrique. ce lecture est le dernière avant les class plus avancés, comme géométrie algébrique. les mathématiciens italians, les équations cubiques.

continuing in english. 16. & 17. century italian mathematicians. we review relations, equivalence relations, equivalence classes. *les classes d'équivalence forment une partition de* E.

homework 1.1.1. montrer que, pour chaque partition de E il existe une relation d'équivalence dont les classes sont les élément de cette partition de E.

m. macauley has a nice website. **pattern** is an important keyword. we start the articulation with *axe de symmétrie*. we consider regular polygons like triangles, rectangles, hexagons etc. one can classify those regarding the parity of the number of the edges. pay attention to the definition of d_A. rotations are simple though. or, are they? anyways, now think about the compositions of those operations. this is like adding all numbers. behold that in this case, we have finite amount of *numbers*. we mention *fermeture de l'opération* et la *table de cayley*.

homework 1.1.2. read about cayley.

there are three conditions for being a cayley table. we call this above structure a group and specifically D_3. we now mention *générateur*.

homework 1.1.3. write down the cayley table and the graph for square and pentagon groups. give two sets of generators for each of them.

homework 1.1.4. montrer que la table de multiplication pour l'ensemble

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

muni de l'opération

$$[a] + [b] = [a+b]$$

vérifie les propriétés d'un groupe.

after-class, february 24[th] 2022

solution (1.1.1). soient E un ensemble, P un partition de E. posons la relation R comme suit :

$$R = \{(a, b) : a, b \in P'; P' \in P\}$$

par construction, R est réflexive, symétrique et transitive. alors c'est une relation d'équivalence.

soient $P' \in P$ et $a \in P'$. par construction, $[a] = P'$. $\Diamond$

solution (1.1.2). a lawyer... his collected papers took 967 pages?! he apparently appreciated novel-reading and architecture.

solution (1.1.4). notons d'abord la table de multiplication pour $\mathbb{Z}_n$.

	0	1	2	$\dots$	$n-2$	$n-1$
0	$\boxed{0}$	1	2	$\cdots$	$n-2$	$n-1$
1	1	2	3	$\cdots$	$n-1$	$\boxed{0}$
2	2	3	4	$\cdots$	$\boxed{0}$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$n-2$	$n-2$	$n-1$	$\boxed{0}$	$\cdots$	$n-4$	$n-3$
$n-1$	$n-1$	$\boxed{0}$	1	$\cdots$	$n-3$	$n-2$

figure 1.1 – table de cayley pour $\mathbb{Z}_n$.

par la progession arithmétique dans les lignes et colonnes, on voit qu'elles contiennent l'ensemble

$$\{0, 1, 2, \dots, n-1\}$$

en différents ordres. (*composition interne*)

elles toutes contient donc l'élément '0', en différentes positions verticales. (*l'existence d'élément neutre, et d'inverse*) pour *associativité*, on doit agir algébriquement, car ce ne pas impliqué par la table de cayley.

soit $[a], [b], [c] \in \mathbb{Z}_n$. on a :

$$\begin{aligned} ([a]+[b])+[c] = [a+b]+[c] \qquad & = \\ = [a+b+c] & \\ = [a]+[b+c] & \\ = [a]+([b]+[c]) & \end{aligned}$$

en vérifiant ces quatre condition, on a montré que $(\mathbb{Z}_n, +)$ est un groupe. $\Diamond$

solution (1.1.3). commençons avec D_4.

	1	r	r^2	r^3	H	V	D_R	D_L
1	1	r	r^2	r^3	H	V	D_R	D_L
r	r	r^2	r^3	1	D_R	D_L	V	H
r^2	r^2	r^3	1	r	V	H	D_L	D_R
r^3	r^3	1	r	r^2	D_L	D_R	H	V
H	H	D_L	V	D_R	1	r^2	r^3	r
V	V	D_R	H	D_L	r^2	1	r	r^3
D_R	D_R	H	D_L	V	r	r^3	1	r^2
D_L	D_L	V	D_R	H	r^3	r	r^2	1

figure 1.2 – table de cayley pour D_4.

notons que $r \circ r = r^2, r \circ r^2 = r^3, r \circ r^3 = 1, r \circ H = D_R$, $r \circ D_R = V, r \circ V = D_L$. donc, $\langle r, H \rangle$ est une générateur pour D_4. mais similairement, $\langle r, V \rangle$ l'est aussi. traçons la graph de cayley pour le générateur $\langle r, H \rangle$.

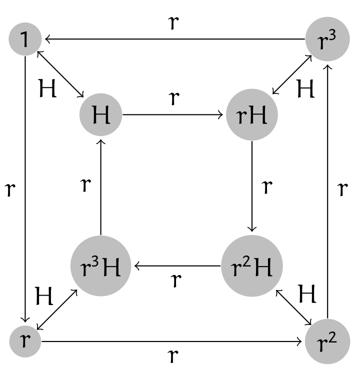

figure 1.3 – table de cayley pour D_4, $\langle r, H \rangle$.

on considère maintenant D_5.

	1	r	r^2	r^3	r^4	U	U_L	U_R	D_L	D_R
1	1	r	r^2	r^3	r^4	U	U_L	U_R	D_L	D_R
r	r	r^2	r^3	r^4	1	D_R	U_R	D_L	U	U_L
r^2	r^2	r^3	r^4	1	r	U_L	D_L	U	D_R	U_R
r^3	r^3	r^4	1	r	r^2	U_R	U	D_R	U_L	D_L
r^4	r^4	1	r	r^2	r^3	D_L	D_R	U_L	U_R	U
U	U	D_L	U_R	U_L	D_R	1	r^3	r^2	r	r^4
U_L	U_L	D_R	U	D_L	U_R	r^2	1	r^4	r^3	r
U_R	U_R	U_L	D_R	U	D_L	r^3	r	1	r^4	r^2
D_L	D_L	U_R	U_L	D_R	U	r^4	r^2	r	1	r^3
D_R	D_R	U	D_L	U_R	U_L	r	r^4	r^3	r^2	1

figure 1.4 – table de cayley pour D_5.

notons que $r \circ r = r^2, r \circ r^2 = r^3, r \circ r^3 = r^4$, $r \circ r^4 = 1, r \circ U = D_R, r \circ D_R = U_L, r \circ U_L = U_R$, $r \circ U_R = D_L$. donc, $\langle r, U \rangle$ est une générateur. mais similairement, $\langle r, U_L \rangle$ l'est aussi. traçons la graph de cayley pour le générateur $\langle r, U \rangle$.

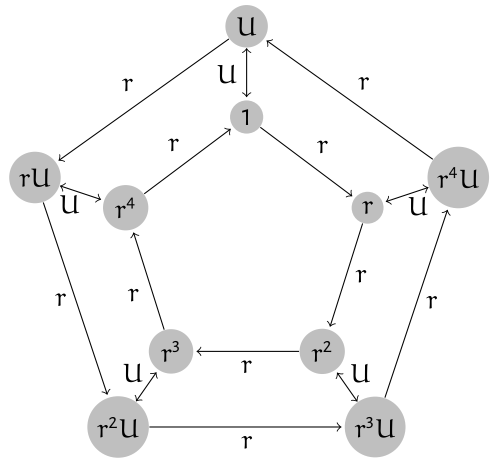

figure 1.5 – table de cayley pour D_5, $\langle r, U \rangle$.

1.2 passage à un définition plus formelle

lecture 2, march 2nd 2022

note. some parts are missing here. find and type them.

définition 1.2.1 (élément neutre). $(E, \star)$ admet un élément neutre si $\exists e \in E, \forall a \in E, a \star e = e \star a = a$.

définition 1.2.2 (inversibilité). on dit que $a \in E$ est inversible si $\exists b \in E$ tel que $a \star b = e$. on le note par $a^{-1} = b$. (notons que $b \star a = e$ n'est pas toujours le cas.)

exemple 1.2.1.

— $(\mathbb{Z}, +)$, $a \in \mathbb{Z}$, l'inverse additif $a^{-1} = -a \in \mathbb{Z}$

— $(\mathbb{Q}^*, \cdot)$, $a \in \mathbb{Q}^*$, l'inverse multiplicatif $a^{-1} = \frac{1}{a} \in \mathbb{Q}^*$

— $(GL_n(\mathbb{R}), \cdot)$, pour $n = 2$ par example

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

définition 1.2.3. soit $(E, \star)$ un monoïde. si tous les éléments dans E sont inversibles, on dit que $(E, \star)$ est un groupe.

the older definition of a group. un groupe est une ensemble des rototations, réflexions d'un n-gone régulier.

exemple 1.2.2.

— $(\mathbb{N}, +)$ est un non-example. peut-être le plus *simple*.

— $(\mathbb{Z}, \star)$ est un non-example.

— $(\mathbb{Z}, +)$ et $(\mathbb{Q}^\star, \cdot)$ **est** un groupe.

homework 1.2.1. read about abel.

définition 1.2.4 (abélien). un groupe $(E, \star)$ est dit abélien si $\star$ est commutatif.

exemple 1.2.3.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}^\star, \cdot)$ sont des groupes abéliens.
- $(GL_n(\mathbb{R}), \cdot)$ n'est pas un groupe abélien.
- $(M_n(\mathbb{R}), +)$ est un groupe abélien.
- $(GL_n(\mathbb{R}), +)$ n'est pas un groupe.

notons que $(M_n(\mathbb{R}))^\star = GL_n(\mathbb{R})$. $\star$ est pour donc exclure les éléments qui n'a pas d'inverse.

exemple 1.2.4. $\mathbb{Z}_n$ (ou on note quelque fois $\mathbb{Z}/n\mathbb{Z}$). notons explicitement :

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{1.1}$$
$$a \sim b \iff a \equiv b \mod n \tag{1.2}$$

ceci est un ensemble important pour ce cours et en fait est un groupe.

after-class, march 3rd 2022

solution. about the classification of groups of order 4,5,..., i have asked for help in `chat.se` and got help from ted. *the strategy is to think about the possible orders for elements of the group and perform an organized case analysis.*

in that journey, find that there is no group that has an element of order 3, and that there is only one group that has an element of order 2 and 4, each. in fact, the one that has an element of order 4 is $\mathbb{Z}_4$.

exercice 1.2.1 (suggested by *lukas heger* from `chat.se`)**.** if in a group G, we have for all $a \in G : a^2 = e$, then $\forall a, b \in G : ab = ba$, i.e. the cayley table is symmetric.

solution. soit $a, b \in G$. notons d'abord que :

- par la loi de composition interne, $ba \in G$.
- par la supposition, $a^2 = b^2 = (ba)^2 = e$.

alors, on a :

$$\begin{aligned} ab &= abbaba \quad ((ba)^2 = e) \\ &= aaba \quad (b^2 = e) \\ &= ba \quad (a^2 = e) \end{aligned}$$

$\Diamond$

lecture 3, march 9th 2022

définition 1.2.5 (ordre d'un élément)**.** G un groupe fini, $g \in G$. on note ord $g = n$ si $g^n = e_G$ et n est le plus petit.

exemple 1.2.5. pour le groupe diédrale D_n, on note la rotation r et le symétrie d. on a :

- ord $r = n$
- ord $d = 2$
- $drd^{-1} = r^{-1}$

exemple 1.2.6. classifions D_n :

- pour $n = 1$, $D_1 = \{e, d\}$
- pour $n = 2$, $D_2 = \{e, r, d, rd\}$
- $(D_n, \circ)$ est non-abélien pour $n \geqslant 3$.
- $(D_1, \circ)$ est abélien, $|D_1| = 2$. $D_1 \cong \mathbb{Z}_2$
- $(D_2, \circ)$ est abélien d'ordre 4.

proposition 1.2.1. *soit $n \geqslant 1$. les propriétés suivantes sont équivalentes :*

- *$(G, \cdot)$ est isomorphe à D_n.*
- *$|G| = 2n$ et $\exists\, g_1, g_2 \in G$ tel que $|g_1| = n$, $|g_2| = 2$,*

$$g_2 \times g_1 \times g_2^{-1} = g_1^{-1}$$

et $g_2 \notin \langle g_1 \rangle$ si $n = 2$.

exemple 1.2.7 (groupes des matrices)**.**

- $M_n(\mathbb{R})$, l'ensemble des matrices $n \times n$ à coefficients dans $\mathbb{R}$.
- $GL_n(\mathbb{R})$, groupe linéaire générale, l'ensemble des matrices $n \times n$ dont $\det A \neq 0$.
- $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$ et on note similairement $SL_n(\mathbb{Z})$. le groupe linéaire spécial.
- $O(n) = \{A \in M_n(\mathbb{R}) : AA^t = \mathrm{Id}_n\}$, groupe orthogonal.

exemple 1.2.8. soit $\mathbb{H}$ l'ensemble des matrices 2×2 à coefficients dans $\mathbb{C}$ qui sont de la forme

$$\begin{bmatrix} u & v \\ -\bar{v} & \bar{u} \end{bmatrix}$$

$u, v \in \mathbb{C}$.

$$\mathbb{H} = \{A \in M_2(\mathbb{C}) : A \begin{bmatrix} u & v \\ -\bar{v} & \bar{u} \end{bmatrix}\}$$

les éléments de $\mathbb{H}$ sont appelés les quaternions.

$$i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, ij = k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

notons que $i^2 = j^2 = k^2 = ijk = -\mathrm{Id} = -1$. donc, en reécrit :

$$\mathbb{H} = \{\mathrm{Id}, -\mathrm{Id}, i, j, k, -i, -j, -k\}$$

et de même, ord $\mathbb{H} = 8$.

- ord $\mathrm{Id} = 1$
- ord i = ord j = ord $k = 4$
- ord $-\mathrm{Id} = 2$
- est-ce que $(\mathbb{H}, \cdot)$ un groupe ?
- le groupe $(\mathbb{H}, \cdot)$ n'est pas abélien car $ij = ji$

note. remplir la table de cayley de $\mathbb{H}$.

1.3 groupe des permutations

définition 1.3.1 (permutation)**.** soit E un ensemble non-vide. S_E : l'ensemble des bijections de E dans E (appelé *permutations de* E.)

théorème 1.3.1 (groupe des permutations)**.** $(S_E, \circ)$ *est un groupe.*

démonstration. notons d'abord que :

- $\circ$ est un opération binaire.
- $f \circ (g \circ h) = (f \circ g) \circ h$
- $\mathrm{Id} = e = \begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{bmatrix}$
- $f \in S_E \implies f^{-1} \in S_E$.

□

exemple 1.3.1.

- $E = \emptyset \implies S_E = \{\mathrm{Id}\}$ groupe trivial.
- $E = \{a\} \implies S_E = \{\mathrm{Id}\}$ groupe trivial.
- $E = \{a, b\} \implies S_E = \{\begin{bmatrix} a & b \\ a & b \end{bmatrix}, \begin{bmatrix} a & b \\ b & a \end{bmatrix}\}$. ord $S_E = 2$. groupe abélien d'ordre 2, qui est isomorphe à $(\mathbb{Z}_2, +)$.

en générale, on note $(S_n, \circ)$ le groupe de permutations où $E = \{1, \ldots, n\}$. bien sûr, $|S_n| = n!$.

homework 1.3.1. S_n n'est pas abélien pour $n \geqslant 3$. montrer que S_3 n'est pas abélien par trouvant deux élément $a, b \in S_3$ tel que $ab \neq ba$.

définition 1.3.2 (point fix, Fix, Supp)**.** un *point fix* d'une permutation σ est une point $x \in E$ tel que $\sigma(x) = x$. notons Fix (σ) l'ensemble des points fixes de σ. définissons similairement *support* de σ tel que $E \setminus$ Fix (σ) et notons-le Supp (σ).

note. on note σ avec ces points fixs.

note. i missed the definition of a *cycle*. insert it here.

définition 1.3.3 (transposition)**.** un 2-cycle est dit une *transposition*.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 2 & 4 & 7 & 9 & 8 & 5 & 6 & 1 \end{pmatrix}$$

$= (1\,3\,2\,10)(5\,7\,8)(6\,9)$ produit des cycles.

note. change `bmatrix`'s to `pmatrix`.

exemple 1.3.2.

- Id...
- transpositions...
- 3-cycles...
- 4-cycles...

note. fill the example above.

proposition 1.3.1.

- *un cycle de longueur l peut s'écrire comme le produit de $l - 1$ transpositions.*
- *toute permutations de E sont des produits des transpositions.*

définition 1.3.4 (inversion)**.** une *inversion* de σ est une paire (i, j) vérifiant $i < j$ et $\sigma(i) > \sigma(j)$.

définition 1.3.5 (signature)**.** sign $(\sigma) = (-1)^{\mathcal{S}}$ où $\mathcal{S}$ est le nombre d'inversion de σ.

remarque 1.3.1. la signature d'une transposition est -1.

définition 1.3.6 (parité)**.** une permutation est

- paire si sign $(\sigma) = 1$.
- impaire si sign $(\sigma) = -1$.

proposition 1.3.2. *l'ensemble des permutation paires, noté $\mathcal{A}_n$ est un groupe.*

homework 1.3.2. until friday,

- prove the proposition above.
- write down two generators for S_3 and S_4. generalize.

1.4 morphisme des groupes

soit $(G_1, \star)$ et $(G_2, \square)$ deux groupes. on appele *morphisme* de groupes de G_1 dans G_2 une application $\varphi : G_1 \to G_2$ telle que

$$\forall g_1, g_1' \in G_1 \varphi(g_1 \star g_1') = \varphi(g_1) \square \varphi(g_1').$$

- *morphisme des groupes* ou *homomorphisme*.
- si $G_1 = G_2$, alors, on appele φ un *endomorphisme*.
- un homomorphisme bijectif est dit *isomorphisme*.
- si $\varphi : G_1 \to G_2$ est un isomorphisme, alors c'est un automorphisme.

proposition 1.4.1. $\varphi : G_1 \to G_2$ *un homomorphisme. alors,* $\varphi(e_1) = e_2$.

proposition 1.4.2. *homomorphisme preserves inverses.*

proposition 1.4.3. *homomorphisme preserves orders.*

homework 1.4.1. prove the propositions above.

exemple 1.4.1. find homomorphisms for the following two mappings.

- $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto a + 1$.
- $\varphi : M_2(\mathbb{R}) \to \mathbb{R}$