Exercice 1.

Que dire de $x + y$ et $x\,y$ dans les quatre cas suivants ?

1. $x, y \in \mathbb{Q}$;
2. $x, y \in \mathbb{R} \setminus \mathbb{Q}$;
3. $x \in \mathbb{Q}, y \in \mathbb{R} \setminus \mathbb{Q}$;
4. $y \in \mathbb{Q}, x \in \mathbb{R} \setminus \mathbb{Q}$.

Exercice 2.

Soit $\sigma \in \mathfrak{S}_{10}$ définie par

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

1. Décomposer σ en produit de cycles disjoints, puis en produit de transpositions.
2. Calculer la signature de σ.
3. Quel est l'ordre de σ ?

Exercice 3.

Soit $n \geqslant 2$. Déterminer le centre Z de $(\mathfrak{S}_n, \circ)$, c'est-à-dire l'ensemble des permutations σ' telles que

$$\forall \sigma \in \mathfrak{S}_n\ ,\quad \sigma \circ \sigma' = \sigma' \circ \sigma.$$

Exercice 4.

Soit G un groupe. Notre but est de montrer que G est isomorphe à un sous-groupe de $S(G)$.

1. Pour cela considérons pour tout $g \in G$ l'application *translation à gauche par g*

$$\varphi_g : G \to G, h \mapsto gh\,.$$

Montrer que $\varphi_g \in S(G)$.

2. Montrer que $G \longrightarrow S(G), g \longmapsto \varphi_g$, est un morphisme injectif. Conclûre.

Exercice 5.

Montrer que tout groupe dont chaque élément est involutif est un groupe commutatif.

Exercice 6.

Soit G un groupe ayant un nombre fini de sous-groupes. Montrer que G est fini.

Exercice 7.

1. Citez les axiomes qui expriment que le triplet $(A, +, \cdot\,)$ est un anneau.
2. On suppose que $(A, +, \cdot\,)$ vérifie tous les axiomes d'un anneau à ceci près : on n'exige pas que le groupe $(A, +)$ est commutatif. Soient $a, b \in A$. Evaluez de deux manières différentes $(1_A + 1_A) \cdot (a + b)$. Qu'en déduisez-vous ?

Exercice 8.

Montrer que tout morphisme de corps est injectif.

Exercice 9.

1. Avec vos connaissances du collège, montrez que $\sqrt{2} \notin \mathbb{Q}$.
2. On note $\mathbb{Q}[\sqrt{2}]$ l'ensemble de tous les réels de la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. Montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{R}$.

Exercice 10.

Montrer que $\mathbb{Q}$ n'a pas de sous-corps autre que lui-même.

Exercice 11.

Montrer que l'ensemble des nombres décimaux

$$\mathbb{D} = \left\{ \frac{k}{10^n} \ :\ (k, n) \in \mathbb{Z} \times \mathbb{N} \right\}$$

est un sous-anneau de $\mathbb{Q}$. Est-ce aussi un sous-corps ?

1. Solutions

Solution 1.

1. On a $x + y$ et xy dans $\mathbb{Q}$.
2. Il peut tout se passer... Par exemple
$$\sqrt{2} + \sqrt{2} = 2\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$$
mais $\sqrt{2} - \sqrt{2} = 0 \in \mathbb{Q}$. De même, $\sqrt{2} \times \sqrt{2} = 2 \in \mathbb{Q}$ mais
$$\sqrt{2} \times \sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}!$$
3. On a $x + y \in \mathbb{R} \setminus \mathbb{Q}$. Si $x = 0$, $xy = 0 \in \mathbb{Q}$ mais par contre lorsque $x \neq 0$, $xy \in \mathbb{R} \setminus \mathbb{Q}$.
4. C'est la même situation qu'au **3.**

Solution 2.

1. On a
$$\begin{aligned}\sigma &= (1,3,7)(2,5,8,4,10)(6,9)\\ &= (1,3)(3,7)(2,5)(5,8)(8,4)(4,10)(6,9).\end{aligned}$$
2. La décomposition de σ en produit de transpositions compte 7 termes, donc $\varepsilon(\sigma) = -1$.
3. On a $o(\sigma) = \mathrm{ppcm}(2,3,5) = 30$.

Solution 3.

Il faut distinguer les cas $n = 2$ et $n \geqslant 3$.

◇ Si $n = 2$, $\mathfrak{S}_2 = \{id_{\mathbb{N}_2}, (1,2)\}$ donc $Z = \mathfrak{S}_2$.

◇ Soient $n \geqslant 3$ et $\sigma \in Z$. Soit $i \in \mathbb{N}_n$. Il existe j et k dans $\mathbb{N}_n$ tels que i, j, k soient deux à deux distincts. Comme $\sigma \circ (i,j) = (i,j) \circ \sigma$, on a
$$(i,j) = \sigma \circ (i,j) \circ \sigma^{-1} = (\sigma(i), \sigma(j)).$$
Ainsi, $\sigma(i) = i$ ou $\sigma(i) = j$. Comme le même raisonnement nous conduit à $\sigma(i) = i$ ou $\sigma(i) = k \neq j$, on a $\sigma(i) = i$. Ainsi, $\sigma = id_{\mathbb{N}_n}$ et $Z = \{id_{\mathbb{N}_n}\}$.

Solution 4.

1. Pour tout $g, h \in G$ on a
$$\begin{aligned}(\varphi_{g^{-1}} \circ \varphi_g)(h) &= g^{-1}(gh) = (g^{-1}g)h = h\,,\\ (\varphi_g \circ \varphi_{g^{-1}})(h) &= g(g^{-1}h) = (gg^{-1})h = h\,.\end{aligned}$$
Cela signifie que l'application φ_g est bijective, $\varphi_{g^{-1}}$ étant son inverse.
2. $\forall g, g', h \in G$ on a
$$(\varphi_{gg'})(h) = (gg')h = g(g'h) = (\varphi_g \circ \varphi_{g'})(h),$$
d'où $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$.
Soit $g \in \operatorname{Ker}\varphi$. Alors $\varphi_g = Id_G$, c'est-à-dire $gh = h$ pour tout $h \in G$. En particulier $g = ge_G = e_G$. Ainsi $\operatorname{Ker}\varphi = \{e_G\}$, c'est-à-dire φ est un morphisme injectif.

Solution 5.

Soit G un groupe dont chaque élément est involutif, c'est-à-dire $x = x^{-1}$ pour tout $x \in G$. Alors pour tout $(x,y) \in G^2$ on a $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, donc G est commutatif.

Solution 6.

Pour $x \in G$, on note $\langle x \rangle$ le sous-groupe de G engendré par x. Remarquons que $\langle x \rangle$ est d'ordre fini, sinon il serait isomorphe à $(\mathbb{Z}, +)$ qui possède un nombre infini de sous-groupes. Comme G possède un nombre fini de sous-groupes, les sous-groupes de la forme $\langle x \rangle$ sont en nombre fini : on les notera $\langle x_1 \rangle, \ldots, \langle x_n \rangle$. Soit $y \in G$: $\langle y \rangle$ est un des sous-groupes $\langle x_i \rangle$. En particulier, y appartient à l'un des $\langle x_i \rangle$. Ainsi $G = \cup_{i=1}^n \langle x_i \rangle$. Comme les $\langle x_i \rangle$ sont tous d'ordre fini, G est fini.

Solution 7.

1. C'est du cours.
2. On a d'une part
$$\begin{aligned}(1+1)\cdot(a+b) &= (1+1)\cdot a + (1+1)\cdot b\\ &= 1\cdot a + 1\cdot a + 1\cdot b + 1\cdot b\\ &= a + a + b + b\end{aligned}$$
et d'autre part
$$\begin{aligned}(1+1)\cdot(a+b) &= 1\cdot(a+b) + 1\cdot(a+b)\\ &= (a+b) + (a+b)\\ &= a + b + a + b\end{aligned}$$
Ainsi
$$a + b = b + a\,.$$

La commutativité de du groupe additif dans un anneau découle donc des autres axiomes ; il est superflu de l'exiger.

Solution 8.

Soit $f : K \to L$ un morpisme de corps. Soit $(a, b) \in K^2$ tel que $f(a) = f(b)$ et supposons par l'absurde que $a \neq b$. Alors $a - b$ est inversible et on obtient la contradiction

$$1_L = f(1_K) = f\left((a-b)\cdot\frac{1}{a-b}\right) = f(a-b)\cdot f\left(\frac{1}{a-b}\right) = (f(a)-f(b))\cdot f\left(\frac{1}{a-b}\right) = 0_L\cdot f\left(\frac{1}{a-b}\right) = 0_L\,. \quad \lightning$$

Solution 9.

1. Supposons par l'absurde qu'il existe des entiers non-nuls m, n tels que $2 = (m/n)^2$. On écrit $m = 2^k m_1$ et $n = 2^\ell n_1$ avec $k, \ell \in \mathbb{N}^*$ et m_1, n_1 deux entiers impairs. Comme $2n^2 = m^2$ on a $2^{2\ell+1}n_1^2 = 2^{2k}m_1^2$. Or n_1^2 et m_1^2 sont impairs, d'où la contradiction $2\ell + 1 = 2k$.

2. Il faut vérifier plusieurs propriétés.

- $\mathbb{Q}\left[\sqrt{2}\right]$ est un sous-groupe de $(\mathbb{R}, +)$. C'est facile.
- $\mathbb{Q}\left[\sqrt{2}\right]$ est stable par multiplication.
Soient $a, b, c, d \in \mathbb{Q}$. Alors le produit
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$
est aussi dans $\mathbb{Q}\left[\sqrt{2}\right]$.
- $\mathbb{Q}\left[\sqrt{2}\right]\setminus\{0\}$ est stable par inversion. Si a, b sont des rationnels non tous nuls, alors
$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}\left[\sqrt{2}\right].$$

Remarque : On ne risque pas de d'avoir $a^2 - 2b^2 = 0$ car d'après la première question il n'existe pas de rationnels a, b tels que $a^2/b^2 = 2$.

Solution 10.

Soit K un sous-corps de $\mathbb{Q}$. Alors $0, 1 \in K$. Alors $2 = 1 + 1 \in K$ et $3 = 2 + 1 \in K$. Plus généralement on montre par récurrence que $\mathbb{N} \subset K$. Or si $n \in K$ alors aussi $-n \in K$; cela implique $\mathbb{Z} \subset K$.
Si $(m, n) \in K \times K^*$ alors $m/n \in K$; cela implique $\mathbb{Q} \subset K$.

Solution 11.

Evidemment 0 et 1 sont dans $\mathbb{D}$.
Soient $k, \ell \in \mathbb{Z}$ et $n, m \in \mathbb{N}$.Stabilité par produit.

$$\frac{k}{10^n} \times \frac{\ell}{10^m} = \frac{k\ell}{10^{n+m}} \in \mathbb{D}\,.$$

Stabilité par addition. On peut supposer $n \geqslant m$. Alors

$$\frac{k}{10^n} + \frac{\ell}{10^m} = \frac{k + 10^{n-m}\ell}{10^n} \in \mathbb{D}\,.$$

Ce n'est pas un sous-corps car $\dfrac{3}{10^0}$ ne possède pas d'inverse dans $\mathbb{D}$.