



EXERCICES DE

**THÉORIE DES ENSEMBLES**

**EXERCICE 1.**

Niveau : Premier Cycle

Auteur : Ruben Ricchiuto (16.03.05)

Mots Clés : Unions, intersections

**Énoncé :**

Soit  $X$  un ensemble et  $(A_i)_I$  une famille de sous-ensembles de  $X$  indexée sur  $I$  ( $I$  un ensemble quelconque). Nous notons pour tout  $B \subseteq X$ ,  $B^c = \{x \in X \mid x \notin B\}$  le complémentaire de  $B$ .

On vérifie facilement que  $(B^c)^c = B$ . Montrer les relations suivantes :  $\left(\bigcup_I A_i\right)^c = \bigcap_I A_i^c$ ,

$$\left(\bigcap_I A_i\right)^c = \bigcup_I A_i^c.$$

**Solution :**

Dire qu'un élément  $x \in X$  appartient à  $\left(\bigcup_I A_i\right)^c$  est équivalent à dire que  $x \notin \bigcup_I A_i$  et cette dernière affirmation est équivalente à dire que  $x$  n'appartient à aucun des  $A_i$  donc (c'est toujours une équivalence)  $x$  appartient à tous les  $A_i^c$  c'est-à-dire  $x \in \bigcap_I A_i^c$ . Ainsi

$\left(\bigcup_I A_i\right)^c = \bigcap_I A_i^c$ . Pour montrer que  $\left(\bigcap_I A_i\right)^c = \bigcup_I A_i^c$  on utilise le premier point. En effet,

$\left(\bigcup_I A_i^c\right)^c = \bigcap_I A_i$  (par le premier point). Donc en prenant le complémentaire des deux côtés de

l'égalité nous obtenons  $\bigcup_I A_i^c = \left(\bigcap_I A_i\right)^c$ .

**EXERCICE 2.***Niveau* : Premier Cycle*Auteur* : Ruben Ricchiuto (16.03.05)*Mots Clés* : Différence symétrique**Énoncé :**

Soit  $X$  un ensemble. Nous définissons l'opération de différence symétrique par : pour tout  $A, B \subseteq X$ ,  $A \Delta B = (A \setminus B) \cup (B \setminus A)$ . Montrer que  $(\mathcal{P}(X), \Delta, \cap)$  est un anneau ( $\Delta$  joue le rôle de l'addition et  $\cap$  celui de la multiplication).

**Solution :**

$(\mathcal{P}(X), \Delta)$  est un groupe commutatif. En effet  $\emptyset$  est l'élément neutre pour  $\Delta$ , si  $A \subseteq X$  alors  $A \Delta A = \emptyset$  ( $A$  est son propre opposé) et il est évident que  $A \Delta B = B \Delta A$ . L'associativité est aussi vérifiée car  $A \Delta (B \Delta C) = A \setminus (B \Delta C) \cup (B \Delta C) \setminus A = A \setminus (B \setminus C \cup C \setminus B) \cup (B \setminus C \cup C \setminus B) \setminus A$ .

Or

$$\begin{aligned} A \setminus (B \setminus C \cup C \setminus B) &= A \cap (B \setminus C \cup C \setminus B)^c = A \cap (B^c \cup C) \cap (C^c \cup B) \\ &= (A \cap B^c \cap C^c) \cup (A \cap C \cap B) \text{ et} \end{aligned}$$

$$\begin{aligned} (B \setminus C \cup C \setminus B) \setminus A &= (B \setminus C \cup C \setminus B) \cap A^c = ((B \cap C^c) \cup (C \cap B^c)) \cap A^c \\ &= (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c). \text{ Ainsi} \end{aligned}$$

$A \Delta (B \Delta C) = (A \cap B^c \cap C^c) \cup (A \cap C \cap B) \cup (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c)$ . D'un autre côté,  $(A \Delta B) \Delta C = C \Delta (B \Delta A)$  et en permutant les rôles de  $A$  et  $C$  on peut réutiliser les calculs ci-dessus. Nous obtenons,

$$(A \Delta B) \Delta C = C \Delta (B \Delta A) = (C \cap B^c \cap A^c) \cup (A \cap C \cap B) \cup (B \cap C^c \cap A^c) \cup (A \cap B^c \cap C^c) \text{ ce qui montre que } (A \Delta B) \Delta C = A \Delta (B \Delta C).$$

Il ne reste qu'à vérifier la distributivité.

$$A \cap (B \Delta C) = A \cap (B \setminus C \cup C \setminus B) = (A \cap B \setminus C) \cup (A \cap C \setminus B). \text{ Or}$$

$$(A \cap B \setminus C) = (A \cap B) \setminus (A \cap C) \text{ et } A \cap C \setminus B = (A \cap C) \setminus (A \cap B). \text{ Donc}$$

$$A \cap (B \Delta C) = ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B)) = (A \cap B) \Delta (A \cap C).$$

**EXERCICE 3.***Niveau* : Premier Cycle*Auteur* : Ruben Ricchiuto (16.03.05)*Mots Clés* : Applications et ensembles**Énoncé:**

Soit  $X, Y$  deux ensembles et  $f : X \rightarrow Y$  une application. Montrer que si  $(A_i)_I$  est une famille de sous-ensembles de  $Y$  alors  $f^{-1}\left(\bigcup_I A_i\right) = \bigcup_I f^{-1}(A_i)$  et  $f^{-1}\left(\bigcap_I A_i\right) = \bigcap_I f^{-1}(A_i)$ .  
Montrer aussi que pour  $B \subseteq Y$ ,  $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$ .

**Solution :**

$x \in f^{-1}\left(\bigcup_I A_i\right) \Leftrightarrow \exists j \in I, f(x) \in A_j \Leftrightarrow \exists j \in I, x \in f^{-1}(A_j) \Leftrightarrow x \in \bigcup_I f^{-1}(A_i)$  ce qui prouve

que  $f^{-1}\left(\bigcup_I A_i\right) = \bigcup_I f^{-1}(A_i)$ . Pour  $B \subseteq Y$  nous avons,

$x \in f^{-1}(Y \setminus B) \Leftrightarrow f(x) \in Y \setminus B \Leftrightarrow f(x) \notin B \Leftrightarrow x \notin f^{-1}(B) \Leftrightarrow x \in X \setminus f^{-1}(B)$  ce qui prouve que  $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$ . Pour finir, en utilisant les deux premier résultats,

$$f^{-1}\left(\bigcap_I A_i\right) = f^{-1}\left(\left(\bigcup_I A_i^c\right)^c\right) = f^{-1}\left(\bigcup_I A_i^c\right) = X \setminus f^{-1}\left(\bigcup_I A_i^c\right) = X \setminus \bigcup_I f^{-1}(A_i^c) = \bigcap_I f^{-1}(A_i)$$

**EXERCICE 4.***Niveau* : Premier Cycle*Auteur* : Ruben Ricchiuto (16.03.05)*Mots Clés* : Ensembles et applications**Énoncé :**Soit  $X, Y$  deux ensembles et  $f : X \rightarrow Y$  une application.

1. Soit  $(A_i)_I$  une famille de sous-ensembles de  $X$ . Montrer que :  $f\left(\bigcup_I A_i\right) = \bigcup_I f(A_i)$   
et  $f\left(\bigcap_I A_i\right) \subseteq \bigcap_I f(A_i)$ . Donner un exemple où la deuxième inclusion est stricte.
2.  $\forall A, B \subseteq X, f(A \cap B) = f(A) \cap f(B) \Leftrightarrow f$  est injective.

**Solution :**

1.  $y \in f\left(\bigcup_I A_i\right) \Leftrightarrow \exists x \in \bigcup_I A_i, y = f(x) \Leftrightarrow \exists j \in I, \exists x \in A_j, y = f(x)$   
 $\Leftrightarrow \exists j \in I, y \in f(A_j) \Leftrightarrow y \in \bigcup_I f(A_i)$ . Donc  $f\left(\bigcup_I A_i\right) = \bigcup_I f(A_i)$ .  
 $y \in f\left(\bigcap_I A_i\right) \Leftrightarrow \exists x \in \bigcap_I A_i, y = f(x) \Rightarrow \forall i \in I, \exists x \in A_i, y = f(x)$   
 $\Leftrightarrow \forall i \in I, y \in f(A_i) \Leftrightarrow y \in \bigcap_I f(A_i)$ . Donc  $f\left(\bigcap_I A_i\right) \subseteq \bigcap_I f(A_i)$ . Si on considère  
l'application  $x \mapsto x^2$  de  $\mathbb{R} \rightarrow \mathbb{R}$  alors  $f([-1,0] \cap [0,1]) = f(0) = \{0\}$  mais  
 $f([-1,0]) \cap f([0,1]) = [0,1]$ .
2. Supposons que  $\forall A, B \subseteq X, f(A \cap B) = f(A) \cap f(B)$  et soit  $x, x' \in X$  tels que  
 $f(x) = f(x')$  alors  $x = x'$  car autrement  $\emptyset = f(\{x\} \cap \{x'\}) = f(\{x\}) \cap f(\{x'\}) = f(x)$   
ce qui est absurde. Réciproquement, supposons  $f$  injective. Soit  $A, B \subseteq X$  et  
 $y \in f(A) \cap f(B)$  alors il existe  $a \in A$  et  $b \in B$  tels que  $y = f(a) = f(b)$ . Ce qui  
entraîne  $a = b \in A \cap B$ , donc  $y \in f(A \cap B)$  et vu que  $f(A \cap B) \subseteq f(A) \cap f(B)$   
nous avons  $f(A \cap B) = f(A) \cap f(B)$ .

**EXERCICE 5.**

*Niveau* : Premier Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Ensembles, applications et relations

---

**Énoncé :**

Soit  $f : A \rightarrow B$  une application d'un ensemble  $A$  à un ensemble  $B$ . On définit la relation  $R$  suivante  $\forall x, y \in A, xRy \Leftrightarrow f(x) = f(y)$ .

1. Montrer que  $R$  est une relation d'équivalence.
2. Soit  $A/R$  l'ensemble des classes d'équivalence pour la relation  $R$  et  $\pi : A \rightarrow A/R$  la projection canonique. Montrer que  $R$  induit une application injective  $\tilde{f} : A/R \rightarrow B$  vérifiant  $f = \tilde{f} \circ \pi$ .

**Solution :**

1.  $xRx$  car  $f(x) = f(x)$ .  $xRy \Leftrightarrow yRx$  (symétrie de l'égalité...). Enfin  $xRy$  et  $yRz \Leftrightarrow f(x) = f(y) = f(z)$  donc  $xRz$ .
2. Pour tout  $a \in A$ , on pose  $\tilde{f}(\pi(a)) := f(a)$ .  $\tilde{f}$  ne dépend pas du représentant  $a$  choisi mais seulement de la classe de  $a$ , en effet si  $aRb$  alors  $f(a) = f(b)$ . Ainsi  $\tilde{f}$  est bien définie et  $f = \tilde{f} \circ \pi$ .  $\tilde{f}$  est injective car  $\tilde{f}(\pi(a)) = \tilde{f}(\pi(b)) \Leftrightarrow f(a) = f(b) \Leftrightarrow aRb \Leftrightarrow \pi(a) = \pi(b)$ .

**EXERCICE 6.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Ensembles, applications

---

**Énoncé :**

Soit  $f : A \rightarrow B$  une application surjective. Montrer (utiliser l'axiome du choix) qu'il existe une application injective  $g : B \rightarrow A$  telle que  $f \circ g = id$  (où  $id$  est l'application identité).

**Solution :**

Soit  $\phi : \mathcal{P}(A) \setminus \{\emptyset\} \rightarrow A$  une application choix (c'est-à-dire  $\forall C \subseteq A, \phi(C) \in C$ ). Posons pour tout  $b \in B$ ,  $g(b) = \phi(f^{-1}(b))$ . Alors  $\forall b \in B, f \circ g(b) = f(\phi(f^{-1}(b))) = b$  car

$\phi(f^{-1}(b)) \in f^{-1}(b)$ . Ainsi  $f \circ g = id$  et  $g$  est injective car

$g(b) = g(b') \Rightarrow f(g(b)) = f(g(b')) = b = b'$ .

**EXERCICE 7.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Ensembles ordonnés

---

**Énoncé :**

Soit  $X$  un ensemble ordonné non vide. Notons  $\leq$  l'ordre sur  $X$ . Montrer que nous avons l'équivalence suivante : tout sous-ensemble non vide de  $X$  possède un élément maximal  $\Leftrightarrow$  toute suite croissante  $(x_n)_{\mathbb{N}}$  d'éléments de  $X$  est stationnaire.

**Solution :**

Montrons l'implication  $\Rightarrow$ . Soit  $(x_n)_{\mathbb{N}}$  une suite croissante. Considérons l'ensemble non vide  $\{x_n \mid n \in \mathbb{N}\}$ . Par hypothèse,  $\{x_n \mid n \in \mathbb{N}\}$  possède un élément maximal. Notons  $x_m$  cet élément ( $m \in \mathbb{N}$ ). Alors pour tout  $n \geq m$ ,  $x_m \leq x_n$  et par maximalité on en déduit  $x_m = x_n$ . Ce qui montre que la suite est stationnaire.

Montrons  $\Leftarrow$ . Soit  $A \subseteq X$  non vide et supposons que  $A$  ne possède pas d'élément maximal. Soit  $a_0 \in A$ , il existe  $a_1 \in A$  tel que  $a_0 < a_1$  (vu que  $a_0$  n'est pas maximal) avec le même raisonnement on obtient l'existence d'un élément  $a_2 \in A$  tel que  $a_0 < a_1 < a_2$  etc. Nous voyons donc qu'il est possible de construire une suite strictement croissante  $(a_n)_{\mathbb{N}}$  ce qui est absurde vu que toutes les suite croissantes sont stationnaires.

**EXERCICE 8.**

*Niveau* : Premier Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Cardinal de l'ensemble des parties

---

**Énoncé :**

Soit  $E$  un ensemble. On note  $\mathcal{P}(E)$ , parfois aussi  $2^E$ , l'ensemble des parties de  $E$  (on rappelle qu'une partie est un sous-ensemble de  $E$ ). Montrer que si  $E$  est un ensemble fini alors  $\mathcal{P}(E)$  possède  $2^{\text{Card}(E)}$  éléments (où  $\text{Card}(E)$  est le cardinal de  $E$ ).

Remarque : ceci justifie la notation  $2^E$  employée certaines fois pour désigner l'ensemble des parties de  $E$ .

**Solution :**

Notons  $n = \text{Card}(E)$ . Pour tout  $0 \leq k \leq n$ , il y a  $\binom{n}{k}$  sous-ensembles de  $E$  à  $k$  éléments.

Donc  $\text{Card}(\mathcal{P}(E)) = \sum_{k=0}^n \binom{n}{k} = (1+1)^n$  par la formule du binôme. C'est-à-dire

$$\text{Card}(\mathcal{P}(E)) = 2^n.$$

**EXERCICE 9.**

*Niveau* : Premier Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Applications

---

**Énoncé :**

Soit  $A, B, C, D$  des ensembles,  $f$  une application de  $A$  dans  $B$ ,  $g$  une application de  $B$  dans  $C$  et  $h$  une application de  $C$  dans  $D$ . Montrer que si  $g \circ f$  et  $h \circ g$  sont bijectives alors  $f, g, h$  sont bijectives.

**Solution :**

Si  $g \circ f$  est bijective alors  $g$  est surjective et  $f$  injective (facile à voir). De même,  $h \circ g$  bijective entraîne  $h$  surjective et  $g$  injective. Ainsi,  $g$  est bijective. Soit  $b \in B$ , il existe  $a \in A$  tel que  $g \circ f(a) = g(b)$  mais vu que  $g$  est bijective, cette égalité entraîne  $f(a) = b$ . Donc  $f$  est bijective. Si  $h(c) = h(c')$  alors il existe  $b, b' \in B$  tels que  $c = g(b)$  et  $c' = g(b')$  et par suite,  $h(g(b)) = h(g(b'))$ .  $h \circ g$  est bijective donc  $b = b'$  et par conséquent  $c = c'$ . Ainsi,  $h$  est bijective.

**EXERCICE 10.***Niveau* : Premier Cycle*Auteur* : Ruben Ricchiuto (16.03.05)*Mots Clés* : Ensembles et applications**Énoncé :**

Soit  $X$  un ensemble. Montrer qu'on a l'équivalence suivante :  $X$  est infini ssi pour toute application  $f : X \rightarrow X$  il existe  $A \subset X$  non vide,  $A \neq X$  tel que  $f(A) \subset A$ .

**Solution :**

Montrons  $\Leftarrow$ . Si  $X$  est fini alors nous pouvons écrire  $X = \{x_1, \dots, x_n\}$  avec  $n \in \mathbb{N}^*$ .

Considérons l'application  $f : X \rightarrow X$  définie par  $f(x_i) = x_{i+1}$  si  $i < n$  et  $f(x_n) = x_1$ . Nous voyons facilement que  $f(A) \subset A$  entraîne  $A = X$ . Ce qui est contradictoire. Donc  $X$  est infini.

Montrons  $\Rightarrow$ . Supposons qu'il n'existe pas de  $A \subset X$  comme dans l'énoncé. Soit  $x \in X$ .

Posons  $A = \{f^n(x) \mid n \in \mathbb{N}\}$  où  $f^0(x) = x$  et  $f^n(x) = \underbrace{f \circ f \circ \dots \circ f}_{n \text{ fois}}(x)$ . Nous vérifions

immédiatement que  $f(A) \subset A$ . Par hypothèse, ceci entraîne  $X = A$ . Or pour  $n < m$  on a

$f^n(x) \neq f^m(x)$  car autrement  $A = \{x, f(x), \dots, f^m(x)\}$  et donc  $X$  est fini. Considérons alors

l'ensemble  $B = \{f^n(x) \mid n \geq 1\}$  qui est strictement contenu dans  $X$ . On a  $f(B) \subset B$  ce qui est manifestement en contradiction avec notre hypothèse. Donc l'hypothèse est fautive et il existe bien un ensemble  $A \subset X$  non vide  $A \neq X$  tel que  $f(A) \subset A$ .

**EXERCICE 11.**

*Niveau* : Premier Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Ensemble des parties

---

**Énoncé :**

Voici un résultat dû à Cantor. Soit  $X$  un ensemble non vide. Il n'existe pas d'application surjective  $f : X \rightarrow \mathcal{P}(X)$  (où  $\mathcal{P}(X)$  est l'ensemble des parties de  $X$ ). [Indication : considérer l'ensemble  $\{x \in X \mid x \notin f(x)\}$ ].

**Solution :**

Supposons que  $f : X \rightarrow \mathcal{P}(X)$  est surjective. Alors il existe  $y \in X$  tel que  $f(y) = \{x \in X \mid x \notin f(x)\}$ . Et on voit que  $y \in \{x \in X \mid x \notin f(x)\} \Leftrightarrow y \notin \{x \in X \mid x \notin f(x)\}$  ce qui est absurde.

**EXERCICE 12.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (16.03.05)

*Mots Clés* : Ensemble ordonnés, axiome du choix et lemme de Zorn

**Énoncé :**

Cet exercice à pour but de montrer que le lemme de Zorn implique l'axiome du choix. Soit  $X, Y$  des ensembles non vides. On définit  $E = \{(A, f) \mid A \subseteq X, A \neq \emptyset, f : A \rightarrow Y\}$ . On définit la relation  $\preceq$  sur  $E$  par  $(A, f) \preceq (B, g) \Leftrightarrow A \subseteq B$  et  $\forall a \in A, f(a) = g(a)$ .

1. Montrer que  $\preceq$  est une relation d'ordre sur  $E$ .
2. Soit  $(Y_x)_{x \in X}$  une famille de parties de  $Y$  avec  $Y_x \neq \emptyset$  pour tout  $x \in X$ . Soit  $S$  le sous-ensemble de  $E$  constitué par les éléments  $(A, f)$  tels que  $\forall a \in A, f(a) \in Y_a$ . Montrer que  $S$  est non vide et que  $(S, \preceq)$  est inductif. (On rappelle qu'un ensemble ordonné est inductif si toute partie totalement ordonnée possède un majorant).
3. Dédurre de 2. que le lemme de Zorn implique l'axiome du choix. (On rappelle que le lemme de Zorn dit que tout ensemble ordonné et inductif possède un élément maximal).

**Solution :**

1. La réflexivité est évidente. Si  $(A, f) \preceq (B, g)$  et  $(B, g) \preceq (A, f)$  alors  $A = B$  et  $f = g$ . Si  $(A, f) \preceq (B, g)$  et  $(B, g) \preceq (C, h)$  alors  $A \subseteq B \subseteq C$  et  $\forall b \in B, h(b) = g(b)$  à fortiori pour tout  $a \in A, h(a) = g(a) = f(a)$ . Donc  $(A, f) \preceq (C, h)$ .
2.  $S$  est non vide car soit  $x \in X$  et  $y \in Y_x$  alors  $(\{x\}, f) \in S$  avec  $f : \{x\} \rightarrow Y$ ,  $f(x) = y$ . Soit  $W \subseteq S$  une partie totalement ordonnée. On pose  $U = \bigcup_{A \in D} A$  où  $D = \{A \in \mathcal{P}(X) \mid \exists f : A \rightarrow Y \text{ tel que } (A, f) \in W\}$ . Si  $x \in U$ , il existe  $A \in D$  tel que  $x \in A$ . Par suite il existe  $f : A \rightarrow Y$  tel que  $(A, f) \in W$ . On définit l'application  $\phi : U \rightarrow Y$  par  $\forall x \in U, \phi(x) = f(x)$ . Montrons que  $\phi$  est bien définie, c'est-à-dire qu'elle ne dépend ni de  $A$  ni de  $f$ . En effet si  $(B, g) \in W$  et que  $x \in B$  alors vu que  $W$  est totalement ordonné on a  $(A, f) \preceq (B, g)$  ou  $(B, g) \preceq (A, f)$  et de toute façon  $f(x) = g(x)$ .  $(U, \phi) \in S$  car en reprenant les notations d'avant, pour  $x \in U$ ,  $\phi(x) = f(x)$  et vu que  $(A, f) \in W \subseteq S$ ,  $f(x) \in Y_x$ . Donc  $\phi(x) \in Y_x$ . De plus,  $(U, \phi)$  majore  $W$  en effet, si  $(B, g) \in W$  alors  $B \subseteq U$  (par définition de  $U$ ) et pour tout  $b \in B$ ,  $\phi(b) = g(b)$  (par définition de  $\phi$ ).  $(S, \preceq)$  est donc inductif.
3. Si dans 2. on prend  $X = \mathcal{P}(Y) \setminus \{\emptyset\}$  et pour tout  $x \in X, Y_x = x$  alors par Zorn,  $S$  possède un élément maximal. Notons-le  $(M, \pi)$ .  $M = X$  car autrement il existe  $K \in X \setminus M$ . Dans ce cas on peut définir l'application  $\phi : M \cup \{K\} \rightarrow Y$  par

$\varphi(A) = \pi(A)$  pour tout  $A \in M$  et  $\varphi(K) = y$  avec  $y \in K$  quelconque.

$(M \cup \{K\}, \varphi) \in S$  et  $(M, \pi) \prec (M \cup \{K\}, \varphi)$  ce qui contredit la maximalité de  $(M, \pi)$ .

Ainsi  $(X, \pi) \in S$  ce qui veut justement dire que  $\pi$  est une fonction choix sur  $Y$ .

**EXERCICE 13.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés* : Extensions finies de corps, séparabilité

---

**Énoncé :**

Soit  $L/K$  une extension de corps, algébrique et séparable. On suppose qu'il existe  $n \geq 1$  tel que pour tout  $x \in L$ ,  $[K(x):K] \leq n$ . Montrer que dans ce cas  $L/K$  est une extension finie et que  $[L:K] \leq n$ . [Indication: si  $x \in L$  est de degré maximal, c'est-à-dire

$\forall y \in L, [K(y):K] \leq [K(x):K]$ , montrer en utilisant le théorème de l'élément primitif que pour tout  $y \in L$ ,  $K(x, y) = K(x)$ ].

**Solution :**

Soit  $x \in L$  de degré maximal et soit  $y \in L$ . Nous avons les inclusions  $K \subseteq K(x, y) \subseteq L$ .

$L/K$  séparable entraîne  $K(x, y)/K$  séparable.  $x, y$  étant algébriques sur  $K$ ,  $K(x, y)/K$  est une extension de degré fini. Par le théorème de l'élément primitif, il existe  $z \in K(x, y)$  tel que  $K(x, y) = K(z)$ . Ainsi  $[K(x):K] \leq [K(z):K]$  et par maximalité de  $x$ ,  $[K(x):K] = [K(z):K]$  et donc  $K(x) = K(z) = K(x, y)$ . Nous venons de montrer que  $y \in L \Rightarrow y \in K(x)$ , c'est-à-dire  $L = K(x)$ . Par suite  $L/K$  est une extension finie de degré  $\leq n$ .

**EXERCICE 14.**

*Niveau* : Premier Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés*: Sous-groupes du groupe des permutations

---

**Énoncé :**

Démontrer que tout groupe fini d'ordre  $n$  est isomorphe à un sous-groupe de  $\mathcal{S}_n$  (où  $\mathcal{S}_n$  est le groupe des permutations). [Indication: Considérer l'application  $\varphi: G \rightarrow \text{Perm}(G)$ , où  $\text{Perm}(G)$  est le groupe des permutations des éléments de  $G$ , définie par  $\varphi(g)(x) = g \cdot x$  ].

**Solution :**

L'application  $\varphi: G \rightarrow \text{Perm}(G)$  est un homomorphisme car

$\varphi(g_1 \cdot g_2)(x) = g_1 \cdot g_2 \cdot x = g_1 \cdot \varphi(g_2)(x) = \varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1) \circ \varphi(g_2)(x)$ . De plus  $\varphi(g) = id \Leftrightarrow \forall x \in G, g \cdot x = x \Leftrightarrow g = 1$  ce qui prouve que  $\varphi$  est injective. On termine en remarquant que  $\text{Perm}(G) \simeq \mathcal{S}_n$  ( $n = |G|$ ).

**EXERCICE 15.***Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Groupes finis**Énoncé :**

Montrer que pour tout groupe fini  $G$ , si  $|G| = p^2$  avec  $p$  premier alors  $G$  est abélien.

[Indication: utiliser l'équation des classes  $|G| = |Z(G)| + \sum_{x \in Y} |Conj(x)|$  où

$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$  est le centre de  $G$  (c'est un sous-groupe),  $Y$  est un système de représentants pour les classes de conjugaison qui contiennent au moins deux éléments et  $Conj(x)$  est la classe de conjugaison de  $x$ .]

**Solution :**

$Z(G)$  est un sous-groupe de  $G$  et donc  $|Z(G)|$  divise  $|G|$  ce qui entraîne  $|Z(G)| \in \{1, p, p^2\}$ .

Supposons  $|Z(G)| = 1$ . Dans ce cas  $Y \neq \emptyset$ . Notant  $S_x = \{g \in G \mid gxg^{-1} = x\}$  le stabilisateur de

$x$  (c'est un sous-groupe) on sait que  $|S_x| \cdot |Conj(x)| = |G|$ . Ainsi  $|Conj(x)|$  divise  $p^2$  et si  $x \in Y$

on a  $|Conj(x)| \in \{p, p^2\}$ , de plus  $|Conj(x)| = p^2$  étant impossible on a forcément

$|Conj(x)| = p$  et donc  $p$  divise  $|G| - \sum_{x \in Y} |Conj(x)| = |Z(G)| = 1$  ce qui est absurde. Par

conséquent  $|Z(G)| = p$  ou  $p^2$ .  $|Z(G)| = p$  est aussi impossible car sinon pour  $x \in Y$ ,

$|S_x| \cdot |Conj(x)| = |G|$  implique  $|S_x| = p$  et vu que  $Z(G) \subseteq S_x$  on aurait  $Z(G) = S_x$  et par suite

$x \in S_x = Z(G)$  ce qui est absurde. Donc  $|Z(G)| = p^2 = |G|$  et  $G$  est abélien.

**EXERCICE 16.**

*Niveau* : Premier Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés*: Sous-groupes de  $\mathbb{Z}$

---

**Énoncé :**

Déterminer les sous-groupes de  $\mathbb{Z}$ .

**Solution :**

Si  $n$  est un entier, l'ensemble des multiples de  $n$  noté  $n \cdot \mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ . Nous allons montrer que tous les sous-groupes de  $\mathbb{Z}$  sont de ce type.

Soit  $G \subseteq \mathbb{Z}$  un sous-groupe. Notons  $n$  le plus petit entier strictement positif appartenant à  $G$ . Soit  $m \in G$ . Divisons  $m$  par  $n$  :  $m = q \cdot n + r$  ( $0 \leq r < n$ ).  $r = m - q \cdot n \in G$  et par minimalité de  $n$ ,  $r = 0$ . Donc  $G = n \cdot \mathbb{Z}$ .

**EXERCICE 17.**

Niveau : Deuxième Cycle

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés : Groupe dérivé

**Énoncé:** Soit  $G$  un groupe. Pour tout  $a, b \in G$  on note  $[a, b] := aba^{-1}b^{-1}$ . Les éléments  $[a, b]$  sont appelés *commutateurs*. On définit le *groupe dérivé*  $D(G)$  comme étant le sous-groupe de  $G$  engendré par les commutateurs.

- 1) Démontrer que  $D(G)$  est normal.
- 2) Démontrer que pour tout sous groupe normal  $H \subseteq G$ ,  $G/H$  est abélien ssi  $D(G) \subseteq H$ .
- 3)  $G/D(G)$  est l'abélianisé de  $G$ . Démontrer que deux groupes isomorphes ont des abélianisés isomorphes.
- 4) Déterminer le groupe dérivé et l'abélianisé de  $\mathcal{S}_n$  (le groupe des permutations) pour  $n \geq 3$ . [Indication: démontrer que le sous-groupe  $Alt(n) = \{\sigma \in \mathcal{S}_n \mid \varepsilon(\sigma) = 1\}$ , où  $\varepsilon$  est la signature, est engendré par les 3-cycles. En déduire que  $Alt(n) \subseteq D(\mathcal{S}_n)$ .]

**Solution:**

1. Soit  $x \in G$ .  
 $x[a, b]x^{-1} = xaba^{-1}b^{-1}x^{-1} = xax^{-1}xbx^{-1}xa^{-1}x^{-1}xb^{-1}x^{-1} = [xax^{-1}, xbx^{-1}] \in D(G)$  ce qui prouve la normalité de  $D(G)$  (tout élément de  $D(G)$  est produit de commutateurs).
2. Si  $G/H$  abélien et  $\pi : G \rightarrow G/H$  est la projection canonique  $\pi([a, b]) = \pi(1)$  et donc  $[a, b] \in H$  ce qui entraîne  $D(G) \subseteq H$ . Réciproquement si  $D(G) \subseteq H$ , les commutateurs sont dans  $H$  ce qui veut dire que  
 $\pi([a, b]) = \pi(a) \cdot \pi(b) \cdot \pi(a)^{-1} \cdot \pi(b)^{-1} = \pi(1)$  c'est-à-dire  $\pi(a) \cdot \pi(b) = \pi(b) \cdot \pi(a)$ .
3. Soit  $\varphi : G \rightarrow H$  un isomorphisme.  $\varphi([a, b]) = [\varphi(a), \varphi(b)]$ , donc  $\varphi$  induit par restriction un isomorphisme entre  $D(G)$  et  $D(H)$  d'où un isomorphisme  
 $\phi : G/D(G) \rightarrow H/D(H)$ ,  $\bar{g} \mapsto \overline{\varphi(g)}$ .
4. Démontrons que  $Alt(n) = \{\sigma \in \mathcal{S}_n \mid \varepsilon(\sigma) = 1\}$  est engendré par les 3-cycles. Soit  $(a, b, c)$  un 3-cycle alors  $(a, b, c) = (a, b) \cdot (b, c)$  et donc  $\varepsilon(a, b, c) = \varepsilon(a, b) \cdot \varepsilon(b, c) = 1$  ce qui prouve que les 3-cycles sont dans  $Alt(n) = \{\sigma \in \mathcal{S}_n \mid \varepsilon(\sigma) = 1\}$ . Les transpositions du type  $(1, j)$  engendrent  $\mathcal{S}_n$  en effet  $(i, j) = (1, i) \cdot (1, j) \cdot (1, i)$ . Par conséquent tout élément de  $Alt(n)$  est un produit pair de transpositions du type  $(1, j)$  et donc  $Alt(n)$  est engendré par les permutations du type  $(1, j) \cdot (1, i) = (1, i, j)$  qui sont des 3-cycles. Etant donné que  $\underbrace{(b, c) \cdot (a, b, c) \cdot (b, c)}_{\in D(\mathcal{S}_n)} \cdot (a, b, c)^{-1} = (a, b, c)$  on a

$Alt(n) \subseteq D(\mathcal{S}_n)$ . L'inclusion  $D(\mathcal{S}_n) \subseteq Alt(n)$  est triviale. Donc  $D(\mathcal{S}_n) = Alt(n)$ . On a l'homomorphisme surjectif  $\varepsilon : \mathcal{S}_n \rightarrow \{-1,1\}$  qui induit un iso  $\tilde{\varepsilon} : \mathcal{S}_n / \ker(\varepsilon) \rightarrow \{-1,1\}$  or  $\ker(\varepsilon) = Alt(n)$  et  $\{-1,1\} \simeq \mathbb{Z}/2\mathbb{Z}$  donc l'abélianisé de  $\mathcal{S}_n$  est isomorphe à  $\mathbb{Z}/2\mathbb{Z}$ .

**EXERCICE 18.***Niveau* : Premier Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Corps finis et applications polynomiales**Énoncé :**

1. Soit  $\mathbb{K}$  un corps fini. Montrer que toute application  $f : \mathbb{K} \rightarrow \mathbb{K}$  est polynomiale.
2. Si  $\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$  déterminer un polynôme passant par les points:  
(0;1), (1;0), (2;1), (3;0), (4;1).

**Solution :**

1. Si  $\mathbb{K} = \{x_0, \dots, x_{n-1}\}$ ,  $P_j(X) = \frac{\prod_{i \neq j} (X - x_i)}{\prod_{i \neq j} (x_j - x_i)} \in \mathbb{K}[X]$  est un polynôme vérifiant

$P_j(x) = 0$  si  $x \neq x_j$  et 1 sinon. Soit  $f : \mathbb{K} \rightarrow \mathbb{K}$  une application. On a

$$\forall k \in \{0, \dots, n-1\}, f(x_k) = \sum_{j=0}^{n-1} f(x_j) P_j(x_k) \text{ et donc } f = \sum_{j=0}^{n-1} f(x_j) P_j \in \mathbb{K}[X].$$

2. On calcule  $P_0(X) = -X^4 + 1$ ,  $P_2(X) = -X^4 - 2X^3 + X^2 + 2X$ ,  
 $P_4(X) = -X^4 + X^3 - X^2 + X$ . Donc  $f = P_0 + P_2 + P_4 = 2X^4 - X^3 - 2X + 1$  passe par les points voulus.

**EXERCICE 19.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés* : Extensions de corps

---

**Énoncé :**

1. Montrer que le corps  $\mathbb{R}$  n'admet (à isomorphisme près) que  $\mathbb{C}$  comme extension finie de degré supérieur à 1. [Indication: utiliser le fait que tout corps possède une "unique" clôture algébrique].
2. Est-ce que le fait que le corps  $\mathbb{H}$  des quaternions est une extension de degré quatre de  $\mathbb{R}$  est en contradiction avec 1. ?

**Solution :**

1. Soit  $\mathbb{L}$  une extension finie de  $\mathbb{R}$ , de degré supérieur à 1 et  $\mathbb{K}$  la clôture algébrique de  $\mathbb{L}$ . On a la tour d'extension  $\mathbb{R} \subseteq \mathbb{L} \subseteq \mathbb{K}$ . Par transitivité de l'algébricité,  $\mathbb{K}$  est algébrique sur  $\mathbb{R}$  et donc  $\mathbb{K}$  est une clôture algébrique de  $\mathbb{R}$ . Par ailleurs nous savons que  $\mathbb{C}$  est la clôture algébrique de  $\mathbb{R}$ . Par unicité, il existe donc un  $\mathbb{R}$ -isomorphisme entre  $\mathbb{C}$  et  $\mathbb{K}$ . Etant donné que  $\mathbb{C}/\mathbb{R}$  est une extension de degré deux il en résulte que  $\mathbb{K}/\mathbb{R}$  est aussi une extension de degré deux et par suite que  $\mathbb{K}/\mathbb{L}$  est de degré un, c'est-à-dire  $\mathbb{L} = \mathbb{K} \simeq \mathbb{C}$ .
2. Le point 1. montre entre autre que toutes les extensions finies de  $\mathbb{R}$  sont de degré un ou deux. Le fait que  $\mathbb{H}/\mathbb{R}$  soit de degré quatre n'est pas une contradiction, car dans 1. nous avons utilisés des résultats qui implicitement supposent que les corps considérés soient commutatifs or  $\mathbb{H}$  ne l'est pas.

(Remarque: dire que  $\mathbb{L}$  est une extension de  $\mathbb{R}$  signifie qu'il existe un homomorphisme  $\varphi: \mathbb{R} \rightarrow \mathbb{L}$ . Etant donné que les homomorphismes de corps sont tous injectifs, dans la résolution de cet exercice nous avons utilisé l'abus d'écriture  $\mathbb{R} \subseteq \mathbb{L}$  qui consiste à identifier  $\mathbb{R}$  et  $\varphi(\mathbb{R})$  sous-corps de  $\mathbb{L}$ .)

**EXERCICE 20.***Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Modules**Énoncé :**

Soit  $A$  un anneau commutatif unitaire et  $X, Y, Z$  trois  $A$ -modules. Soit  $0 \rightarrow X \xrightarrow{i} Y \xrightarrow{j} Z \rightarrow 0$  une suite exacte.

1. Montrer que  $Y/i(X) \simeq Z$ .
2. Montrer que s'il existe un morphisme  $s: Z \rightarrow Y$  tel que  $j \circ s = id_Z$  alors  $Y \simeq i(X) \oplus Z$ .
3. Donner un exemple pour lequel  $Y$  n'est pas isomorphe à  $i(X) \oplus Z$ .

**Solution :**

1.  $j$  étant surjective induit un isomorphisme  $Y/Ker(j) \rightarrow Z$ . Mais  $Ker(j) = i(X)$  et donc  $Y/i(X) \simeq Z$ .
2. Soit  $s: Z \rightarrow Y$  un morphisme tel que  $j \circ s = id_Z$ . Nous considérons le morphisme  $\varphi: i(X) \oplus Z \rightarrow Y$  défini par  $\varphi(i(x) + z) = i(x) + s(z)$ .  $\varphi$  est injectif, en effet,  $\varphi(i(x) + z) = i(x) + s(z) = 0 \Rightarrow j(i(x)) + j(s(z)) = 0 \Rightarrow z = 0$ . Montrons que  $\varphi$  est surjectif. Soit  $y \in Y$ ,  $j(s(j(y)) - y) = j(y) - j(y) = 0$ . Donc  $s(j(y)) - y \in Ker(j) = Im(i)$  et par suite il existe  $x \in X$  tel que  $s(j(y)) - y = i(x)$ , c'est-à-dire  $y = s(j(y)) - i(x) = \varphi(i(-x) + j(y))$ .
3.  $0 \rightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{j} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$  est suite exacte mais  $\mathbb{Z} \neq 2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .

**EXERCICE 21.***Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Anneaux noethériens**Énoncé :**

On dit qu'un anneau commutatif unitaire  $A$  est noethérien si tout idéal de  $A$  est de type fini c'est-à-dire engendré par un nombre fini d'éléments.

1. Montrer que  $\mathbb{Z}$  est noethérien.
2. Montrer que si  $\mathbb{K}$  est un corps alors  $\mathbb{K}[X]$  est noethérien.
3. Démontrer l'équivalence suivante:  $A$  noethérien  $\Leftrightarrow$  toute suite croissante d'idéaux  $I_1 \subseteq I_2 \subseteq \dots$  est stationnaire ( il existe  $n \in \mathbb{N}$  tel que  $I_{n+k} = I_n$  pour tout  $k \geq 0$  ).
4. Donner un exemple d'anneau non noethérien.

**Solution :**

1.  $\mathbb{Z}$  est principal, à fortiori il est noethérien.
2. Si  $\mathbb{K}$  est un corps, on sait que  $\mathbb{K}[X]$  est principal donc noethérien.
3. Supposons  $A$  noethérien. Soit  $I_1 \subseteq I_2 \subseteq \dots$  une suite croissante d'idéaux. On remarque que l'union  $I = \bigcup_{k \geq 1} I_k$  est encore un idéal. Si  $a_1, \dots, a_m$  engendrent  $I$  alors il existe  $n \geq 1$  tel que  $\{a_1, \dots, a_m\} \subseteq I_n$ , ce qui entraîne  $I_n = I$  et donc  $I_{n+j} = I$  pour tout  $j \geq 0$ . Réciproquement, soit  $I$  un idéal de  $A$  et  $a_1 \in I$ . Si  $I$  n'est pas de type fini on peut construire une suite de la façon suivante:  $a_2 \in I \setminus a_1 \cdot A$ ,  $a_3 \in I \setminus (a_1 \cdot A + a_2 \cdot A)$ , ... Ainsi  $I_n := a_1 A + \dots + a_n A$  est une suite strictement croissante d'idéaux, ce qui est absurde, donc  $I$  est de type fini.
4.  $\mathbb{K}[X_1, X_2, \dots]$  est non noethérien. En effet si l'on note par  $(X_1, \dots, X_k)$  l'idéal engendré par  $X_1, \dots, X_k$ ,  $(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \dots$  constitue une suite strictement croissante d'idéaux.

**EXERCICE 22.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés* : Anneaux noethériens

---

**Énoncé :**

Démontrer qu'un quotient d'un anneau noethérien est noethérien.

**Solution :**

Soit  $A$  un anneau noethérien et  $I$  un idéal de  $A$ . Soit  $\pi : A \rightarrow A/I$  la projection canonique et  $J_1 \subseteq J_2 \subseteq \dots$  une suite croissante d'idéaux de  $A/I$ .  $\pi^{-1}(J_1) \subseteq \pi^{-1}(J_2) \subseteq \dots$  est donc une suite croissante d'idéaux de  $A$  et  $A$  étant noethérien, il existe  $N$  tel que  $\pi^{-1}(J_N) = \pi^{-1}(J_{N+k})$  pour tout  $k \geq 0$ . Par suite,

$$\forall k \geq 0, \pi(\pi^{-1}(J_N)) = J_N = \pi(\pi^{-1}(J_{N+k})) = J_{N+k}.$$

Ce qui prouve que  $A/I$  est noethérien.

**EXERCICE 23.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés* : Produit d'anneaux et idéaux

---

**Énoncé :**

Soit  $A_1, \dots, A_n$  des anneaux commutatifs unitaires et  $A = A_1 \times \dots \times A_n$  l'anneau produit. Montrer que les idéaux de  $A$  sont de la forme  $I_1 \times \dots \times I_n$  avec  $I_j$  idéal de  $A_j$ .

**Solution :**

On voit facilement que  $I_1 \times \dots \times I_n$  est un idéal de  $A$ . Il faut montrer que tous les idéaux de  $A$  sont de cette forme. Soit  $I$  un idéal de  $A$ , notons  $p_k : A \rightarrow A_k$ ,  $1 \leq k \leq n$ , la  $k$ -ème projection. Pour tout  $1 \leq k \leq n$ ,  $p_k(I)$  est un idéal de  $A_k$ . Notons  $I_k := p_k(I)$  cet idéal. Nous avons évidemment l'inclusion  $I \subseteq I_1 \times \dots \times I_n$ . Réciproquement, si  $(a_1, \dots, a_n) \in I_1 \times \dots \times I_n$  alors il existe  $x_1, \dots, x_n \in I$  tels que  $p_k(x_k) = a_k$ . Notant  $e_k = (0, \dots, 0, 1, 0, \dots, 0)$  avec 1 à la  $k$ -ème place, nous avons  $(a_1, \dots, a_n) = \sum_{k=1}^n e_k \cdot x_k \in I$ . Donc  $I_1 \times \dots \times I_n \subseteq I$  et par suite  $I_1 \times \dots \times I_n = I$ .

**EXERCICE 24.***Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Anneaux noethériens**Énoncé :**Soit  $A$  un anneau commutatif unitaire.

1. Montrer que si  $A$  est noethérien, tout homomorphisme surjectif  $\varphi : A \rightarrow A$  est un isomorphisme.
2. Montrer que 1. est équivalent à dire  $\forall I$  idéal de  $A, A \simeq A/I \Leftrightarrow I = \{0\}$ .
3. Donner un exemple qui montre que si  $A$  n'est pas noethérien 1. est faux. [Indication: considérer l'anneau  $\mathbb{K}[X_1, X_2, \dots]$ ].

**Solution :**

1. Soit  $A$  noethérien et  $\varphi : A \rightarrow A$  un homomorphisme surjectif. Posons  $\varphi^n := \varphi \circ \dots \circ \varphi$   $n$  fois. On a la suite croissante d'idéaux:  $\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \dots$ .  $A$  étant noethérien, il existe un entier  $N$  tel que  $\ker(\varphi^N) = \ker(\varphi^{N+k})$  pour tout  $k \geq 0$ . Soit  $x \in \ker(\varphi)$ ,  $\varphi^N$  est surjective et donc il existe  $y \in A$  tel que  $\varphi^N(y) = x$ , par suite  $\varphi^{N+1}(y) = \varphi(x) = 0$  et étant donné que  $\ker(\varphi^N) = \ker(\varphi^{N+1})$  on a  $\varphi^N(y) = x = 0$ . Ainsi  $\ker(\varphi) = \{0\}$  ce qui montre que  $\varphi$  est injective donc un isomorphisme.
2. Supposons que tout homomorphisme  $\varphi : A \rightarrow A$  surjectif soit un isomorphisme et soit  $I$  un idéal pour lequel il existe un isomorphisme  $\psi : A/I \rightarrow A$  alors  $\psi \circ \pi : A \rightarrow A$  est un homomorphisme surjectif de noyau  $I$  (où  $\pi : A \rightarrow A/I$  est la projection canonique). Donc  $\psi \circ \pi$  est un isomorphisme et par conséquent  $I = \{0\}$ . On a donc montré que 1. entraîne  $A \simeq A/I \Leftrightarrow I = \{0\}$ . Réciproquement si  $A \simeq A/I \Leftrightarrow I = \{0\}$  est vérifié soit  $\varphi : A \rightarrow A$  un homomorphisme surjectif,  $\varphi$  induit un isomorphisme  $A/\ker(\varphi) \rightarrow A$  et donc par hypothèse  $\ker(\varphi) = \{0\}$ , c'est-à-dire  $\varphi$  est un iso.
3. Soit  $\mathbb{K}$  un corps. Considérons l'anneau  $\mathbb{K}[X_1, X_2, \dots]$  et l'homomorphisme surjectif  $\varphi : \mathbb{K}[X_1, X_2, \dots] \rightarrow \mathbb{K}[X_1, X_2, \dots]$  défini par  $\varphi(X_{2n}) = X_n, \varphi(X_{2n+1}) = 0$ .  $\varphi$  n'est visiblement pas un isomorphisme.

**EXERCICE 25.**

Niveau : Deuxième Cycle

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés : Caractères, groupe dual

**Énoncé :**

Soit  $G$  un groupe. Un *caractère* est un homomorphisme  $\chi : G \rightarrow \mathbb{C}^*$ . L'ensemble des caractères de  $G$  est noté  $\widehat{G}$ , c'est le *dual* de  $G$ .

1. Montrer que  $\widehat{G}$  est un groupe abélien pour la multiplication des fonctions.
2. Montrer que si  $G$  et  $H$  sont deux groupes alors  $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$ .
3. Montrer que  $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$ . En déduire que si  $G$  est abélien fini  $\widehat{\widehat{G}} \simeq G$ . [Indication: utiliser le théorème de structure des groupes abéliens finis].
4. Montrer que pour  $G$  fini on a  $\widehat{G} \simeq G/D(G)$  où  $D(G)$  est le groupe dérivé. [Indication: commencer par montrer que  $\widehat{G} \simeq \widehat{G/D(G)}$ ].
5. Déterminer le groupe  $\widehat{G}$  où  $G = \mathcal{S}_n$ .

**Solution :**

1. Le caractère constant égal à 1 noté  $\mathbf{1}$  est l'élément neutre de  $\widehat{G}$ . Si  $\chi : G \rightarrow \mathbb{C}^*$  est un caractère alors  $\chi^{-1} : G \rightarrow \mathbb{C}^*, g \mapsto \chi(g)^{-1}$  est l'inverse de  $\chi$ .  $\mathbb{C}^*$  étant abélien, il en résulte que  $\widehat{G}$  l'est aussi.
2. Considérons l'homomorphisme  $\psi : \widehat{G} \times \widehat{H} \rightarrow \widehat{G \times H}$  défini par  $\psi(\chi_G, \chi_H)(g, h) = \chi_G(g) \cdot \chi_H(h)$ . Si pour tout  $(g, h) \in G \times H$ ,  $\psi(\chi_G, \chi_H)(g, h) = 1$  alors en particulier pour tout  $g \in G$ ,  $\psi(\chi_G, \chi_H)(g, h) = \chi_G(g) \cdot \chi_H(1) = \chi_G(g) = 1$  donc  $\chi_G = \mathbf{1}$ . Le même raisonnement montre que  $\chi_H = \mathbf{1}$ , donc que  $\psi$  est injective.  $\psi$  est surjective car si  $\chi \in \widehat{G \times H}$  les caractères définis par  $\chi_G : G \rightarrow \mathbb{C}^*, g \mapsto \chi(g, 1)$  et  $\chi_H : H \rightarrow \mathbb{C}^*, h \mapsto \chi(1, h)$  vérifient  $\psi(\chi_G, \chi_H) = \chi$ .
3. Soit  $\chi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^*$  un homomorphisme.  $\chi(\bar{1})$  est une racine  $n$ -ème de l'unité, par suite  $\chi(\bar{k}) = \exp(2\pi i k/n)$  avec  $0 \leq k \leq n-1$  et  $\chi(\bar{j}) = \exp(2\pi i j k/n)$ . Nous avons donc un homomorphisme surjectif  $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow \widehat{\mathbb{Z}/n\mathbb{Z}}$ ,  $\varphi(\bar{k})(\bar{j}) = \exp(2\pi i j k/n)$ .  $\varphi$  est injectif car  $\bar{k} \in \ker(\varphi) \Leftrightarrow \exp(2\pi i k/n) = 1 \Leftrightarrow n | k \Leftrightarrow \bar{k} = \bar{0}$ . Donc  $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$ . Si  $G$  est un groupe abélien fini, nous savons par le théorème de structure que  $G$  est isomorphe à un produit du type  $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$  avec  $n_j \geq 2$  par suite en utilisant 2. on a,  $\widehat{G} \simeq \widehat{\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}} \simeq \widehat{\mathbb{Z}/n_1\mathbb{Z}} \times \dots \times \widehat{\mathbb{Z}/n_k\mathbb{Z}} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \simeq G$

4. Soit  $\chi \in \widehat{G}$ .  $D(G)$  est contenu dans  $\ker(\chi)$ , par suite il existe un unique morphisme  $\widehat{\chi} : G/D(G) \rightarrow \mathbb{C}^*$  tel que,  $\chi = \widehat{\chi} \circ \pi$  où  $\pi : G \rightarrow G/D(G)$  est la projection canonique. L'application  $\widehat{G} \rightarrow \widehat{G/D(G)}, \chi \mapsto \widehat{\chi}$  est un isomorphisme. En effet  $\alpha \cdot \beta = \widehat{\alpha \cdot \beta} \circ \pi$  d'une part et  $\alpha \cdot \beta = (\widehat{\alpha} \circ \pi) \cdot (\widehat{\beta} \circ \pi) = (\widehat{\alpha} \cdot \widehat{\beta}) \circ \pi$  d'autre part, l'unicité de  $\widehat{\alpha \cdot \beta}$  implique donc  $\widehat{\alpha \cdot \beta} = \widehat{\alpha} \cdot \widehat{\beta}$ , ce qui prouve que l'application en question est un homomorphisme. Si  $\widehat{\chi} = \mathbf{1}$  (où  $\mathbf{1}$  est le caractère constant égal à 1) alors  $\chi = \widehat{\chi} \circ \pi = \mathbf{1}$  et si  $\widehat{\alpha} \in \widehat{G/D(G)}$  alors en posant  $\alpha = \widehat{\alpha} \circ \pi$  nous avons bien un antécédent de  $\widehat{\alpha}$ . Nous avons donc montré que  $\widehat{G} \simeq \widehat{G/D(G)}$  mais comme  $G/D(G)$  est abélien le point 3. nous donne  $\widehat{G} \simeq \widehat{G/D(G)} \simeq G/D(G)$ .
5. L'abélianisé de  $\mathcal{S}_n$  est  $\mathcal{S}_n/D(\mathcal{S}_n) \simeq \mathbb{Z}/2\mathbb{Z}$  par conséquent  $\widehat{\mathcal{S}_n} \simeq \mathbb{Z}/2\mathbb{Z}$ .

**EXERCICE 26.**

*Niveau* : Deuxième Cycle

*Auteur* : Ruben Ricchiuto (30.12.04)

*Mots Clés* : Groupe des automorphismes de  $\mathbb{R}$

---

**Énoncé :**

Montrer que  $Aut(\mathbb{R}) = \{id\}$  où  $Aut(\mathbb{R})$  est le groupe des automorphismes du corps  $\mathbb{R}$ .

**Solution :**

Commençons par remarquer que si  $\varphi \in Aut(\mathbb{R})$  alors  $\forall p, q \in \mathbb{Z}, \varphi(p/q) = p/q$ , en effet  $\varphi(p/q) = \varphi(p)/\varphi(q) = p\varphi(1)/q\varphi(1) = p/q$ . De plus pour  $x \in \mathbb{R}_+$  on a  $\varphi(x) = \varphi(\sqrt{x})^2 \geq 0$  ainsi  $\varphi$  est croissante. Supposons qu'il existe  $x \in \mathbb{R}$  tel que  $\varphi(x) > x$ , alors il existe  $a \in \mathbb{Q}$  tel que  $x < a < \varphi(x)$  et par croissance de  $\varphi$  on aurait  $\varphi(x) < a$  ce qui est absurde. Le même raisonnement s'applique si  $\varphi(x) < x$ . Nous avons donc prouvé que  $Aut(\mathbb{R}) = \{id\}$ .

**EXERCICE 27.***Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Cardinal de l'ensemble des nombres algébriques et transcendants**Énoncé :**

On rappelle qu'un nombre complexe est algébrique si il est racine d'un polynôme appartenant à l'anneau  $\mathbb{Q}[X]$ .

1. Montrer que l'ensemble des nombres réels algébriques est dénombrable.
2. Que peut-on déduire de 1. au sujet de l'ensemble des nombres réels transcendants.

**Solution :**

1. L'ensemble  $\mathcal{P}_n$  des polynômes de degré inférieur ou égal à  $n$  appartenants à  $\mathbb{Q}[X]$  est dénombrable vu qu'il est en bijection avec  $\mathbb{Q}^{n+1}$  et que  $\mathbb{Q}$  est dénombrable. Ainsi l'ensemble  $\mathbb{Q}[X]$  est dénombrable car  $\mathbb{Q}[X] = \bigcup_{n \geq 0} \mathcal{P}_n$ . Soit  $R_n$  l'ensemble des racines complexes des polynômes appartenants à  $\mathcal{P}_n$ . Chaque polynôme ayant un nombre fini de racines dans  $\mathbb{C}$ , il en résulte que  $R_n$  est dénombrable. Par suite si  $\overline{\mathbb{Q}_{\mathbb{C}}}$  est l'ensemble des nombres complexes algébriques, alors  $\overline{\mathbb{Q}_{\mathbb{C}}} = \bigcup_{n \geq 0} R_n$  est dénombrable. Si  $\overline{\mathbb{Q}_{\mathbb{R}}}$  est l'ensemble des nombres réels algébriques alors  $\overline{\mathbb{Q}_{\mathbb{R}}} = \overline{\mathbb{Q}_{\mathbb{C}}} \cap \mathbb{R} \subset \overline{\mathbb{Q}_{\mathbb{C}}}$ . Donc  $\overline{\mathbb{Q}_{\mathbb{R}}}$  est dénombrable.

Sachant que  $\mathbb{R}$  n'est pas dénombrable il en résulte qu'il existe une infinité non dénombrable de nombres réels transcendants.

**EXERCICE 28.***Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Extensions de  $\mathbb{Q}$  et groupe de Galois**Énoncé :**

1. Est-ce que  $\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$  ?
2. Quel est le degré de l'extension  $\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q}$  ?
3. Montrer que  $\mathbb{Q}[\sqrt{3}, \sqrt{5}] = \mathbb{Q}[\sqrt{3} + \sqrt{5}]$ .
4. Déterminer le groupe de Galois de  $\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q}$ .
5. Est-ce que  $\sqrt{8} \in \mathbb{Q}[\sqrt{18}]$  ? Soit  $a, b$  deux nombres entiers positifs tels que  $\sqrt{a}, \sqrt{b} \notin \mathbb{Q}$ . Montrer que  $\mathbb{Q}[\sqrt{a}, \sqrt{b}]/\mathbb{Q}$  est de degré 4 ssi  $\sqrt{a} \cdot \sqrt{b} \notin \mathbb{Q}$ . Montrer de plus que dans ce cas  $\mathbb{Q}[\sqrt{a} + \sqrt{b}] = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$  et que le polynôme minimal de  $\sqrt{a} + \sqrt{b}$  sur  $\mathbb{Q}$  est  $p(X) = X^4 - 2(a+b)X^2 + (a-b)^2$ .

**Solution :**

1.  $\sqrt{3}$  a  $X^2 - 3$  comme polynôme minimal ce qui montre que  $\mathbb{Q}[\sqrt{3}]$  est un  $\mathbb{Q}$ -espace vectoriel de dimension deux et  $\{1, \sqrt{3}\}$  est une base de  $\mathbb{Q}[\sqrt{3}]$ . Si  $\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$  alors il existe  $a, b \in \mathbb{Q}$  tels que  $\sqrt{5} = a + b\sqrt{3}$ . En élevant au carré on obtient  $5 = a^2 + 3b^2 + 2ab\sqrt{3}$  ce qui entraîne  $5 = a^2 + 3b^2$  et  $ab = 0$ .  $b = 0$  est impossible car sinon  $5 = a^2$  et par suite  $\sqrt{5} \in \mathbb{Q}$ , absurde.  $a = 0$  est aussi impossible car sinon  $5 = 3b^2$ . Or si  $b = p/q$  avec  $p, q \in \mathbb{Z}$  premiers entre eux la dernière égalité nous donne  $5q^2 = 3p^2$  et donc  $p^2$  divise 5 ce qui implique  $p = \pm 1$ . Le même raisonnement avec  $q$  donne  $q = \pm 1$ . Ainsi  $b = \pm 1$  ce qui est absurde. En conclusion  $\sqrt{5} \notin \mathbb{Q}[\sqrt{3}]$ .
2. Le polynôme  $X^2 - 5$  est irréductible sur  $\mathbb{Q}[\sqrt{3}]$  car autrement  $\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$ . Ainsi  $\mathbb{Q}[\sqrt{3}][\sqrt{5}] = \mathbb{Q}[\sqrt{3}, \sqrt{5}]$  est une extension de degré deux de  $\mathbb{Q}[\sqrt{3}]$ . Etant donné que  $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$  est aussi une extension de degré deux et que l'on a la tour  $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}] \subset \mathbb{Q}[\sqrt{3}, \sqrt{5}]$ ,  $\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q}$  est une extension de degré quatre.
3. On a la tour d'extensions  $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3} + \sqrt{5}] \subseteq \mathbb{Q}[\sqrt{3}, \sqrt{5}]$ . Vu que  $\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q}$  est une extension de degré quatre,  $\mathbb{Q}[\sqrt{3} + \sqrt{5}]/\mathbb{Q}$  est de degré deux ou quatre. On calcule  $(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{3}\sqrt{5} = 2 + 2\sqrt{3}(\sqrt{3} + \sqrt{5})$ , par suite  $(\sqrt{3} + \sqrt{5})^2 - 2\sqrt{3}(\sqrt{3} + \sqrt{5}) - 2 = 0$ . Ainsi  $\sqrt{3} + \sqrt{5}$  est racine du polynôme  $X^2 - 2\sqrt{3} \cdot X - 2 \in \mathbb{Q}[\sqrt{3}][X]$ . Ce polynôme est irréductible dans  $\mathbb{Q}[\sqrt{3}][X]$  car autrement  $\sqrt{3} + \sqrt{5} \in \mathbb{Q}[\sqrt{3}]$  et par suite  $\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$ , ce qui n'est pas le cas. Donc

$q(X) = X^2 - 2\sqrt{3} \cdot X - 2$  est le polynôme minimal de  $\sqrt{3} + \sqrt{5}$  sur  $\mathbb{Q}[\sqrt{3}]$ . Si  $p(X)$  est le polynôme minimal de  $\sqrt{3} + \sqrt{5}$  sur  $\mathbb{Q}$  on a  $\deg(p) = 2$  ou  $4$  et  $q$  divise  $p$  dans  $\mathbb{Q}[\sqrt{3}][X]$ . Par conséquent  $\deg(p) = 4$  sinon  $p = q$ . Ainsi  $\mathbb{Q}[\sqrt{3} + \sqrt{5}]/\mathbb{Q}$  est de degré quatre ce qui prouve que  $\mathbb{Q}[\sqrt{3} + \sqrt{5}] = \mathbb{Q}[\sqrt{3}, \sqrt{5}]$ .

4.  $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3} \cdot \sqrt{5}\}$  est une base du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$  et les  $\mathbb{Q}$ -automorphismes de  $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$  sont  $\{\varphi_0, \varphi_1, \varphi_2, \varphi_1 \circ \varphi_2\}$  avec  $\varphi_0 = id$ ,

$$\varphi_1 = \begin{cases} \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}, \quad \varphi_2 = \begin{cases} \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}. \text{ Il n'y en a pas d'autres car}$$

$$|\text{Gal}(\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q})| \leq 4. \text{ Ainsi}$$

$$\text{Gal}(\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q}) = \{\varphi_0, \varphi_1, \varphi_2, \varphi_1 \circ \varphi_2\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

$\frac{3}{2}\sqrt{8} = \sqrt{18}$ , donc  $\sqrt{8} \in \mathbb{Q}[\sqrt{18}]$ . Soit  $a, b$  deux nombres entiers positifs tels que  $\sqrt{a}, \sqrt{b} \notin \mathbb{Q}$ . L'extension  $\mathbb{Q}[\sqrt{a}, \sqrt{b}]/\mathbb{Q}$  est de degré quatre ssi  $\sqrt{b} \notin \mathbb{Q}[\sqrt{a}]$  en effet dans ce dernier cas le polynôme  $X^2 - b$  est irréductible sur  $\mathbb{Q}[\sqrt{a}]$ , donc  $\mathbb{Q}[\sqrt{a}, \sqrt{b}]/\mathbb{Q}[\sqrt{a}]$  est de degré deux et vu que  $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{a}] \subseteq \mathbb{Q}[\sqrt{a}, \sqrt{b}]$ ,  $\mathbb{Q}[\sqrt{a}, \sqrt{b}]/\mathbb{Q}$  est de degré quatre. Or  $\sqrt{b} \in \mathbb{Q}[\sqrt{a}] \Leftrightarrow$  il existe  $x, y \in \mathbb{Q}$  tels que  $\sqrt{b} = x + y\sqrt{a}$  car  $\{1, \sqrt{a}\}$  est une base du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{Q}[\sqrt{a}]$ . En élevant la dernière égalité au carré nous obtenons  $b = x^2 + ay^2 + 2xy\sqrt{a}$ , donc  $xy = 0$ , mais  $y \neq 0$  sinon  $\sqrt{b} = x \in \mathbb{Q}$ . Donc  $x = 0$  et  $\sqrt{b}/\sqrt{a} = y \in \mathbb{Q}$ . Ainsi  $\sqrt{b} \in \mathbb{Q}[\sqrt{a}] \Leftrightarrow \sqrt{b}/\sqrt{a} \in \mathbb{Q}$ , par suite l'extension  $\mathbb{Q}[\sqrt{a}, \sqrt{b}]/\mathbb{Q}$  est de degré quatre ssi  $\sqrt{b}/\sqrt{a} \notin \mathbb{Q}$ . Or  $\sqrt{b}/\sqrt{a} \notin \mathbb{Q} \Leftrightarrow \sqrt{b} \cdot \sqrt{a} \notin \mathbb{Q}$ . Supposons cette condition vérifiée. On calcule:  $(\sqrt{a} + \sqrt{b})^2 = a + b + 2\sqrt{a}\sqrt{b} = -a + b + 2\sqrt{a}(\sqrt{a} + \sqrt{b})$ ,  $\sqrt{a} + \sqrt{b}$  est racine de  $q(X) = X^2 - 2\sqrt{a}X + a - b \in \mathbb{Q}[\sqrt{a}][X]$  qui est par conséquent irréductible sur  $\mathbb{Q}[\sqrt{a}]$ , ce qui prouve que  $\sqrt{a} + \sqrt{b}$  est de degré quatre sur  $\mathbb{Q}$  et donc que  $\mathbb{Q}[\sqrt{a} + \sqrt{b}] = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$ . De plus on calcule  $(\sqrt{a} + \sqrt{b})^4 = 2(a+b)(\sqrt{a} + \sqrt{b})^2 - (a-b)^2$ , donc  $\sqrt{a} + \sqrt{b}$  est racine de  $X^4 - 2(a+b)X^2 + (a-b)^2 \in \mathbb{Q}[X]$  qui est le polynôme minimal de  $\sqrt{a} + \sqrt{b}$  sur  $\mathbb{Q}$ .