

1.  $\sqrt{2}$ ,  $\sqrt{3}$ ,  $\sqrt[4]{2}$  sont respectivement racines des polynômes  $X^2 - 2$ ,  $X^2 - 3$  et  $X^4 - 2$ . Ce sont donc des nombres algébriques

2. Si  $q \in \mathbb{Q}$  alors  $q$  est racine de  $X - q$ .

3. Si  $P$  est un polynôme annulateur non nul de  $x$  alors  $P(X^2)$  est un polynôme annulateur non nul de  $\sqrt{x}$ .

4. L'ensemble  $\mathcal{D}$  est non vide. En effet, puisque  $a$  est algébrique, il existe un polynôme annulateur non nul. Donc d'après l'axiome de la borne supérieure dans  $\mathbb{N}$ , l'ensemble  $\mathcal{D}$  admet un minimum.

5. D'après la question précédente, il existe un polynôme  $P$  de  $\mathcal{P}$  de degré  $n$ . Posons  $\mu = \frac{1}{c}P$  où  $c$  est le coefficient dominant de  $P$ . Comme  $P(a) = 0$ , on a aussi  $\mu(a) = 0$ ;  $\mu$  est donc dans  $\mathcal{P}$  de coefficient dominant 1. Pour l'unicité, choisissons deux polynômes unitaires  $P_1$  et  $P_2$  de  $\mathcal{P}$  ayant un degré égal à  $n$ . Effectuons la division euclidienne de  $P_1$  par  $P_2$ . On obtient :

$$P_1 = QP_2 + R$$

Puis en appliquant  $a$ , on obtient  $R(a) = 0$ . Ainsi  $R$  est un polynôme annulateur de  $a$ . S'il est non nul son degré est dans  $\mathcal{D}$  et est donc plus grand ou égal à  $n$ , ce qui est absurde; donc  $R = 0$  et  $P_1 = QP_2$ . En appliquant le degré à cette équation, on trouve que  $\deg(Q) = 0$  et en regardant les coefficients dominants, on trouve  $Q = 1$ .

6. L'ensemble  $(\mu)$  est non vide puisqu'il contient  $\mu$ , il est bien inclus dans  $\mathbb{Q}[X]$  par définition. Il reste à voir la stabilité par combinaison linéaire. Soit  $\lambda_1, \lambda_2$  dans  $\mathbb{Q}$  et  $P_1\mu, P_2\mu$  dans  $(\mu)$ , alors :

$$\lambda_1 P_1 \mu + \lambda_2 P_2 \mu = (\lambda_1 P_1 + \lambda_2 P_2) \mu \in (\mu)$$

7. Montrons tout d'abord que  $(\mu) \subset \mathcal{P}$ . Soit  $P\mu$  dans  $(\mu)$  alors  $(P\mu)(a) = P(a) \cdot \mu(a) = 0$ . Donc  $P\mu$  est bien dans  $\mathcal{P}$ .

Réciproquement, montrons que  $\mathcal{P} \subset (\mu)$ . Pour cela considérons  $P$  un polynôme annulateur de  $a$  et effectuons la division euclidienne de  $P$  par  $\mu$  : il existe donc  $Q$  dans  $\mathbb{Q}[X]$  et  $R$  dans  $\mathbb{Q}_{n-1}[X]$  tels que  $P = Q\mu + R$ . En appliquant  $a$ , on obtient  $R(a) = 0$ . Comme dans la question précédente, on en déduit que  $R = 0$  et donc que  $P$  est un multiple de  $\mu$ .

8. Tout d'abord de manière évidente  $1 \in L$  et  $L$  est stable par différence.

Montrons que  $L$  est stable par produit. Soient  $x_1 + y_1\sqrt{2}$  et  $x_2 + y_2\sqrt{2}$  dans  $L$ , alors :

$$(x_1 + y_1\sqrt{2}) \times (x_2 + y_2\sqrt{2}) = (x_1x_2 + 2y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{2} \in L$$

Montrons que  $L$  est stable par inverse. Soient  $x + y\sqrt{2}$  dans  $L$  non nul :

$$\frac{1}{x + y\sqrt{2}} = \frac{x - y\sqrt{2}}{(x + y\sqrt{2})(x - y\sqrt{2})} = \left( \frac{x}{x^2 - 2y^2} \right) + \left( \frac{-y}{x^2 - 2y^2} \right) \sqrt{2} \in L$$

**9.** Soit  $L$  un sous-corps de  $\mathbb{R}$ . Montrons tout d'abord par récurrence que :

$$\forall n \in \mathbb{N}, n \in L$$

Pour l'initialisation,  $1 \in L$  et  $0 = 1 - 1 \in L$  car  $L$  est stable par différence. Supposons que pour  $n$  fixé dans  $\mathbb{N}$  on ait  $n \in L$ . Comme 0 et 1 sont dans  $L$ , alors  $-1 = 0 - 1$  est encore dans  $L$ . Enfin :

$$n + 1 = n - (-1) \in L$$

La propriété est donc vérifiée pour tout  $n$  de  $\mathbb{N}$  et  $\mathbb{N} \subset L$ .

De plus pour tout  $n$  de  $\mathbb{N}$  :  $-n = 0 - n \in L$  par différence d'élément de  $L$ . Ainsi  $\mathbb{Z} \in L$ . Enfin pour toute fraction  $\frac{p}{q}$  de  $\mathbb{Q}$ , on a :

$$\frac{p}{q} = p \times \frac{1}{q} \in L$$

par stabilité par inverse et produit. On a donc  $\mathbb{Q} \subset L$ .

**10.**  $K(a)$  est non vide puisqu'il contient 1 (le polynôme 1 appliqué à  $a$ ). De plus il est inclus dans  $\mathbb{R}$  par définition. Par ailleurs, si  $P_1(a)$  et  $P_2(a)$  sont dans  $K(a)$ , alors

$$\lambda_1 P_1(a) + \lambda_2 P_2(a) = (\lambda_1 P_1 + \lambda_2 P_2)(a) \in K(a)$$

puisque :

$$\deg(\lambda_1 P_1 + \lambda_2 P_2) \leq \max(\deg(P_1), \deg(P_2)) \leq n - 1$$

Ainsi, d'après le théorème de caractérisation,  $K(a)$  est un sous-espace vectoriel de  $\mathbb{R}$ .

**11.** On effectue la division euclidienne de  $P_1 P_2$  par  $\mu$ , on obtient :  $P_1 P_2 = A\mu + Q$ . En appliquant  $a$ , on obtient  $P_1(a)P_2(a) = Q(a)$  où  $Q$  est bien de degré inférieur ou égal à  $n - 1$  puisque c'est le reste de la division euclidienne par  $\mu$ . Ainsi  $K(a)$  est bien stable par produit.

**12.** Tout d'abord, montrons que la famille est libre. Soient  $\lambda_0, \dots, \lambda_{n-1}$  dans  $K$  tels que :

$$\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \dots + \lambda_{n-1} a^{n-1} = 0$$

Posons  $P = \lambda_0 + \dots + \lambda_{n-1} X^{n-1}$ , on a donc  $P(a) = 0$ . Ainsi  $P$  est un polynôme annulateur de  $a$ , c'est donc un multiple de  $\mu$ . Cependant  $\deg(\mu) = n$  et  $\deg(P) \leq n - 1$  ; on a donc forcément  $P = 0$ .

De plus la famille est génératrice puis si  $b$  est dans  $K(a)$ , il existe un polynôme  $P = \lambda_0 + \lambda_1 X + \dots + \lambda_{n-1} X^{n-1}$  tel que  $b = P(a) = \lambda_0 + \lambda_1 a + \dots + \lambda_{n-1} a^{n-1}$

**13.** Tout d'abord  $\phi$  est clairement une application linéaire puisque pour tout  $\lambda_1, \lambda_2$  dans  $K$  et  $x_1, x_2$  dans  $K(a)$ , on a :

$$\phi(\lambda_1 x_1 + \lambda_2 x_2) = b(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 b x_1 + \lambda_2 b x_2 = \lambda_1 \phi(x_1) + \lambda_2 \phi(x_2)$$

De plus  $\phi$  est injective puisque son noyau est réduit à  $\{0\}$ . En effet :

$$\phi(x) = 0 \implies bx = 0 \implies x = 0$$

Enfin l'espace de départ et l'espace d'arrivée sont de même dimension finie, donc  $\phi$  est automatiquement surjective.

**14.** Comme  $\phi$  est bijective, 1 doit avoir un antécédent. Il existe donc  $c$  dans  $K(a)$  tel que  $bc = 1$ . Comme le produit est commutatif, on a aussi  $cb = 1$ . Ainsi  $b$  est inversible et  $K(a)$  est un sous-corps de  $\mathbb{R}$ .

**15.** Soit  $L$  un corps contenant  $K$  et  $a$ . Puisque  $L$  est stable par produit, il contient aussi  $1, a, \dots, a^n$ . De plus, on peut le considérer comme un  $K$ -espace vectoriel, il est donc stable par combinaison linéaire. Ainsi pour tout polynôme  $P$ , on a  $P(a)$  dans  $L$  et donc  $K(a)$  est inclus dans  $L$ . Tout sous-corps contenant  $K$  et  $a$  contient également  $K(a)$ ; le corps  $K(a)$  est donc le plus petit corps contenant à la fois  $K$  et  $a$ .

**16.** Montrons tout d'abord que la famille est libre. Pour considérons l'expression :

$$0 = \sum_{i=1}^p \sum_{j=1}^q \lambda_{ij} e_i f_j = \sum_{j=1}^q \left( \sum_{i=1}^p \lambda_{ij} e_i \right) f_j$$

Comme la famille  $(f_j)$  est libre, on a pour tout  $j$  de  $\{1, \dots, q\}$  :

$$\sum_{i=1}^p \lambda_{ij} e_i = 0$$

On utilise ensuite que la famille  $(e_i)$  est libre et on obtient  $\lambda_{ij} = 0$  pour tous  $i, j$  convenables.

Montrons ensuite que la famille est génératrice. Soit  $x$  dans  $K_2$ , décomposons-le dans la base  $(f_j)$  :

$x = \sum_{j=1}^q \alpha_j f_j$ . Puis décomposons chaque  $\alpha_j$  de  $K_1$  dans la base  $(e_i)$ . On obtient :

$$x = \sum_{j=1}^q \left( \sum_{i=1}^p \lambda_{ij} e_i \right) f_j = \sum_{i=1}^p \sum_{j=1}^q \lambda_{ij} e_i f_j$$

**17.** On utilise la question précédente avec  $K_1 = \mathbb{Q}$ ,  $K_2 = \mathbb{Q}(a_1)$  et  $K_3 = \mathbb{Q}(a_1, a_2)$ .

**18.** Ce sont des familles ayant plus de vecteurs que la dimensions de l'espace, elles sont donc liées. Il existe ainsi des polynômes  $P_1$  et  $P_2$  de  $\mathbb{Q}[X]$  non nuls tels que  $P_1(a_1 + a_2) = 0$  et  $P_2(a_1 a_2) = 0$

**19.** L'ensemble  $\mathcal{A}$  est stable par  $+$  et  $\times$  d'après la question précédente et il contient 1.

Montrons que  $\mathcal{A}$  est stable par opposé. Soit  $a$  un nombre algébrique et  $P$  un polynôme annulateur de  $a$ . Alors  $Q = P(-X)$  est un polynôme annulateur de  $-a$  et  $-a$  est algébrique.

Montrons que  $\mathcal{A}$  est stable par inverse. Soit  $a$  un nombre algébrique non nul et  $P$  un polynôme annulateur de  $a$  de degré  $n$ . Alors  $Q = X^n P\left(\frac{1}{X}\right)$  est un polynôme annulateur de  $a^{-1}$  et  $a^{-1}$  est algébrique.

Ainsi par définition,  $\mathcal{A}$  est un sous-corps de  $\mathbb{R}$ .