FEUILLE DE TRAVAUX DIRIGÉS 1

RAPPELS SUR LES GROUPES, ANNEAUX ET CORPS

1. Groupes

Définition 1 (Groupe)**.** Un *groupe* $(G, \star, e)$ est un ensemble G muni d'une loi de composition interne $\star : G \times G \to G$ telle que
- la loi $\star$ est associative, i.e. $(x \star y) \star z = x \star (y \star z)$, pour tout $x, y, z \in G$,
- il existe un *élément neutre* e, i.e. $x \star e = e \star x = x$, pour tout $x \in G$,
- tout élément a un *inverse*, i.e. pour tout $x \in G$ il existe $y \in G$ tel que $x \star y = y \star x = e$

Lorsque la loi $\star$ est commutative, on parle de groupe *commutatif* ou de groupe *abélien*.

Définition 2 (Sous-groupe)**.** Un *sous-groupe* d'un groupe G est un sous-ensemble $H \subset G$ tel que $e \in H$ et la restriction de la loi $\star$ à H lui confèrent une structure de groupe.

Proposition 1. Soit G un groupe et $H \subset G$ un sous-ensemble. L'ensemble H est un sous-groupe de G si et seulement si $H \neq \emptyset$ et pour tout couple $(x, y) \in H^2$, on a $x \star y^{-1} \in H$.

Définition 3 (Morphisme de groupes)**.** Soient $(G, \star, e)$ et $(G', \star', e')$ deux groupes. Un *morphisme de groupes* est une application $\varphi : G \to G'$ telle que $\varphi(x \star y) = \varphi(x) \star' \varphi(y)$.
Le *noyau* d'un morphisme de groupes φ est égal à

$$Ker\, \varphi := \varphi^{-1}(\{e'\}) = \{x \in G; \varphi(x) = e'\}.$$

Exercice 1 (Injectivité et noyau)**.** Montrer qu'un morphisme de groupes $f : G \to G'$ est injectif, c'est-à-dire $f(x) = f(y)$ implique $x = y$, si et seulement si le noyau de f est égal à $\{e\}$.

Exercice 2 (Le cercle unitaire)**.**

(1) Montrer que l'application

$$\mathbb{R} \to GL_2(\mathbb{R}) \quad ; \quad \theta \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

est un morphisme de groupes.

(2) Quelle est son image ?

(3) Quel est son noyau ?

(4) Déterminer un isomorphisme de groupes de $SO(2)$ sur $U := \{z \in \mathbb{C}\,;\, |z| = 1\}$.

Exercice 3 (Union et intersection de sous-groupes)**.**
Soit un G un groupe et soient H_1 et H_2 deux sous-groupes de G.

(1) Montrer que, pour que l'union $H_1 \cup H_2$ soit un sous-groupe de G, il faut que $H_1 \subset H_2$ ou que $H_2 \subset H_1$.

(2) Si les ordres de H_1 et de H_2 sont finis et premiers entre eux, décriver l'intersection $H_1 \cap H_2$.

Exercice 4 (Générateurs de $\mathbb{S}_n$)**.**

(1) Soit $\sigma \in \mathbb{S}_n$ une permutation de $\{1, \ldots, n\}$ et soit $(a_1, \ldots, a_k)$ un cycle de longueur k de $\mathbb{S}_n$, avec $a_1, \ldots, a_k \in \{1, \ldots, n\}$. Que vaut le conjugué $\sigma(a_1, \ldots, a_k)\sigma^{-1}$?

(2) Montrer que les familles suivantes sont des systèmes de générateurs du groupe symétrique $\mathbb{S}_n$.
- $S_1 = \{(1, 2), (1, 3), \ldots, (1, n)\}$.
- $S_2 = \{(1, 2), (2, 3), \ldots, (n-1, n)\}$.
- $S_3 = \{(1, 2), (1, 2, 3, \ldots, n)\}$.

2. Anneaux

Définition 4 (Anneau)**.** Un *anneau* $(A, +, .)$ est un ensemble A muni de deux lois de composition internes $+, . : G \times G \to G$ telles que
- $(A, +)$ est un groupe abélien,
- la loi . est associative,
- la loi . est distributive par rapport à la loi $+$, i.e. pour tout $a, b, c \in A$ on a $a.(b + c) = a.b + a.c$ et $(a + b).c = a.c + b.c$.

Si la loi . admet un élément neutre, on parle d'anneau *unitaire*. Si la loi . est commutative, on parle d'anneau *commutatif*. Un élément de A est dit *inversible* s'il l'est pour la loi . de A.

Le neutre de la loi $+$ est souvent noté 0 et le neutre de la loi . est souvent noté 1.

Définition 5 (Anneau intégre)**.** Un anneau est dit *intégre* s'il n'a pas de diviseur de zéro, i.e. si $a.b = 0$ alors $a = 0$ ou $b = 0$.

Définition 6 (Sous-anneau)**.** Un sous-ensemble $B \subset A$ d'un anneau A est un *sous-anneau* de A si les restrictions de $+$ et de . à B en font un anneau.

Définition 7 (Idéal)**.** Un sous-ensemble $I \subset A$ d'un anneau A est un *idéal* de A si
- $(I, +)$ est un sous-groupe de $(A, +)$,
- pour tout $x \in I$ et $a \in A$, on a $a.x \in I$ et $x.a \in I$.

Définition 8 (Morphisme d'anneaux)**.** Soient $(A, +, .)$ et $(A', +', .')$ deux anneaux. Un *morphisme d'anneaux* est une application $\varphi : A \to A'$ telle que $\varphi(x+y) = \varphi(x) +' \varphi(y)$ et $\varphi(x.y) = \varphi(x) .' \varphi(y)$ pour tout $x, y \in A$.
Le *noyau* d'un morphisme d'anneaux φ est égal à

$$Ker\,\varphi := \varphi^{-1}(\{0'\}) = \{x \in A; \varphi(x) = 0'\}.$$

Exercice 5 (Image d'un idéal)**.**
Soit $f : A \to B$ un morphisme d'anneaux commutatifs unitaires.

(1) Montrer que l'image réciproque $f^{-1}(I')$ d'un idéal I' de A' est encore un idéal de A. Que peut-on dire du noyau de f ?

(2) Si on suppose que f soit surjectif, montrer que l'image de tout idéal I de A par f est un idéal de B.

(3) Donner un exemple de morphisme $f : A \to B$ et d'idéal I de A tel que $f(I)$ ne soit pas un idéal de B.

Exercice 6 (Entiers de Gauss et entiers quadratiques)**.**

(1) Montrer que $\mathbb{Z}[i] := \{z = a + ib;\, a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$ (appelé anneau des entiers de Gauss).

(2) Soit $d \in \mathbb{N}$. Montrer que $\mathbb{Z}[\sqrt{d}] := \{x = a + b\sqrt{d};\, a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.

(3) Montrer que 2 n'est pas un carré dans $\mathbb{Z}[\sqrt{3}]$. En déduire qu'il n'existe pas de morphismes d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$.

3. Corps

Définition 9 (Corps)**.** Un *corps* est un anneau commutatif $(\mathbb{K}, +, .)$ [en France] tel que $(\mathbb{K} - \{0\}, .)$ soit un groupe.

Exercice 7 (Idéaux d'un corps)**.** Montrer qu'un anneau commutatif A différent de $\{0\}$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

Exercice 8 (Le corps des nombres complexes)**.** Montrer que l'ensemble des matrices de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $a, b \in \mathbb{R}$ est un sous-anneau commutatif de $M_2(\mathbb{R})$. Montrer que c'est un corps isomorphe à $\mathbb{C}$, le corps des nombres complexes.

Exercice 9 (Corps des fractions)**.**
Soit A un anneau commutatif unitaire intègre. Sur l'ensemble $X := A \times (A - \{0\})$, on considère la relation :

$$(n,\, d)\, \mathcal{R}\, (n',\, d') \quad \text{si} \quad nd' = n'd.$$

(1) Montrer que $\mathcal{R}$ est une relation d'équivalence.
On note $\mathrm{Frac}(A)$ l'ensemble des classes d'équivalence. Et on écrit $\dfrac{n}{d}$ la classe de $(n,\, d)$.

(2) Montrer que les deux lois de composition interne suivantes sont bien définies

$$\frac{n_1}{d_1} + \frac{n_2}{d_2} := \frac{n_1 d_2 + n_2 d_1}{d_1 d_2} \quad \text{et} \quad \frac{n_1}{d_1} . \frac{n_2}{d_2} := \frac{n_1 n_2}{d_1 d_2}.$$

(3) Montrer que $\mathrm{Frac}(A)$ est un corps. On appelle ce corps, le *corps des fractions de* A.

(4) Que se passe-t-il si A n'est pas intègre ?

(5) Décrire les corps de fractions $\mathrm{Frac}(\mathbb{Z})$, $\mathrm{Frac}(\mathbb{K}[X])$, avec $\mathbb{K}$ un corps, et $\mathrm{Frac}(\mathbb{K})$.

(6) On considère l'application suivante

$$\begin{cases} \iota : & A & \to & \mathrm{Frac}(A) \\ & a & \mapsto & \dfrac{a}{1} \end{cases}$$

Montrer que ι est un morphisme d'anneaux.

(7) (Propriété universelle des corps de fractions) Montrer que tout morphisme d'anneaux $f : A \to \mathbb{K}$, avec $\mathbb{K}$ un corps, se factorise de manière unique en $f = \bar{f} \circ \iota$ où $\bar{f} : \mathrm{Frac}(A) \to \mathbb{K}$ est un morphisme de corps.

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "f"'] & \mathrm{Frac}(A) \arrow[d, dashed, "\exists!\,\bar{f}"] \\ & \mathbb{K} \end{tikzcd}$$

Cours : Bruno Vallette (`brunov@unice.fr`), **TDs** : Georges Elencwajg (`elenc@unice.fr`) et Bruno Vallette

Page web du cours : Depuis `http ://math.unice.fr/∼brunov`, le lien vers le site du cours se trouve en bas de l'écran.

(Pour la retrouver rapidement : Taper "Bruno Vallette" sur Google. Cliquer sur le premier lien proposé.)