HAX501X – Groupes et anneaux 1

CM13 16/11/2023

Clément Dupont

Retour sur des exercices du cours

Exercice 58
Écrire les tables de multiplication des groupes diédraux D_3 et D_4.

On écrit les produits "ligne $\circ$ colonne". Pour $D_3 = \{\mathrm{id}, r, r^2, s_0, s_1, s_2\}$:

$\circ$	id	r	r^2	s_0	s_1	s_2
id	id	r	r^2	s_0	s_1	s_2
r	r	r^2	id	s_1	s_2	s_0
r^2	r^2	id	r	s_2	s_0	s_1
s_0	s_0	s_2	s_1	id	r^2	r
s_1	s_1	s_0	s_2	r	id	r^2
s_2	s_2	s_1	s_0	r^2	r	id

Pour $D_4 = \{\mathrm{id}, r, r^2, r^3, s_0, s_1, s_2, s_3\}$:

$\circ$	id	r	r^2	r^3	s_0	s_1	s_2	s_3
id	id	r	r^2	r^3	s_0	s_1	s_2	s_3
r	r	r^3	r^3	id	s_1	s_2	s_3	s_0
r^2	r^2	r^3	id	r	s_2	s_3	s_0	s_1
r^3	r^3	id	r	r^2	s_3	s_0	s_1	s_2
s_0	s_0	s_3	s_2	s_1	id	r^3	r^2	r
s_1	s_1	s_0	s_3	s_2	r	id	r^3	r^2
s_2	s_2	s_1	s_0	s_3	r^2	r	id	r^3
s_3	s_3	s_2	s_1	s_0	r^3	r^2	r	id

Exercice 59

Démontrer que les groupes D_3 et $\mathfrak{S}_3$ sont isomorphes.

- Première approche : comparer les tables de multiplication pour trouver un isomorphisme de groupes entre D_3 et $\mathfrak{S}_3$. Vu que r est d'ordre 3, on a envie de le faire correspondre au 3-cycle $(1\,2\,3)$. Donc

$$r \longleftrightarrow (1\,2\,3) \quad \text{et} \quad r^2 \longleftrightarrow (1\,2\,3)^2 = (1\,3\,2).$$

On choisit, pour voir, de faire correspondre (il y a d'autres choix possibles)

$$s_0 \longleftrightarrow (2\,3).$$

Vu que $rs_0 = s_1$, on n'a pas le choix et on doit faire correspondre

$$s_1 \longleftrightarrow (1\,2\,3)(2\,3) = (1\,2).$$

Vu que $s_0 r = s_2$, on n'a pas le choix et on doit faire correspondre

$$s_2 \longleftrightarrow (2\,3)(1\,2\,3) = (1\,3).$$

On vérifie, grâce aux tables de multiplication, que la bijection $D_3 \longleftrightarrow \mathfrak{S}_3$ ainsi définie est bien un isomorphisme de groupes.

- Deuxième approche : voir l'exercice 16 de la feuille de TD 3, où l'on définit un morphisme de groupes $D_n \to \mathfrak{S}_n$, qui est injectif.

  Pour $n = 3$, ce morphisme est bijectif car $|D_3| = |\mathfrak{S}_3| = 6$.

Exercice 60

Montrer que l'élément neutre 1_A est unique.

Si on a un autre élément neutre $1'_A$ alors on a, en utilisant que les deux sont des éléments neutres :

$$1_A = 1_A \times 1'_A = 1'_A.$$

Exercice 61

Soit $(A, +, \times)$ un anneau.

- Montrer qu'on a $x \times 0_A = 0_A = 0_A \times x$ pour tout $x \in A$.
- Montrer qu'on a $(-x) \times y = -(x \times y) = x \times (-y)$ pour tous $x, y \in A$.
- Montrer qu'on a $(-1_A) \times x = -x = x \times (-1_A)$ pour tout $x \in A$.

- On calcule :

$$x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A.$$

  En simplifiant (pour la loi $+$) par $x \times 0_A$ on obtient : $x \times 0_A = 0_A$. De même dans l'autre sens : $0_A \times x = 0_A$.

- On calcule :

$$(-x) \times y + x \times y = (-x + x) \times y = 0_A \times y = 0_A.$$

  Et donc $(-x) \times y$ est l'opposé de $x \times y$: $-(x \times y) = (-x) \times y$. De même dans l'autre sens : $-(x \times y) = x \times (-y)$.

- Cas particulier du précédent.

Exercice 62

Soit $(A, +, \times)$ un anneau. Montrer que si $0_A = 1_A$ alors $A = \{0_A\}$ est l'anneau nul.

Si $0_A = 1_A$ alors pour tout $x \in A$ on a :

$$x \times 0_A = x \times 1_A$$

et donc $x = 0_A$. Donc $A = \{0_A\}$.

Exercice 63

Pour les exemples d'anneaux A qu'on vient de voir, déterminer les groupes des inversibles $A^\times$.

- On a déjà rencontré $\mathbb{Z}^\times = \{-1, 1\}$, et $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{C}^\times = \mathbb{C}^*$.
- On a déjà rencontré $(\mathbb{Z}/n\mathbb{Z})^\times$.
- On a $\mathbb{R}[X]^\times = \mathbb{R}^*$, l'ensemble des polynômes constants non nuls.
- On a $\left(\mathbb{R}^{\mathbb{N}}\right)^\times = (\mathbb{R}^*)^{\mathbb{N}}$, l'ensemble des suites dont tous les termes sont non nuls.
- On a $\left(\mathbb{R}^{\mathbb{R}}\right)^\times = (\mathbb{R}^*)^{\mathbb{R}}$, l'ensemble des fonctions qui ne s'annulent jamais.
- On a déjà rencontre $\mathrm{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$, et $\mathrm{End}(V)^\times = \mathrm{Aut}(V)$.

Exercice 65

Montrer que dans un anneau intègre on peut simplifier pour la multiplication, c'est-à-dire : si $ax = ay$ alors $a = 0$ ou $x = y$.

Si $ax = ay$ alors $a(x - y) = 0$ et donc $a = 0$ ou $x - y = 0$, d'où la conclusion.

Exercice 66
Montrer que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$.

Soit A un sous-anneau de $\mathbb{Z}$. Alors $1 \in A$, et donc comme A est un sous-groupe de $\mathbb{Z}$, on a forcément $A = \mathbb{Z}$.

Exercice 67
Montrer que la composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Exercice 68
Montrer que si $A \simeq B$ et $B \simeq C$ alors $A \simeq C$.

Facile !

Exercice 69

Soient A et B deux anneaux qui sont isomorphes.

1) Montrer que si A est commutatif alors B est commutatif.

Comme A et B sont isomorphes, il existe un isomorphisme d'anneaux $f : A \to B$. On suppose que A est commutatif et on montre que B est commutatif.

Soient $y, y' \in B$. Comme f est surjectif, il existe $x, x' \in A$ tels que $y = f(x)$ et $y' = f(x')$. Alors, en utilisant le fait que f est un morphisme d'anneaux et le fait que A est commutatif :

$$yy' = f(x)f(x') = f(xx') = f(x'x) = f(x')f(x) = y'y.$$

Exercice 69

2) Montrer que si A est intègre alors B est intègre.

Comme A et B sont isomorphes, il existe un isomorphisme d'anneaux $f : A \to B$. On suppose que A est intègre et on montre que B est intègre. Par le point précédent, vu que A est commutatif, B l'est aussi. De plus, si $A \neq \{0_A\}$ alors $B \neq \{0_B\}$.

Soient $y, y' \in B$ et supposons que $yy' = 0_B$. Comme f est surjectif, il existe $x, x' \in A$ tels que $y = f(x)$ et $y' = f(x')$. On a alors

$$f(xx') = f(x)f(x') = yy' = 0_B.$$

Comme f est injectif, on en déduit que $xx' = 0_A$ et donc que $x = 0_A$ ou $x' = 0_A$ car A est intègre. Donc $y = f(0_A) = 0_B$ ou $y' = f(0_A) = 0_B$.

Exercice 69

3) Montrer que si l'équation $x^2 = -1_A$ n'a pas de solution dans A alors l'équation $y^2 = -1_B$ n'a pas de solution dans B.

Soit $f : A \to B$ un isomorphisme d'anneaux. Par l'absurde : supposons qu'il existe $y \in B$ tel que $y^2 = -1_B$. Comme f est surjectif, il existe $x \in A$ tel que $y = f(x)$. On calcule :

$$f(x^2) = f(x)^2 = y^2 = -1_B.$$

Or,

$$f(-1_A) = -f(1_A) = -1_B.$$

Comme f est injectif, on en conclut que $x^2 = -1_A$. C'est une contradiction.

Exercice 70

Montrer que $\mathbb{C}$ et $\mathbb{R}^2$ sont isomorphes en tant que groupes mais pas en tant qu'anneaux.

L'anneau $\mathbb{C}$ est intègre (c'est même un corps) alors que l'anneau $\mathbb{R}^2$ ne l'est pas. En effet, $(1,0) \times (0,1) = (0,0)$. Donc ces deux anneaux ne sont pas isomorphes.

La caractéristique d'un anneau

Définition

Soit A un anneau. La **caractéristique** *de A est le plus petit entier $n \in \mathbb{N}^*$ tel que $n1_A = 0_A$, si ce nombre existe, et 0 sinon.*

Exemple

$\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n, et $\mathbb{Z}$ est de caractéristique 0.

- Si A est de caractéristique 0 alors A contient un sous-anneau isomorphe à $\mathbb{Z}$, qui est

$$\mathbb{Z} \simeq \{\ldots, -1_A, 0_A, 1_A, 2 \times 1_A = 1_A + 1_A, \ldots\}.$$

- Si A est de caractéristique $n > 0$ alors A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$, qui est

$$\mathbb{Z}/n\mathbb{Z} \simeq \{0_A, 1_A, \ldots, (n-1) \times 1_A\}.$$

Caractéristique d'un anneau intègre

Proposition

Un anneau intègre est soit de caractéristique 0 soit de caractéristique p premier.

La notion de caractéristique est particulièrement importante dans le cas des corps.

- Si K est un corps de caractéristique zéro alors K contient un sous-corps isomorphe à $\mathbb{Q}$, qui est

$$\mathbb{Q} \simeq \left\{ \frac{a \times 1_K}{b \times 1_K}, a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} \right\}.$$

  En particulier, c'est un $\mathbb{Q}$-espace vectoriel.

- Soit K un corps de caractéristique p premier. Alors K contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$, qui est

$$\mathbb{Z}/p\mathbb{Z} \simeq \{0_K, 1_K, \ldots, (p-1) \times 1_K\}.$$

  En particulier, c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

Corps finis

Théorème

Soit K un corps **fini**. *Alors il existe un nombre premier p et un entier $r \in \mathbb{N}^*$ tel que le cardinal de K est p^r.*

- En particulier, il n'existe pas de corps de cardinal $6 = 2 \times 3$ ou $20 = 4 \times 5$.

Remarques

Remarque

En fait, on peut prouver que pour tout nombre premier p et tout entier $r \in \mathbb{N}^*$ il **existe bien** un corps de cardinal p^r. Mieux, un tel corps est en fait unique à isomorphisme près. Un tel corps est généralement noté $\mathbb{F}_{p^r}$. Nous n'étudierons pas ces corps dans ce cours.

Remarque

Il y a évidemment des corps de caractéristique non nulle qui ne sont pas finis. Par exemple le corps des fractions rationnelles $(\mathbb{Z}/p\mathbb{Z})(X)$, pour p premier, est un corps infini de caractéristique p.

Pour votre culture...

Le corps à 4 éléments est

$$\mathbb{F}_4 = \{0, 1, a, 1+a\}$$

où la loi $+$ est uniquement déterminée par

$$1 + 1 = 0 \ , \ a + a = 0$$

et la loi $\times$ est uniquement déterminée par

$$a^2 = 1 + a.$$

(Vérifier que c'est bien un corps !)

L'endomorphisme de Frobenius

Proposition

Soit A un anneau commutatif de caractéristique p premier. Alors l'application $F : A \to A\ ,\ x \mapsto x^p$ est un morphisme d'anneaux.

Définition

*On appelle F l'***endomorphisme de Frobenius** *de l'anneau A.*

Définition

On se contente ici de considérer des polynômes dont les coefficients sont pris dans un **anneau commutatif** R.

Définition

Soit R un anneau commutatif. Un polynôme à une indéterminée à coefficients dans R est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de R qui est nulle à partir d'un certain rang (il existe un $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $a_n = 0$). On le note comme la combinaison linéaire

$$f = \sum_{n=0}^{N} a_n X^n \ ,$$

où l'indéterminée X est un symbole formel.

L'anneau $R[X]$

- La somme et le produit des polynômes est définie comme d'habitude : si f a pour coefficients a_n et g a pour coefficients b_n alors

$$f+g \text{ a pour coefficients } a_n+b_n$$

et

$$fg \text{ a pour coefficients}$$

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0.$$

- Cela donne à l'ensemble des polynômes une structure d'anneau commutatif (vérifiez-le !), dont le zéro est le polynôme nul (dont tous les coefficients sont 0) et dont le 1 est le polynôme 1 (dont les coefficients sont $1, 0, 0, \ldots$). On note cet anneau $R[X]$.

Degré etc.

Définition

Pour un polynôme non nul f de coefficients a_n, le **degré** *de f est le plus grand entier $n \in \mathbb{N}$ tel que $a_n \neq 0$. Le coefficient a_n correspondant est appelé* **coefficient dominant** *de f. On dit que f est* **unitaire** *si son coefficient dominant est 1.*

- On adopte la convention que le polynôme nul 0 est de degré $-\infty$: $\deg(0) = -\infty$. On adopte la convention que le polynôme nul 0 est unitaire.

Exercice 71

Lister les polynômes de degré $\leqslant 3$ à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Même chose pour $\mathbb{Z}/3\mathbb{Z}$.

Attention...

Remarque

Vous avez une certaine familiarité des polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$. Mais attention, des choses non intuitives peuvent arriver si R est un anneau (commutatif) général : par exemple,

$$\text{dans } (\mathbb{Z}/4\mathbb{Z})[X] \text{ on a } (\overline{1} + \overline{2}X)^2 = \overline{1}.$$

Un produit de deux polynômes de degré 1 peut être de degré 0...
Heureusement rien de tout cela ne se passe si l'anneau des coefficients est intègre !

Degré d'un produit

Proposition

Soit R un anneau intègre. Pour $f, g \in R[X]$ on a :

$$\deg(fg) = \deg(f) + \deg(g).$$

(On étend la somme à $\mathbb{N} \cup \{-\infty\}$ de manière évidente.)

Intégrité

Proposition

Si R est un anneau intègre alors $R[X]$ est aussi un anneau intègre.

Démonstration. Soient $f, g \in R[X]$ non nuls. Alors $\deg(f) \neq -\infty$ et $\deg(g) \neq -\infty$, et donc par la proposition précédente, $\deg(fg) \neq -\infty$ donc $fg \neq 0$. □

Inversibles

Proposition

Soit R un anneau intègre. Les inversibles de $R[X]$ sont les polynômes constants inversibles dans R :

$$R[X]^\times = R^\times.$$

Démonstration. Clairement, tous les polynômes constants inversibles dans R sont inversibles dans $R[X]$. Réciproquement, soit $f \in R[X]^\times$, alors il existe $g \in R[X]$ tel que $fg = 1$. On a donc $0 = \deg(fg) = \deg(f) + \deg(g)$ et donc $\deg(f) = \deg(g) = 0$. Donc f et g sont des polynômes constants, $f = a$ et $g = b$ avec $a, b \in R$. Comme $ab = 1$, on a $a \in R^\times$. □