Structures algébriques

PCSI 2 Lycée Pasteur

15 octobre 2007

1 Structures algébriques

1.1 Lois de composition

Définition 1. Soit E un ensemble. Une loi de composition interne (ou lci) sur E est tout simplement une application $* : E \times E \to E$. on note $x * y$ plutôt que $*(x, y)$ l'image d'un couple d'éléments de E.

Remarque 1. Autrement dit, $*$ est une opération interne à l'ensemble E.

Exemples : Vous connaissez déjà un bon paquet de lois de compositions internes. La somme ou le produit sur $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ en sont bien sûr. Par contre, la soustraction n'est pas une loi de composition interne sur $\mathbb{N}$, et la division n'est une loi de composition interne sur aucun de ces ensembles puisqu'on ne peut pas diviser par 0.

La composition sur l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ ou l'intersection sur l'ensemble des parties de $\mathbb{N}$ sont également des lois de composition internes.

Le produit scalaire n'est pas une loi de composition interne sur l'ensemble des vecteurs du plan puisque le résultat de l'opération n'est pas un vecteur.

Définition 2. Une lci $*$ sur un ensemble E est dite associative si $\forall (x, y, z) \in E^3$, $(x*y)*z = x*(y*z)$. Une lci $*$ sur un ensemble E est dite commutative si $\forall (x, y) \in E^2$, $x * y = y * x$.

Exemples : La plupart des lci que vous connaissez sont associatives (somme, composition, intersection). Pourtant, une opération aussi simple que la soustraction sur $\mathbb{Z}$ n'est pas associative. Un bon exemple de lci qui n'est pas commutative est la composition sur l'ensemble de fonctions de $\mathbb{R}$ dans $\mathbb{R}$.

Définition 3. Un élément $e \in E$ est dit neutre pour une lci $*$ si $\forall x \in E$, $x * e = e * x = x$.

Proposition 1. Si une lci admet un élément neutre, celui-ci est unique.

Démonstration. Supposons qu'il existe deux éléments neutres e_1 et e_2. On a alors $e_1 * e_2 = e_1$ car e_2 est un élément neutre, mais aussi $e_1 * e_2 = e_2$ car e_1 est un élement neutre, donc $e_1 = e_2$. □

Exemples : L'addition, sur tous les ensembles où elle est définie, a pour élément neutre 0, et le produit 1. L'élément neutre pour la composition est l'application identité, celui de la réunion est l'ensemble vide.

Définition 4. Soit $(E, *)$ un ensemble muni d'une lci possédant un élément neutre e. On dit que $x \in E$ est inversible s'il existe $y \in E$ tel que $x * y = y * x = e$.

Remarque 2. Cette notion d'inverse correspond bien à l'inverse usuel quand l'opération est un produit, mais il s'agira de l'équivalent de l'opposé pour la somme. Pour la composition, seules les applications bijectives sont inversibles. Notons qu'un élément peut être inversible à gauche mais pas à droite, c'est-à-dire qu'il peut existe un y tel que $y * x = e$, mais pas de z tel que $x * z = e$. Par exemple, dans l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$, la fonction $n \mapsto 2n$ est inversible à gauche (son inverse à gauche est $g : n \mapsto E(\frac{n}{2})$), mais pas à droite.

Définition 5. Lorsqu'il existe, on note x^{-1} l'inverse de x (même si la lci n'est pas un produit).

Proposition 2. L'inverse d'un élément, lorsqu'il existe, est unique. Il est lui-même inversible, et $(x^{-1})^{-1} = x$. Si deux élements x et y sont inversibles, alors $x*y$ est inversible et $(x*y)^{-1} = y^{-1}*x^{-1}$. On peut par ailleurs simplifier par un élément inversible : si $x * y = x * z$, avec x inversible, alors $y = z$ (et de même à droite).

Démonstration. Supposons que x ait deux inverses, notés y et z. On a alors $y*x*z = y*(x*z) = y*e = y$, mais aussi $y*x*z = (y*x)*z = e*z = z$ donc $y = z$. La relation $(x^{-1})^{-1}$ découle de la symétrie de la définition de l'inverse. L'inverse du produit ne pose pas de problème : $y^{-1}*x^{-1}*x*y = y^{-1}*y = e$, et de même dans l'autre sens, donc ça marche. Et pour obtenir les simplifications, il suffit de multiplier par x^{-1}. □

Définition 6. Soit E un ensemble muni de deux lci . et $*$. On dit que . est distributive sur $*$ si $\forall (x, y, z) \in E^3$, $x.(y * z) = (x.y) * (x.z)$ et $(y * z).x = (y.x) * (z.x)$.

1.2 Groupes

Définition 7. Un groupe $(E, *)$ est un ensemble E muni d'une lci $*$ associative, possédant un élément neutre et pour laquelle tout élement de E est inversible. Si de plus la loi $*$ est commuttative, on dit que $(E, *)$ est un groupe commutatif, ou abélien.

Exemples : Le couple $(\mathbb{N}, +)$ n'est pas un groupe, mais $(\mathbb{Z}, +)$ en est un. De même, $(\mathbb{R}, \times)$ n'est pas un groupe mais $(\mathbb{R}^*, \times)$ en est un. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de la composition n'est pas un groupe. Si on se restreint aux applications bijectives, c'en est un.

L'ensemble des polynomes de degré n, muni de l'addition, n'est pas un groupe. Par contre, l'ensemble des polynomes de degré inférieur ou égal à n en est un.

Définition 8. Soit $(G, *)$ un groupe et $H \subset G$, on dit que H est un sous-groupe de G si $(H, *_{|H})$ est un groupe.

Exemples : Le groupe $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est lui-même un sous-groupe de $(\mathbb{R}, +)$, qui est enfin un sous-groupe de $(\mathbb{C}, +)$. Plus intéressant, le groupe des nombres complexes de module 1 est un sous-groupe du groupe multiplicatif $\mathbb{C}^*, \times)$.

Proposition 3. Un sous-ensemble H de $(G, *)$ est un sous-groupe si et seulement si il contient e et est stable par produit et passage à l'inverse.

Démonstration. Si un sous-ensemble de G vérifie ces trois propriétés, c'est bien un sous-groupe. Réciproquement, si H est un sous-groupe, il possède un élément neutre e_0. Soit alors x un élément de H, on a $x * e_0 = x = x * e$ (la première étoile prise dans H, la deuxième dans G), donc $e_0 = e$ par simplification. De même, l'inverse de x dans H est nécessairement un inverse dans G également, donc il s'agit de l'unique inverse de x par $*$, et H est stable par inversion. Enfin, H doit clairement être stable par produit. □

Définition 9. Soient $(G, *)$ et $(H, .)$ deux groupes. on dit que l'application $f : G \to H$ est un morphisme de groupes si $\forall (x, y) \in G$, $f(x * y) = f(x).f(y)$.

Exemples : La multiplication par 2 est un morphisme de groupes de $(\mathbb{Z}, +)$ dans lui-même, puisque $2(x + y) = 2x + y$. En fait, la multiplication par n'importe quel entier reste un morphisme de groupes. L'opération de dérivation de l'ensemble des fonctions de $\mathbb{R}$ dans lui-même, muni de la somme de fonctions, est un morphisme de groupes.

On a par ailleurs démontré en deux temps dans les chapitres précédents que les applications de la forme $t \mapsto e^{at}$ $(a \in \mathbb{R})$ étaient des morphismes de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \times)$, et même que c'était les seuls. Réciproquement, les logarithmes sont les seuls morhismes de groupe de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$.

Proposition 4. Soit f un morphisme de groupes de $(G, *)$ vers $(H, .)$, alors l'image par f de l'élément neutre de G est l'élément neutre de H, et $\forall x \in G$, $(f(x))^{-1} = f(x^{-1})$.

Démonstration. On a $\forall x \in G$, $f(x).f(e) = f(x*e) = f(x)$, et $f(e).f(x) = f(e*x) = f(x)$, donc $f(e)$ est bien l'élément neutre e' de H. On en déduit que $\forall x \in G$, $e' = f(e) = f(x * x^{-1}) = f(x).f(x^{-1})$ (et de même en échangeant les rôles de x et de x^{-1}), donc $f(x)$ et $f(x^{-1})$ sont bien inverses l'un de l'autre dans H. □

Exemples : On retrouve le fait, par exemple, que $e^{-x} = (e^x)^{-1}$.

Définition 10. Soient $f : (G, *) \to (H, .)$ et $g : (H, .) \to (K, \S)$ deux morphismes de groupe, alors $g \circ f$ est un morphisme de groupes de G dans K.

Démonstration. C'est en fait évident : $\forall (x, y) \in G^2$, $g \circ f(x * y) = g(f(x).f(y)) = (g \circ f(x))\S(g \circ f(y))$. □

Définition 11. Soit $f : (G, *) \to (H, .)$ un morphisme de groupes et e_H l'élément neutre de H pour la loi ., on appelle noyau de f, et on note $\ker f$, l'ensemble $\{x \in G \mid f(x) = e_H\}$. On appelle image de f, et on note $\operatorname{im} f$, l'ensemble image de G par l'application f.

Proposition 5. Le noyau d'un morphisme est un sous-groupe du groupe de départ, son image un sous-groupe du groupe d'arrivée.

Démonstration. D'après ce qui précède, l'élément neutre de G est un élément du noyau. De plus, le noyau est stable par produit et par inverse : si $(x, y) \in (\ker f)^2$, $f(x * y) = f(x).f(y) = e_H.e_H = e_H$, et $f(x^{-1}) = (f(x))^{-1} = e_H^{-1} = e_H$. Pour l'image, ce n'est pas plus dur : le neutre est image du neutre, le produit est image des produits et l'inverse image de l'inverse donc c'est immédiat. □

Proposition 6. Un morphisme de groupe f est surjectif si et seulement si $\operatorname{im} f = H$. Il est injectif si et seulement si $\ker f = \{e_G\}$.

Démonstration. Pour la surjectivité, c'est la définition. Pour l'injectivité, on a clairement, si f est injectif, $\ker f = \{e_G\}$, puisque e_G est un antécédent de e_H, et que celui-ci n'a pas le droit d'en avoir plus d'un. Réciproquement, raisonnons par contraposée. Supposons qu'un élément $y \in H$ ait deux antécédents distincts x et x' par f, on a alors $f(x^{-1} * x') = y^{-1}.y = e_H$, donc $x^{-1} * x' \in \ker f$, et $x^{-1} * x' \neq e_G$ car x et x' sont distincts. □

Exemple : L'image de $\mathbb{Z}$ par l'application qui à un entier associe son double est l'ensemble des entiers pairs, qui est donc un sous-groupe de $\mathbb{Z}$.

Définition 12. Un morphisme de groupes bijectif est appelé isomorphisme de groupes. Deux groupes sont dits isomorphes s'il existe un isomorphisme de groupes entre eux.

1.3 Anneaux, corps

Définition 13. Un anneau $(A, +, .)$ est un ensemble A muni de deux lois de composition internes $+$ et . telles que $(A, +)$ soit un groupe commutatif, d'élément neutre noté 0_A, et la loi . soit associative, admette un élément neutre 1_A, et soir distributive par rapport à $+$. Si de plus la loi . est commutative, on dit que A est un anneau commutatif.

Remarque 3. Dans un anneau, on notera donc $-x$ l'inverse d'un élément x pour la loi $+$, et x^{-1} son inverse pour la loi ., lorsqu'il existe.

Exemples : $(\mathbb{Z}, +, .)$ est un anneau commutatif(on n'impose absolument pas que la loi multiplicative soit une loi de groupe). L'ensemble $\mathcal{P}(\mathbb{R})$ muni des lois $\cap$ et $\cup$ n'est pas un anneau : chacune des deux lois et associative, commutative, elles sont distributives l'une par rapport à l'autre, et il y a un élément neutre pour chaque ($\emptyset$ pour la réunion, $\mathbb{R}$ pour l'intersection), mais aucune n'est une loi de groupe car tous les éléments de l'ensemble ne sont pas inversibles.

Proposition 7. Quelques règles de calcul dans un anneau $(A, +, .)$:

- $\forall a \in A$, $0_A.a = a.0_A = 0$.
- $\forall a \in A$, $(-1_A).a = -a$.

Démonstration. Constatons que $a.0 + a.0 = a.(0 + 0) = a.0$, donc en simplifiant par $a.0$ (on a le droit, car $+$ est une loi de groupe), on obtient $a.0 = 0$. Même preuve pour le produit à droite. Pour la deuxième propriété, on a $1.a + (-1).a = (1 + (-1)).a = 0.a = 0$, donc $(-1).a$ est l'opposé de $1.a = a$, c'est-à-dire égal à $-a$. □

Définition 14. Dans un anneau, on peut définir par récurrence na, comme valant 0 si $n = 0$, et $a + (n-1)a$ si $n \geqslant 1$. On a en fait $na = n.a$, où $n = 1_1 + \cdots + 1_A$ (n fois). En utilisant la propriété précédente, on a de même pour $n \neq 0$, $(-n).a = -(n.a)$. On peut également définir les puissances (positives) d'un élément quelconque de l'anneau de façon usuelle.

Proposition 8. Soit $(A, +, .)$, un anneau, et $(a, b) \in A^2$ deux éléments qui commutent ($a.b = b.a$), alors $\forall n \in \mathbb{N}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ (formule du binome de Newton).

On a également $\forall n \geqslant 1$, $(a-b)^n = (a-b)(\sum_{k=0}^{n-1} a^{n-1-k} b^k)$. Lorsque $1-a$ est inversible, on a aussi $\sum_{k=0}^{n} a^k = (1-a^{n+1})(1-a)^{-1}$ (somme d'une suite géométrique).

Démonstration. La formule du binome se démontre exactement comme dans le cas réel. Pour la deuxième formule, pas besoin de récurrence : $(a-b)(\sum_{k=0}^{n-1} a^{n-1-k} b^k) = \sum_{k=0}^{n-1} a^{n-k} b^k - \sum_{k=0}^{n-1} a^{n-1-k} b^{k+1} = \sum_{k=0}^{n-1} a^{n-k} b^k - \sum_{j=1}^{n} a^{n-j} b^j = a^n - b^n$. Il suffit ensuite d'appliquer la formule au rang $n+1$ à a et 1 pour obtenir la somme géométrique. □

Définition 15. Un anneau commutatif est dit intègre si $\forall (a, b) \in A^2$, $a.b = 0 \Rightarrow a = 0$ ou $b = 0$.

Remarque 4. Une autre façon de voir les choses est de dire que, dans un anneau intègre, on peut simplifier des produits à droite ou à gauche : si $a.b = a.c$ avec $a \neq 0$, alors $b = c$ (en effet, on a $a.(b-c) = 0$, donc $b - c = 0$). Tous les anneaux ne sont pas intègres (vous verrez un exemple extrêmement courant en maths quand vous étudierez les matrices), et il faut énormément se méfier de cette simplification qui peut paraitre naturelle mais qui n'est pas toujours vraie.

Définition 16. Soit $(A, +, .)$ un anneau et $B \subset A$. On dit que B est un sous-anneau de A si B est un anneau pour les lois de A.

Proposition 9. B est un sous-anneau de A si B est un sous-groupe de A pour l'addition, contient 1_A et est stable par produit.

Exemple : Le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même (on dit que $\mathbb{Z}$ ne possède pas de sous-anneau propre). En effet, si B est un sous-anneau de $\mathbb{Z}$, il contient 0 et 1. Par récurrence, on montre alors qu'il contient tous les entiers positifs, car si $n \in B$ et $1 \in B$, $n + 1 \in B$ qui est stable par somme. Mais comme sous-groupe, B est aussi stable par passage à l'opposé, donc contient également tous les entiers négatifs.

Définition 17. Une application $f : (A, +, .) \to (B, \bigoplus, \times)$ (A et B étant deux anneaux) est un morphisme d'anneaux si $\forall (a, a') \in A^2$, $f(a + a') = f(a) \bigoplus f(a')$ et $f(a.a') = f(a).f(a')$ **et** $f(1_A) = A_{A'}$. Si $A = B$, on parle d'endomorphisme d'anneaux.

Remarque 5. La dernière condition est indispensable et pas automatique.

Définition 18. On appelle corps un anneau commutatif $(K, +, .)$ non nul dans lequel tout élément non nul est inversible pour la loi multiplicative. Autrement dit, $(K^*, .)$ est un groupe.

Définition 19. Un sous-ensemble L d'un corps K est un sous-corps de K s'il est un corps pour les lois de K, ce qui se produit dès que L est un sous-groupe additif de K et L^* un sous-groupe multiplicatif de K^*.

Exemple : $(\mathbb{Q}, +, .)$ est un sous-corps de $(\mathbb{R}, +, .)$, qui est lui-même un sous-corps de $(\mathbb{C}, +, .)$.

2 Arithmétique

2.1 Divisibilité, congruences

Définition 20. Soient $(a, b) \in \mathbb{N}^* \times \mathbb{Z}$, a divise b (et b est un diviseur de a) s'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$. On le note $a \mid b$.

Proposition 10. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}^*$. On a de plus les propriétés suivantes : si $a \mid b$ et $a \mid c$ alors $\forall (u, v) \in \mathbb{Z}^2$, $a \mid (bu + cv)$. Si $a \mid b$ et $c \mid d$ alors $ab \mid cd$.

Démonstration. Le fait que ce soit une relation d'ordre a déjà été vu en exercice lors du chapitre sur les relations d'ordre. Le reste est essentiellement évident : si $b = ka$ et $c = la$, avec k et l entiers, alors $bu + cv = (ku + lv)a$, donc $a \mid bu + cv$. De même, si $b = ka$ et $d = lc$ alors $bd = (kl)ac$, donc $ac \mid bd$. □

Théorème 1. Division euclidienne

Soient $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, alors il existe un couple unique d'entiers (p, q) tels que $a = bq + r$, et $0 \leqslant r \leqslant b - 1$. L'entier q est appelé quotient de la division euclidienne de a par b, et r est le reste de la division.

Démonstration. Commençons par traiter le cas $a \geqslant 0$, et notons $A = \{k \in \mathbb{N} \mid a - kb \geqslant 0\}$. Ce sous-ensemble de $\mathbb{N}$ est non vide puisqu'il contient 0, et majoré car tous les entiers k strictement supérieurs à a vérifient $a - kb < 0$ (puisque $b \geqslant 1$), donc contient un plus grand élément, que nous allons noter q. Notons $r = a - qb$, on a, par définition de q, $r \geqslant 0$ et $a - (q + 1)b = r - b < 0$, donc $0 \leqslant r \leqslant b - 1$, donc on a trouvé un couple convenable.

Dans le cas où $a < 0$, on sait qu'il existe un couple (q, r) tel que $-a = bq + r$, avec $0 \leqslant r \leqslant b - 1$. Si $r = 0$, on a donc $a = -bq$, et l'existence est prouvée. Si $b > 0$, $-a = b(q + 1) + r - b$, donc $a = b(-q - 1) - r + b$, avec $1 \leqslant b - r \leqslant r - 1$, donc on a également trouvé un couple convenable.

Prouvons désormais l'unicité, supposons qu'on a deux couples (q, r) et (q', r') satisfaisant les deux conditions. Comme $a = bq + r = bq' + r'$, on a $b(q - q') = r' - r$. Or, $-b + 1 \leqslant r' - r \leqslant b - 1$, donc si $q'_q \neq 0$, on doit avoir $r' - r = 0$, pour qu'il puisse être divisible par b. Mais dans ce cas, comme $b \neq 0$, on a tout de même $q = q'$. Dans tous les cas, les deux couples sont les mêmes, il y a donc unicité du couple recherché. □

Théorème 2. Sous-groupes de $\mathbb{Z}$

Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $a\mathbb{Z} = \{k \in \mathbb{Z} \mid a \text{ divise } k\}$, avec $a \in \mathbb{Z}$.

Démonstration. Soit G un sous-groupe de $\mathbb{Z}$, G contient nécessairement l'élément neutre 0. Notons $G_+ = G \cap \mathbb{N}^*$, soit $G_+ = \emptyset$ et $G = \{0\}$ (car G étant stable par opposition, s'il ne contient pas d'entiers positifs, il n'en contient pas non plus de négatifs), soit G_+ est un sous-ensemble non vide de $\mathbb{N}$, donc minoré. Notons a le plus petit élément de $\mathbb{G}_+$. On prouve facilement par récurrence que $\forall n \in \mathbb{N}$, $na \in G$: $0 \in G$ et si $na \in G$, $na + a \in G$ car G est stable par somme. L'ensemble G contient aussi les multiples négatifs de a puisqu'il est stable par opposition. Supposons maintenant qu'il contienne un élément b qui ne soit pas un multiple de a. Par division euclidienne de b par a, il existe deux entiers p et q tels que $b = aq + r$, et $0 < r < a$ (r ne peut pas être nul car b n'est pas multiple de a). Or, $b \in G$ et $aq \in G$, donc $r = b - aq \in G$, ce qui contredit la minimalité de a. C'est absurde, on a donc $G = a\mathbb{Z}$. □

Définition 21. Soient $n \in \mathbb{N}^*$. On dit que deux entiers a et b sont congrus modulo n si $n \mid b-a$ (autrement dit, a et b ont le même reste lors de leur division euclidienne par n). On le note $a \equiv b[n]$.

Proposition 11. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. De plus, cette relation est compatible avec la somme et le produit : si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a+b \equiv c+d[n]$, et $ac \equiv bd[n]$.

Démonstration. La relation est binaire, réflexive ($a-a=0$ est toujours divisible par n), symétrique (si $b-a$ est divisible par n, $a-b$ aussi) et transitive : si $n \mid b-a$ et $n \mid c-b$ alors $n \mid (b-a)+(c-b) = c-a$. C'est donc une relation d'équivalence. De plus, si $n \mid b-a$ et $n \mid d-c$ alors $n \mid b+d-a-c$, d'où la première propriété. Enfin, $n \mid b(d-c)+c(b-a)$, ce qui prouve la deuxième. □

Remarque 6. L'ensemble des classes d'équivalence pour la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$, il est constitué de n classes habituellement notées $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ (la classe $\bar{i}$ est celle qui contient l'entier i). D'après la propriété précédente, on peut munir $\mathbb{Z}/n\mathbb{Z}$ d'une somme et d'un produit qui en font en fait un anneau commutatif. Cet anneau est un corps si et seulement si aucun entier compris entre 2 et $n-1$ n'est divisible par n, c'est-à-dire si n est premier.

2.2 Nombres premiers

Définition 22. Un entier $n \in \mathbb{N}^*$ est dit premier s'il a exactement deux diviseurs : 1 et lui-même.

Remarque 7. L'entier 1 n'est pas premier, par convention. L'entier 2 est le seul entier pair premier.

Théorème 3. Il existe une infinité d'entiers premiers.

Démonstration. On l'a déjà faite au moment de l'explication de ce qu'était une preuve par l'absurde. □

Théorème 4. Soit $n \in \mathbb{N}$, alors n peut s'écrire de façon unique sous la forme $n \prod_{i=1}^{k} p_i^{\alpha_i}$, où $p_1, \ldots, p_k$ sont des entiers premiers, et $\alpha_1, \ldots, \alpha_k$ des entiers non nuls.

Démonstration. La preuve, technique, n'est pas à votre programme, alors on ne la fera pas. □