

► ► 15 : GROUPES-ANNEAUX-CORPS

1►

Une loi de composition interne sur E prend donc deux arguments dans E , et le résultat de son calcul appartient à E .

Par exemple, l'addition est une loi de composition interne sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , $\mathcal{M}_{p,q}(\mathbb{K})$, $\mathcal{F}(\mathbb{R}, \mathbb{R})$, $\mathbb{Z}/n\mathbb{Z}$.

Autres exemples : la multiplication sur \mathbb{R} ou \mathbb{C} , la composition sur $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'intersection et la réunion sur $\mathcal{P}(E)$, le produit vectoriel sur \mathbb{R}^3 .

Des contre-exemples : la multiplication sur \mathbb{R}_- , la soustraction sur \mathbb{N} .

2►

L'addition sur \mathbb{R} ou \mathbb{C} est associative et commutative, la composition sur $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est associative mais non commutative (comparer les composées de $x \mapsto x^2$ et $x \mapsto x + 1$), la soustraction sur \mathbb{R} n'est ni associative ni commutative.

3►

* *Preuve* : Soit e et e' deux éléments neutres pour une loi $*$.

Alors $e * e' = e'$ parce que e est neutre, $e * e' = e$ parce que e' est neutre. Donc $e = e'$. □

* Pour montrer qu'une loi est associative, on rédige comme suit : soit x , y et z éléments de l'ensemble, ... jusqu'à obtenir $(x * y) * z = x * (y * z)$.

Même type de rédaction pour la commutativité.

Pour montrer que e est élément neutre, on écrit : soit x élément de l'ensemble, ... jusqu'à obtenir $x * e = e * x = x$.

Pour chercher (et trouver) l'élément neutre que l'on ne devine pas, on raisonne par analyse-synthèse.

Pratique 1 :

1. oui, neutre 0 2. oui, neutre 1 3. oui, neutre 1

4. \circ est toujours associative, par définition : pour tout $x \in \mathbb{R}$, et toutes fonctions f , g et h dans l'ensemble, $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = (f \circ (g \circ h))(x)$, et les ensembles départ et d'arrivée pour $(f \circ g) \circ h$ et $f \circ (g \circ h)$ étant les mêmes, on a bien $(f \circ g) \circ h = f \circ (g \circ h)$.

Mais \circ n'est pas commutative : les deux composées de $x \mapsto x + 1$ et $x \mapsto x^2$ sont respectivement $x \mapsto x^2 + 1$ et $x \mapsto (x + 1)^2$, distinctes sur \mathbb{R} .

Enfin, $\text{Id}_{\mathbb{R}} : x \mapsto x$ est l'élément neutre pour \circ .

5. oui, neutre E 6. oui, neutre \emptyset .

4►

Preuve : Par simple récurrence sur n pour la première propriété à m naturel fixé.

Pour $n = 0$, l'identité est claire. Soit alors $n \geq 1$, et supposons $x^{m+n-1} = x^m * x^{n-1}$, alors

$x^{m+n} = x^{m+n-1} * x = (x^m * x^{n-1}) * x = x^m * (x^{n-1} * x) = x^m * x^n$ où on a utilisé l'associativité de $*$ et l'hypothèse de récurrence. On conclut par le principe de récurrence.

Enfin, pour la dernière, x et y commutant, on range dans $x^n * y^n$ les termes en alternant x et y . □

5►

* Plutôt qu'"inversible", on peut dire "symétrisable" et un inverse s'appelle un symétrique.

Cela rajoute du vocabulaire, mais donne un adjectif général ; on appelle alors en général "opposé" un symétrique relativement à la loi $+$, et "inverse" un symétrique relativement à une loi multiplicative.

* *Preuve* : a) Supposons y et z être des inverses pour x . Alors $x * y = e$ donne par multiplication à gauche par z : $z * (x * y) = z * e = z = (z * x) * y = e * y = y$, d'où $y = z$.

b) Bien sûr l'identité $x * x^{-1} = x^{-1} * x = e$ se traduit également par : x est l'inverse de x^{-1} .

c) x et x^{-1} commutant : $x^n * x^{-n} = (x * x^{-1})^n = e^n = e$.

d) En effet : $(x * y) * (y^{-1} * x^{-1}) = ((x * y) * y^{-1}) * x^{-1} = (x * (y * y^{-1})) * x^{-1} = x * x^{-1} = e$ et le calcul de $(y^{-1} * x^{-1}) * (x * y)$ est semblable. □

6►

* *Preuve* : Il suffit de composer à gauche par l'inverse de a : $a^{-1} * (a * x) = (a^{-1} * a) * x = x$ et de même $a^{-1} * (a * y) = (a^{-1} * a) * y = y$, ce qui donne $x = y$. Même chose pour la deuxième implication par composition à droite. \square

* Voici le point crucial permettant de résoudre une équation de type $a * x = b$ d'inconnue x : si a est inversible, alors il y a une unique solution, $x = a^{-1} * b$.

La phrase magique n'est donc pas "si a non nul", mais "**si a est inversible**" alors $x = a^{-1} * b$.

Pratique 2 :

1. Le symétrique de 2 dans $(\mathbb{Z}, +)$ est -2 car 0 est l'élément neutre et $2 + (-2) = (-2) + 2 = 0$.
Le symétrique de 2 dans (\mathbb{N}^*, \times) n'existe pas, l'équation $2x = 1$ n'y a pas de solution.
Le symétrique de 2 dans (\mathbb{Q}, \times) est $1/2$ car 1 est l'élément neutre et $2 \times (1/2) = (1/2) \times 2 = 1$.
Le symétrique de 2 dans $(\mathbb{Z}/3\mathbb{Z}, +)$ est 1 car 0 est l'élément neutre et $2 + 1 = 1 + 2 = 0$.
Le symétrique de 2 dans $(\mathbb{Z}/5\mathbb{Z} \setminus \{0\}, \times)$ est 3 car 1 est l'élément neutre et $2 \times 3 = 3 \times 2 = 1$.
Le symétrique de 2 dans $(\mathbb{Z}/4\mathbb{Z} \setminus \{0\}, \times)$ n'existe pas car l'équation $2x = 1$ n'y a pas de solution.
Remarquer que $2 \times 2 = 0$ (non intégrité), l'existence d'un inverse pour 2 conduirait à $2 = 0$.
2. Le symétrique de f est $f^{-1} : x \mapsto \frac{x-1}{2}$ car $\text{Id}_{\mathbb{R}}$ est l'élément neutre est pour tout réel x on a :

$$\frac{(2x+1)-1}{2} = 2 \cdot \frac{x-1}{2} + 1 = x.$$
La solution de l'équation $f \circ g = h$ d'inconnue g est donc $f^{-1} \circ h : x \mapsto \frac{x^2-1}{2}$

7►

* Noter qu'un groupe vide n'existe pas puisqu'il doit contenir un élément neutre...

* Exemples : $(\mathbb{K}, +)$ et (\mathbb{K}^*, \times) où \mathbb{K} désigne \mathbb{Q} , \mathbb{R} ou \mathbb{C} , et on dispose alors de groupes abéliens.

Vérifiez que cela fonctionne aussi avec (\mathbb{U}, \times) et (\mathbb{U}_n, \times) .

Contre-exemples : (\mathbb{Z}^*, \times) et $(\mathbb{N}, +)$ ne sont pas des groupes (2 sans inverse par exemple...).

* $(\mathbb{Z}/n\mathbb{Z}, +)$ forme un groupe. Quant à $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \times)$, on peut vérifier qu'il ne forme un groupe que lorsque n est un nombre premier. En particulier, si $n = pq$ n'est pas premier, p n'a pas d'inverse modulo n , sans quoi il existerait b et k tels que $pb = nk + 1$ et le théorème de Bezout serait mis en contradiction.

* Vérifier que $(\mathcal{P}(E), \cap)$ et $(\mathcal{P}(E), \cup)$ ne sont des groupes que lorsque $E = \emptyset$.

Pratique 3 :

1. Soit $(G, *)$ un groupe à deux éléments distincts e et a , la table est nécessairement :

	$*$	e	a
e	e	a	
a	a	e	

puisque le seul inverse possible pour a est lui-même... On observe une propriété des tables de groupes, conséquence directe de l'existence et de l'unicité de la solution pour les équations $a * x = b$ et $x * a = b$:

Chaque colonne et chaque ligne de la table contient une fois et une seule chaque élément.

En notant $f(e) = 0$ et $f(a) = 1$, on fabrique une bijection de G dans $\mathbb{Z}/2\mathbb{Z}$, qui vérifie :

$f(x * y) = f(x) + f(y)$ pour les couples d'éléments de G formés avec e et a (il y en a 4).

On dit que f est un isomorphisme de groupes. Faire un calcul dans G , c'est le faire à partir des images par f avec la loi dans $f(G)$, et revenir par f^{-1} pour obtenir le résultat. Autrement dit, si on connaît une des deux tables, on connaît parfaitement l'autre.

En ce sens, on peut dire qu'il n'existe qu'un groupe à deux éléments à isomorphisme près (on pourrait dire à "notation près"). En particulier, tout groupe à 2 éléments est commutatif.

2. Soit $(G, *)$ un groupe à trois éléments distincts e , a et b , la table est nécessairement :

	$*$	e	a	b
e	e	a	b	
a	a	b	e	
b	b	e	a	

puisque le seul inverse possible pour a est b (en effet, $a * a = e$ donnerait $a * b = b$ donc $a = e$ en multipliant par b^{-1} ...). Chaque colonne et chaque ligne de la table des résultats contient une fois et une seule chaque élément. De même, ce groupe est nécessairement commutatif, et isomorphe à $(\mathbb{Z}/3\mathbb{Z}, +)$. Il n'y a donc, à isomorphisme de groupes près, qu'un groupe à trois éléments.

8►

* *Preuve* : Ces translations à gauche et à droite sont bien définies puisque $*$ est une loi de composition interne sur E .

Supposons $a * x = a * x'$, alors $x = x'$ par composition à gauche par a^{-1} , donc la translation à gauche est injective (même chose pour la translation à droite).

Soit maintenant $b \in E$, existe-t-il $x \in E$ tel que $a * x = b$? On sait faire puisque a est inversible, c'est $x = a^{-1} * b$, donc la translation à gauche est surjective (même chose pour la translation à droite). \square

* Dans $(\mathbb{R}^2, +)$ commutatif, on parle simplement, par exemple, de la translation de vecteur $(1, 2)$, qui à (x, y) associe $(x + 1, y + 2)$.

9►

* *Preuve* : On sait déjà que la composée de deux bijections est une bijection, la composition est donc bien une loi interne sur \mathcal{S}_E .

La composition est toujours associative, et Id_E est l'élément neutre.

Clairement, si f est une bijection sur E , la bijection réciproque est son inverse pour la composition. \square

* Si E comporte deux éléments, on retrouve à isomorphisme près la table de groupe de la Pratique 2.

* Si E compte n éléments (on dit que E est de cardinal n), alors \mathcal{S}_E compte $n!$ éléments puisque pour le premier élément il y a n images possibles, puis une fois cette image fixée, il reste $n - 1$ images possibles pour le deuxième, etc. Nous reverrons cela en fin d'année.

Dans cet exemple, on voit clairement, puisqu'il ne s'agit que de changer les noms des éléments de E en les numérotant, que \mathcal{S}_E est isomorphe (comme groupe) au groupe noté \mathcal{S}_n des permutations des éléments de $\llbracket 1, n \rrbracket$.

Pratique 4 :

\mathcal{S}_2 contient $2! = 2$ éléments, le neutre Id et la "transposition" échangeant 1 et 2, notée $\tau_{1,2}$. La table de groupe est donc celle obtenue en Pratique 2.

\mathcal{S}_3 comporte $3! = 6$ éléments, le neutre Id , les trois transpositions $\tau_{1,2}$, $\tau_{1,3}$ et $\tau_{2,3}$, et enfin les deux cycles σ_1 qui décale les éléments à gauche ($1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$) et σ_2 qui décale à droite.

Vérifier par exemple que $\tau_{1,2} \circ \tau_{1,3} = \sigma_1$, $\tau_{1,3} \circ \tau_{1,2} = \sigma_2$, $\sigma_1 \circ \tau_{1,2} = \tau_{2,3}$ etc. et utiliser la propriété des tables de groupe pour effectuer moins de calcul. (\mathcal{S}_3, \circ) n'est pas commutatif.

10►

* H est donc une partie de E stable par $*$ et non vide (puisque doit contenir "son" élément neutre). De plus, ce neutre e' ne peut qu'être e puisque $e * e' = e'$ (e neutre de E) et $e' * e' = e'$ (e' neutre de H) donc, en utilisant l'inverse de e' dans E dans l'égalité $e * e' = e' * e'$ on obtient $e' = e$.

* Par exemple, si e est le neutre de E , $\{e\}$ est toujours un sous-groupe de $(E, *)$.

* $C^1([0, 1], \mathbb{R})$ est un sous-groupe de $(C^0([0, 1], \mathbb{R}), +)$. Le théorème suivant donne des outils plus rapides pour le montrer...

11►

* *Preuve* : Les conditions proposées sont clairement nécessaires pour que $(H, *)$ forme un groupe, compte tenu du premier point de 10.

Supposons réciproquement 1) et 2). La restriction de $*$ à $H \times H$ est donc une loi de composition interne sur H , pour laquelle e_E est bien élément neutre. L'associativité de $*$ étant vérifiée dans E , elle l'est clairement dans H , les calculs étant les mêmes. Enfin, tout élément x de H est inversible dans H par hypothèse. \square

* Ainsi, si H est un sous-groupe de $(E, *)$, alors le neutre de H et de E sont identiques, l'inverse de tout élément de H vu dans H est le même que celui vu dans E , ce qui n'était pas évident au départ...

* **Pour montrer que $(E, *)$ est un groupe, on tâche de montrer plus rapidement que E est un sous-groupe d'un groupe $(E', *)$ connu.** D'où l'intérêt de bien connaître les exemples de groupes vus en cours.

Pratique 5 :

1. Appliquer le théorème de caractérisation : $1 = \exp(2i \cdot 0 \cdot \pi/n)$ appartient bien à \mathbb{U}_n , et pour tout k et k' dans \mathbb{N} , $\exp(2ik\pi/n) \times \exp(-2ik'\pi/n) = \exp(2i(k - k')\pi/n)$ appartient bien à \mathbb{U}_n .

2. Notons \mathcal{S}_a l'ensemble des bijections de E laissant a invariant. \mathcal{S}_a est non vide puisque contient l'identité. Si enfin f et g sont deux bijections transformant a en a , alors il en est de même de g^{-1} , et $f \circ g^{-1}$ est une bijection qui transforme a en a .

Ainsi \mathcal{S}_a est un sous-groupe de $(\mathcal{S}(E), \circ)$.

3. C est non vide car contient l'élément neutre e_E de E qui commute avec tout élément de E .

Si x et y sont deux éléments de C , pour tout z dans E on a : $x * y * z = x * z * y = z * x * y$ donc $x * y$ appartient bien à C , et enfin de $x * z = z * x$ on déduit par composition par x^{-1} à gauche et à droite que $z * x^{-1} = x^{-1} * z$, donc x^{-1} appartient à C .

Le centre d'un groupe est donc bien toujours un sous-groupe de ce groupe.

12►


* *Preuve* : 1) L'élément neutre de E appartient à tous les sous-groupes H_i donc à leur intersection qui est donc non vide.

Si x et y appartiennent à tous les H_i , alors $x * y^{-1}$ également puisque chaque H_i est un sous-groupe de $(E, *)$. Ainsi, $\bigcap_{i \in I} H_i$ est un sous-groupe de $(E, *)$.

2) Soit H une partie de E , alors E contient H et c'est un sous-groupe de $(E, *)$, donc l'intersection de tous les sous-groupes de $(E, *)$ qui contiennent H est une partie non vide de E , qui forme un sous-groupe de $(E, *)$ d'après 1). C'est bien sûr le plus petit au sens de l'inclusion puisqu'inclus dans tout sous-groupe de $(E, *)$ contenant H . \square

* Le sous-groupe de $(\mathbb{Z}, +)$ engendré par le naturel n est l'ensemble des multiples de n , noté $n\mathbb{Z} = \langle n \rangle$.

* $\exp(2ik\pi/n)$ génère le groupe (\mathbb{U}_n, \times) si, et seulement si, k et n sont premiers entre eux. En effet, si c'est le cas il existe k' entier tel que $\exp(2ikk'\pi/n) = \exp(2i\pi/n)$, donc $kk' \equiv 1 [n]$, donc il existe k' et u entiers tels que $kk' + un = 1$, donc $k \wedge n = 1$. Inversement, dans ce cas, pour $p \in \mathbb{Z}$, $(\exp(2ik\pi/n))^{k'p} = \exp(2ip\pi/n)$.

*  La réunion de deux sous-groupes de E n'a aucune raison d'être un sous-groupe de $(E, *)$.

Par exemple, la réunion $3\mathbb{Z} \cup 4\mathbb{Z}$ ne contient pas 1, alors que, 3 et 4 étant premiers entre eux, il existe u et v entiers tels que $3u + 4v = 1$, ce qui montre que le groupe engendré par cette réunion est $\mathbb{Z} = \langle 3, 4 \rangle$.

13►

* *Preuve* : a) En choisissant $x = y = e_1$, il vient $f(e_1) = f(e_1) \bullet f(e_1)$, donc en composant par l'inverse de $f(e_1)$ dans G_2 il vient : $f(e_1) = e_2$.

b) Pour x donné dans G_1 , en choisissant $y = x^{-1}$ il vient $f(e_1) = e_2 = f(x) \bullet f(x^{-1})$, ce qui montre par unicité de l'inverse que $f(x^{-1}) = (f(x))^{-1}$.

c) Preuve par récurrence simple sur $n \in \mathbb{N}$. □

* Ainsi dès la fin du XVI^e siècle, un astronome a pu, grâce à Napier (ou Néper) et ses tables logarithmiques, effectuer des multiplications en les transformant en additions grâce à l'isomorphisme de groupes \ln entre $(\mathbb{R}_+, *)$ et $(\mathbb{R}, +)$: pour calculer $a \times b$, on utilise la table directe pour obtenir $\ln(a)$ et $\ln(b)$ qu'on somme, puis la table inverse pour connaître $c = a \times b$ tel que $\ln(c) = \ln(a) + \ln(b) = \ln(ab)$.

Pratique 6 :

1. C'est la relation vérifiée pour tous réels x et y : $\exp(x + y) = \exp(x) \cdot \exp(y)$
Comme de plus \exp est bijective \mathbb{R} sur \mathbb{R}_+^* , c'est bien un isomorphisme de groupes.

2. De même pour tous réels θ et φ : $e^{i(\theta+\varphi)} = e^{i\theta} e^{i\varphi}$

À cause de la 2π -périodicité, on répond négativement à la question.

14►

* *Preuve* : a) Montrons que $f(K_1)$ est sous-groupe de (G_2, \bullet) . Comme déjà vu il contient l'image par f du neutre de G_1 , et qui est le neutre de G_2 . Enfin, si $f(x)$ et $f(y)$ sont deux éléments de $f(K_1)$ pour x et y dans K_1 , alors $x * y^{-1}$ est dans K_1 , d'image $f(x) \bullet (f(y))^{-1} = f(x * y^{-1})$ comme déjà vu, qui appartient bien à $f(K_1)$, d'où le résultat.

b) Montrons que $H = f^{-1}(K_2)$ est un sous-groupe de G_1 . Comme $f(e_1) = e_2$ est le neutre de G_2 , il appartient à K_2 , donc $e_1 \in H$. Enfin, si x et y sont dans H , alors $f(x) * (f(y))^{-1} = f(x * y^{-1})$ appartient à K_2 , donc $xy^{-1} \in H$ qui est bien un sous-groupe de G_1 . □

* Vous pouvez vérifier facilement que la composée de deux morphismes de groupes est encore un morphisme de groupes, et que l'inverse d'un isomorphisme de groupe est aussi un isomorphisme de groupe.

* Un morphisme de groupes f est injectif si, et seulement si, son **noyau** $\text{Ker } f$ est réduit à l'élément neutre du groupe de départ : $\text{Ker } f = \{e_1\}$.

En effet, $f(e_1)$ est le neutre du groupe d'arrivée comme déjà vu. Si f est injective, $\text{Ker } f = f^{-1}(\{e_2\})$ contient un unique élément, e_1 .

Si réciproquement $\text{Ker } f = \{e_1\}$, supposons $f(x) = f(y)$, alors $f(x * y^{-1}) = e_2$ donc $x * y^{-1} = e_1$ et finalement $x = y$ donc f est injective.

C'est un raccourci que nous utiliserons systématiquement en algèbre linéaire.

Pratique 7 :

\exp est un isomorphisme entre les groupes $(\mathbb{R}, +)$ et (\mathbb{R}_+^*, \times) , donc de noyau $\{0\}$ et d'image \mathbb{R}_+^* .

$\theta \mapsto e^{i\theta}$ est un morphisme entre $(\mathbb{R}, +)$ et (\mathbb{C}^*, \times) , de noyau le groupe $(2\pi\mathbb{Z}, +)$ et d'image (\mathbb{U}, \times) .

15►

* Il y a deux lois de compositions internes : on note $-x$ l'opposé de x pour $+$: $x - x = (-x) + x = 0_A$, et on note x^{-1} l'inverse (s'il existe) de x relativement à $*$: $x * x^{-1} = x^{-1} * x = 1_A$.

Attention, un élément de A , même non nul, n'admet pas forcément un inverse !

* $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, $(\mathcal{F}(\mathbb{R}), +, \times)$, $(\mathbb{K}[X], +, \times)$ sont des anneaux.

16►

- Preuve :* a) Soit $a \in A$, alors $a * 0 = a * (0 + 0) = a * 0 + a * 0$ donc $a * 0 = 0$, et même calcul pour $0 * a$.
 b) Pour a et b dans A , $(a - a) * b = 0 * b = 0 = a * b + (-a) * b$ donne le résultat.
 c) Pour $a \in A$ inversible, $(-a) * a^{-1} = -1$ donc $(-a) * (-a^{-1}) = 1$, d'où $(-a)^{-1} = -a^{-1}$.
 d) Pour a et b inversibles dans A : $b^{-1} * a^{-1} * a * b = b^{-1} * b = 1$, ce qui donne le résultat.
 e) La preuve est identique à celle vue dans \mathbb{R} ou \mathbb{C} où l'on n'avait utilisé que les règles de calcul dans un anneau commutatif, et ici a et b sont supposés commuter...
 f) Même chose. □

17►

* *Preuve :* A^* est non vide car contient l'élément 1_A . De plus on a avec d) du point 15 que si a et b sont inversibles dans A , alors $a * b$ l'est aussi. Comme de plus tout inverse d'élément est inversible (d'inverse l'élément), A^* contient aussi a^{-1} . D'où le résultat. □

* Par exemple : $\mathbb{Z}^* = \{-1; 1\}$

* Si $E = \mathcal{F}(I, \mathbb{R})$ où I est un intervalle de \mathbb{R} , muni de l'addition et de la multiplication usuelle entre fonctions, alors E^* est constitué des fonctions de E qui ne s'annulent pas sur I .

* Attention aux égalités de type $a * b = 0_A$ dans l'anneau $(A, +, *)$. Elle n'implique pas a ou b nul (cette conclusion n'est sûre que si a ou b est inversible).

Par exemple, dans $(\mathbb{Z}/4\mathbb{Z}, +, \times) : 2 \times 2 \equiv 0 \pmod{4}$ alors que $2 \neq 0$. On dit que 2 est un diviseur de zéro.

Autre exemple dans $(\mathcal{F}([-1, 1], \mathbb{R}), +, \times)$: le produit des fonctions caractéristiques de $[-1, 0]$ et de $]0, 1]$ est nul ; ces deux fonctions sont donc des diviseurs de zéro.

Un anneau sans diviseur de zéro est dit intègre : dans ce cas, l'équation $a * b = 0$ équivaut à $a = 0$ ou $b = 0$.

Par exemple, $(\mathbb{Z}/n\mathbb{Z}, +, *)$ est un anneau intègre si, et seulement si, n est premier.

Autre exemple, $(\mathbb{K}[X], +, \times)$ est un anneau intègre.

* Pour montrer qu'une partie B forme un sous-anneau de $(A, +, \times)$: comme dans la caractérisation des sous-groupes, il suffit de montrer que B est une partie de A qui contient les deux éléments neutres 0 pour $+$ et 1 pour \times , que B est stable par l'addition, par passage à l'opposé, et par la multiplication. En effet, les autres propriétés (associativité, commutativité(s), distributivité) sont vérifiées dans A donc forcément dans B ...

18►

* Un corps est un anneau particulier, toujours intègre. La réciproque est fausse (penser à $(\mathbb{K}[X], +, \times)$).

* Pour a élément d'un corps et distinct de 1, et n naturel, on a : $1 + a + a^2 + \dots + a^n = (1 - a^{n+1})(1 - a)^{-1}$

* La condition supplémentaire assurant qu'un anneau $(A, +, *)$ est un corps se ramène à " $(A \setminus \{0\}, *)$ est un groupe". Et pour un corps \mathbb{K} , la notation \mathbb{K}^* désigne simplement \mathbb{K} privé de $0_{\mathbb{K}}$.

Par exemple, \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des corps, mais ni \mathbb{Z} (2 n'est pas inversible) ni $\mathcal{F}(\mathbb{R}, \mathbb{R})$ n'en sont.

* Pour montrer qu'une partie B forme un sous-corps d'un corps $(C, +, \times)$: on montre que B est une partie de C qui contient les deux éléments neutres 0 pour $+$ et 1 pour \times , que B est stable par l'addition, par passage à l'opposé, par la multiplication et par passage à l'inverse. Les autres propriétés (associativité, commutativité(s), distributivité) sont vérifiées dans C donc forcément dans B ...

Pratique 8 :

On démontre que $\mathbb{Q}(i)$ est un sous-corps de \mathbb{C} .

Comme par les caractérisations des sous-groupes, on montre successivement que $\mathbb{Q}(i) \subset \mathbb{C}$, que $\mathbb{Q}(i)$ contient les éléments neutres $0 = 0 + 0.i$ pour $+$ et $1 = 1 + 0.i$ pour \times , que $\mathbb{Q}(i)$ est stable par $+$, par passage à l'opposé, par \times et par passage à l'inverse (pour un élément non nul).

En effet, si a, b, c et d sont des rationnels, $(a + ib) - (c + id) = (a - c) + i(b - d)$ avec $a - c$ et $b - d$ rationnels, $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$ avec $ac - bd$ et $ad + bc$ rationnels, et enfin si $(a, b) \neq (0, 0)$,

l'inverse $\frac{a - ib}{a^2 + b^2}$ de $a + ib$ est bien dans $\mathbb{Q}(i)$ puisque $\frac{a}{a^2 + b^2}$ et $\frac{b}{a^2 + b^2}$ sont bien rationnels.