

## TD13 : EXTENSIONS SÉPARABLES

Diego Izquierdo

*Les exercices 0, 1 et 3 sont à préparer avant la séance de TD. Nous traiterons les exercices dans l'ordre suivant : 0, 1, 3, 10.*

### Exercice 0 : TD12

Faire les exercices 15 et 17 du TD12.

### Exercice 1 : Une infinité d'extensions intermédiaires

Trouver une infinité d'extensions intermédiaires entre  $\mathbb{F}_p(X^p, Y^p)$  et  $\mathbb{F}_p(X, Y)$ . Existe-t'il  $\alpha \in \mathbb{F}_p(X, Y)$  tel que  $\mathbb{F}_p(X, Y) = \mathbb{F}_p(X^p, Y^p)(\alpha)$  ?

**Indications :** On peut prendre les  $\mathbb{F}_p(X^p, Y^p)(X + X^{p^k}Y)$  pour  $k \geq 1$ . Ces derniers sont de dimension  $p$  sur  $\mathbb{F}_p(X^p, Y^p)$  puisque l'on a  $X + X^{p^k}Y \notin \mathbb{F}_p(X^p, Y^p)$  et  $(X + X^{p^k}Y)^p \in \mathbb{F}_p(X^p, Y^p)$ . Aussi, deux tels sous-corps ne sont pas égaux puisque si  $i \neq j$ ,  $X + X^{p^i}Y$  et  $X + X^{p^j}Y$  engendrent  $\mathbb{F}_p(X, Y)$  sur  $\mathbb{F}_p(X^p, Y^p)$  : on a  $Y = (X^{p^i} - X^{p^j})^{-1}((X + X^{p^i}Y) - (X + X^{p^j}Y))$ .

### Exercice 2 : Une extension inséparable en caractéristique 2

Soient  $K = \mathbb{F}_2(X, Y)$ ,  $L = K(\alpha)$  avec  $\alpha^2 + X\alpha + Y = 0$ , et  $M = K(\beta)$  avec  $\beta^2 = \alpha$ . Soit  $K_s$  la clôture séparable de  $K$  dans  $M$ .

1. Montrer que  $[M : K] = 4$ .
2. Montrer que  $K_s = L$ . En déduire  $[K_s : K]$ .
3. Montrer qu'un élément  $\gamma \in M$  vérifie  $\gamma^2 \in K$  si, et seulement si,  $\gamma \in K$ .
4. Montrer qu'il n'existe pas de corps intermédiaire  $K \subsetneq F \subseteq M$  purement inséparable sur  $K$ .

### Exercice 3 : Extensions séparables et degré

Soit  $F \subseteq E$  une extension finie de corps de caractéristique  $p > 0$ .

1. Montrer qu'un élément  $x \in E$  est séparable si et seulement si on a  $F(x) = F(x^p)$ .

**Indications :** Supposons  $x$  séparable sur  $F$ . Le polynôme  $P = X^p - x^p \in F(x^p)[T]$  est soit scindé, soit irréductible. Comme il n'est pas séparable, s'il était irréductible, alors  $x$  ne serait pas séparable sur  $F(x)$  : absurde ! Donc  $P$  est scindé et  $x \in F(x^p)$ . Cela montre que  $F(x) = F(x^p)$ .  
Supposons  $F(x) = F(x^p)$ . Alors il existe  $Q \in F[T]$  tel que  $x = Q(x^p)$ . Donc  $x$  est racine de  $Q(T) - T$ , qui est un polynôme séparable. On en déduit que  $x$  est séparable sur  $F$ .

2. Montrer l'équivalence des assertions suivantes :

- (i) il existe une base  $(x_1, \dots, x_n)$  de  $E$  sur  $F$  telle que  $(x_1^p, \dots, x_n^p)$  est aussi une  $F$ -base de  $E$  ;
- (ii) pour toute base  $(y_1, \dots, y_n)$  de  $E$  sur  $F$ ,  $(y_1^p, \dots, y_n^p)$  est aussi une  $F$ -base de  $E$ .

**Indications :** Supposons (i). Soit  $(y_1, \dots, y_n)$  une  $F$ -base de  $E$ . Il existe des matrices  $A, B \in GL_n(F)$  telles que :

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix}, \quad B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Soit  $Fr$  le Frobenius sur  $E$ . On a alors :

$$\begin{pmatrix} y_1^p \\ \vdots \\ y_n^p \end{pmatrix} = Fr \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = Fr(B)Fr \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = Fr(B)A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Comme  $Fr(B)A \in GL_n(F)$ , on en déduit que  $(y_1^p, \dots, y_n^p)$  est une  $F$ -base de  $E$ .

3. Montrer que (i) est vraie si et seulement si l'extension  $F \subseteq E$  est séparable.

**Indications :** Supposons (i). Alors on a (ii). Soit  $x \in E$ . Soit  $n = [F(x) : F]$ . Il existe une base de  $E$  de la forme  $(x^i \omega_j)_{1 \leq i \leq n, 1 \leq j \leq \lfloor \frac{[E:F]}{n} \rfloor}$  avec  $\omega_1 = 1$ . Par (ii), on sait que  $(x^{pi} \omega_j^p)_{1 \leq i \leq n, 1 \leq j \leq \lfloor \frac{[E:F]}{n} \rfloor}$  est une  $F$ -base de  $E$ . On en déduit que  $(1, x^p, x^{2p}, \dots, x^{(n-1)p})$  est une famille  $F$ -libre de  $F(x)$  : c'est donc une base et on a  $F(x) = F(x^p)$ . La question 1 permet alors de conclure que  $x$  est séparable sur  $F$ .

Réciproquement, supposons que  $E/F$  est séparable. Alors il existe  $x \in E$  tel que  $E = F(x)$ , d'après le théorème de l'élément primitif. Une  $F$ -base de  $E$  est alors donnée par  $(1, x, x^2, \dots, x^{[E:F]-1})$ . Mais d'après la question 1,  $E = F(x) = F(x^p)$ . Donc  $(1, x^p, x^{2p}, \dots, x^{p([E:F]-p)})$  est aussi une  $F$ -base de  $E$ . Donc (i) est vérifiée.

**Exercice 5 : Éléments primitifs**

1. Soit  $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$ . Pour quelles valeurs de  $t \in \mathbb{Q}$  l'élément  $\sqrt[3]{2} + t\rho$  est-il un élément primitif de l'extension  $K/\mathbb{Q}$ ? Et  $\sqrt[3]{2} + t\rho\sqrt[3]{2}$ ?

**Indications :** D'après la démonstration du théorème de l'élément primitif, les valeurs de  $t \in \mathbb{Q}$  telles que l'élément  $\sqrt[3]{2} + tj$  est un élément primitif de l'extension  $K/\mathbb{Q}$  sont celles qui vérifient  $t(j - j^2) = y - \sqrt[3]{2}$  pour  $y \in \{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$  : on peut donc choisir  $t$  dans  $\mathbb{Q} \setminus \{0\}$ .

Les valeurs de  $t \in \mathbb{Q}$  telles que l'élément  $\sqrt[3]{2} + tj\sqrt[3]{2}$  est un élément primitif de l'extension  $K/\mathbb{Q}$  sont celles qui vérifient  $t(j - x) = y - 1$  pour  $x \in \{1, j^2\}$  et  $y \in \{j, j^2\}$  : ce sont donc les rationnels autres que 1.

2. Donner un élément primitif de l'extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ .

**Indications :** Soient  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  et  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ . Comme dans la question 1, on vérifie que  $\sqrt{2} + \sqrt{3}$  est un élément primitif de  $K$ , puis que  $\sqrt{2} + \sqrt{3} + \sqrt{5}$  est un élément primitif de  $L$ .

**Exercice 6 :  $p$ -dimension**

Soit  $F \subseteq E$  une extension finie de corps de caractéristique  $p > 0$ . On suppose l'inclusion  $E^{\times p} \subseteq F^{\times}$ , de sorte que  $F \subseteq E$  est purement inséparable. Appelons famille génératrice de  $E$  toute famille d'éléments  $(x_1, \dots, x_n)$  de  $E$  telle que  $E = F(x_1, \dots, x_n)$ . Montrer que les familles génératrices minimales de  $E$  sont toutes de même cardinal (on pourra calculer le degré de  $[E : F]$ ). On appelle ce cardinal la  $p$ -dimension de  $E/F$ .

**Indications :** Soit  $(x_1, \dots, x_n)$  une famille génératrice minimale. Pour  $0 \leq j \leq n$ , on note  $E_j = F(x_1, \dots, x_j)$ . Pour  $j \leq n - 1$ , on remarque que  $x_{j+1} \notin E_j$  puisque  $(x_1, \dots, x_n)$  est une famille génératrice minimale. De plus, on a  $x_{j+1}^p \in F$ . On en déduit que le polynôme  $X^p - x_{j+1}^p \in E_j$  est irréductible. Donc  $[E_{j+1} : E_j] = p$ . Par conséquent,  $[F : E] = p^n$ . On en déduit que les familles génératrices minimales de  $E$  sont toutes de même cardinal.

**Exercice 7 : Extensions purement inséparables**

Soient  $K$  un corps de caractéristique  $p > 0$ ,  $\overline{K}$  une clôture algébrique de  $K$  et  $K^s$  la clôture séparable de  $K$  dans  $\overline{K}$ .

1. Rappeler pourquoi  $K^s$  est bien définie.

**Indications :** Pour pouvoir considérer  $K^s$  agréablement, il s'agit de vérifier que la composée de deux extensions séparables  $L$  et  $M$  de  $K$  est séparable. Or tout élément  $x$  de  $M$  annule un polynôme séparable de  $K[X]$ , et le polynôme minimal de  $x$  sur  $L$  est aussi séparable. Ceci assure que  $L \subseteq LM$  est séparable. Une extension  $K \subseteq L$  étant séparable si et seulement si on a  $[L : K] = |\text{Hom}_K(L, \overline{K})|$ , l'extension  $K \subseteq L \subseteq LM$  est séparable.

Soit  $P \in K[X]$  un polynôme unitaire irréductible.

2. Montrer que  $P$  a une unique racine dans  $\overline{K}$  si et seulement si il existe  $r \in \mathbb{N}$  et  $a \in K$  tels que  $P = X^{p^r} - a$ .

**Indications :** Si  $P$  est de la forme  $X^{p^r} - a$ , et si  $\alpha$  est une racine de  $P$  dans  $\overline{K}$ , alors on a sur  $\overline{K} : P = (X - \alpha)^{p^r}$ .  
 Réciproquement, si  $P$  a une unique racine  $\alpha$  dans  $\overline{K}$ , alors  $P$  est de la forme  $(X - \alpha)^k$ . Si l'on a  $\alpha \in K$ , par irréductibilité de  $P$ , on a  $k = 1$ . Sinon, comme  $P$  est irréductible et non séparable, on a  $P \in K[X^p]$ , et donc  $k = pk_1$  pour un entier  $k_1 \geq 1$ . On a alors  $P = (X^p - \alpha^p)^{k_1}$ . Mais alors  $P_1 = (X - \alpha^p)^{k_1}$  est un polynôme irréductible avec une unique racine dans  $\overline{K}$ , et par récurrence on obtient  $k = p^r$ .

Soit  $K \subseteq L$  une extension algébrique.

3. Montrer que  $K \subseteq L$  est purement inséparable si et seulement si il n'existe qu'un homomorphisme de  $K$ -algèbres de  $L$  dans  $\overline{K}$ .

**Indications :** Supposons que  $K \subseteq L$  est purement inséparable et qu'il existe deux morphismes de  $K$ -algèbres distincts de  $L$  dans  $\overline{K}$ . Alors il existe  $x \in L$  tel que leurs valeurs en  $x$  diffèrent. Comme  $x$  est algébrique et purement inséparable sur  $K$ , son polynôme minimal  $P$  divise un certain  $X^{p^r_0} - a_0$ . Mais alors  $P$  est irréductible et a une unique racine dans  $\overline{K}$  : par (a), c'est que l'on a  $P = X^{p^r} - a$ . De ce fait on a un unique morphisme de  $K$ -algèbres de  $K(x)$  dans  $\overline{K}$ , ce qui contredit l'hypothèse initiale. On vient de montrer que si  $K \subseteq L$  est purement inséparable, alors on a  $\text{Hom}_K(L, \overline{K}) = \{1\}$ .  
 Réciproquement, s'il n'y a qu'un seul morphisme  $L \rightarrow \overline{K}$ , pour tout  $x \in L$ , il n'y a aussi qu'un seul morphisme de  $K$ -algèbres  $K(x) \rightarrow \overline{K}$ . Cela veut dire que le polynôme minimal de  $x$  sur  $K$  a une unique racine dans  $\overline{K}$  et on conclut par (a).

4. Montrer que  $L$  est une extension purement inséparable de  $K^s \cap L$ .

**Indications :** Par définition,  $K^s \cap L$  est la plus grande sous-extension séparable de  $L$ . En particulier, on a  $\text{Hom}_K(L, \overline{K}) = \text{Hom}_K(K^s \cap L, \overline{K})$ , ce qui veut aussi dire qu'il n'y a qu'un unique  $(K^s \cap L)$ -homomorphisme de  $L$  dans  $\overline{K}$ . En effet, on a l'application de restriction  $\text{Hom}_K(L, \overline{K}) \rightarrow \text{Hom}_K(K^s \cap L, \overline{K})$ , qui est surjective (parce qu'il existe des prolongements de morphismes). Supposons qu'elle n'est pas injective : il existe alors un  $x \notin K^s \cap L$  et deux morphismes  $L \rightarrow \overline{K}$  qui envoient  $x$  sur des images distinctes. On peut supposer  $x$  de degré minimal sur  $K^s \cap L$ , ce que l'on va faire. On considère alors le polynôme  $P := \prod_{\varphi} (X - \varphi(x))$  où  $\varphi$  parcourt les morphismes  $L \rightarrow \overline{K}$  ayant des valeurs distinctes en  $x$  (il y en a un nombre fini du fait que  $x$  est algébrique). Les coefficients de  $P$  sont dans un sous-corps strict  $M$  de  $(K^s \cap L)(x)$  (puisque les  $\varphi$  ne diffèrent pas sur  $M$ ). On a alors l'alternative suivante : ou bien  $M = K^s \cap L$  et  $x$  est alors séparable, ce qui est absurde; ou bien  $M \supsetneq K^s \cap L$  est séparable puisque  $x$  a été choisi de degré minimal parmi les non séparables, et c'est aussi absurde. Par (c),  $K^s \cap L \subseteq L$  est purement inséparable.

On note  $L^{\text{rad}}$  le sous-corps de  $L$  constitué de tous les éléments  $x \in L$  tels qu'il existe  $r \in \mathbb{N}$  avec  $x^{p^r} \in K$ .

5. Montrer que  $\overline{K}$  est une extension séparable de  $\overline{K}^{\text{rad}}$ .

**Indications :** Comme  $x \mapsto x^p$  est surjectif sur  $\overline{K}^{\text{rad}}$ , tout polynôme irréductible non séparable serait de la forme  $P = a_n X^{np} + a_{n-1} X^{(n-1)p} + \dots + a_0$ ; et en prenant  $b_i^p = a_i$ , on a  $P = (b_n X^n + b_{n-1} X^{n-1} + \dots + b_0)^p$ , qui n'est donc pas irréductible. C'est que toute extension finie de  $\overline{K}^{\text{rad}}$  est séparable. Comme  $\overline{K}^{\text{rad}} \subseteq \overline{K}$  est algébrique, elle est ainsi séparable.

6. Est-ce vrai pour  $L \subsetneq \overline{K}$  et  $L^{\text{rad}}$  ?

**Indications :** Supposons  $p > 2$  et considérons

$$K = \overline{\mathbb{F}_p}(t) \subseteq M = D_K(X^2 - X + t) \subseteq L = D_M(X^p - \alpha) \subseteq \overline{K},$$

où  $\alpha \in M$  est une racine de  $X^2 - X + t$ . Parce que l'on a  $\Delta = 1 - 4t \notin K^{\times 2} \cup \{0\}$ ,  $M$  est une extension de degré 2 de  $K$  et  $L = D_M(X^p - \alpha)$  est de degré  $p$  ( $X^p - \alpha$  est irréductible car une racine n'est pas dans  $M$  car non dans  $L$ , et est de degré un diviseur de  $p$ ). L'extension  $K \subseteq L$  est visiblement non séparable et il y a deux

morphismes dans  $\text{Hom}_K(L, \overline{K}) : Id$  et  $\sigma : x \mapsto \frac{t^{1/p}}{x}$  où  $x$  est zéro de  $X^{2p} - X^p + t$ .

A cause du (c), ces morphismes sont aussi dans  $\text{Hom}_{L^{\text{rad}}}(L, \overline{K}) = \text{Aut}_{L^{\text{rad}}} L$ . En

particulier, on a  $L^{\text{rad}} \subseteq L^\sigma = K\left(x + \frac{t^{1/p}}{x}\right)$ . Or  $x + \frac{t^{1/p}}{x}$  vérifie  $\left(x + \frac{t^{1/p}}{x}\right)^p =$

$x^p + \frac{t}{x^p} = 1$ , et donc on a  $x + \frac{t^{1/p}}{x} = 1$ , de sorte que  $L^{\text{rad}}$  est  $K$ . De ce fait,  $L$  n'est pas une extension séparable de  $L^{\text{rad}}$ .

On remarquera a posteriori que cet exemple repose crucialement sur le fait que  $K \subseteq L$  n'est pas normale.

**Exercice 8 : Plus grand sous-corps parfait**

Soient  $n$  un entier naturel et  $q$  une puissance d'un nombre premier. Quel est le plus grand sous-corps parfait de  $\mathbb{F}_q(X_1, \dots, X_n)$  ?

**Indications :** Soit  $K$  un sous-corps parfait de  $L = \mathbb{F}_q(X_1, \dots, X_n)$ . Soient  $p$  un nombre premier et  $n > 0$  tels que  $q = p^n$ . On sait que  $K$  est de caractéristique  $p > 0$ , et que  $K^p = K$ . On en déduit que  $K$  est contenu dans  $\bigcap_{r \geq 0} L^{p^r} \subseteq \mathbb{F}_q[X_1, \dots, X_n]^\times \cup \{0\} = \mathbb{F}_q$ . Comme les corps finis sont parfaits, le plus grand sous-corps parfait de  $\mathbb{F}_q(X_1, \dots, X_n)$  est  $\mathbb{F}_q$ .

**Exercice 9 : Un exemple de corps parfait**

Donner un exemple de corps parfait infini de caractéristique positive non séparablement clos.

**Indications :** Prendre par exemple  $K = \mathbb{F}_3(X, X^{1/3}, X^{1/3^2}, \dots)$ . C'est un corps de caractéristique 3, parfait car  $K^3 = K$ , non séparablement clos car le polynôme séparable  $T^2 - X$  est irréductible sur  $K$ .

**Exercice 10 : Sous-corps d'un corps parfait**

1. Soit  $M$  un corps de caractéristique  $p$ . Soient  $n$  un entier naturel et  $a \in M$ . Montrer que si  $a$  n'est pas une puissance  $p$ -ième dans  $M$ , alors le polynôme  $X^{p^n} - a$  est irréductible sur  $M$ .
2. Soit  $L/K$  une extension de corps telle que  $L$  est parfait. Montrer que, si  $[L : K] < \infty$ , alors  $K$  est parfait. Que dire si  $[L : K] = \infty$  ?

**Exercice 11 : Extensions de type fini d'un corps parfait**

Soit  $L$  une extension de type fini d'un corps parfait  $K$  de caractéristique  $p > 0$ . Montrer que  $[L : L^p] < \infty$ .

**Indications :** En procédant par récurrence, il faut montrer que, si  $K$  est un corps de caractéristique  $p > 0$  tel que  $[K : K^p] < \infty$  et si  $L$  est une extension de  $K$  pour laquelle il existe  $x \in L$  tel que  $L = K(x)$ , alors  $[L : L^p] < \infty$ . On a :

$$[K(x) : K(x)^p] = [K(x) : K(x^p)][K(x^p) : K^p(x^p)] \leq [K(x) : K(x^p)][K : K^p] < \infty.$$

### Exercice 12 : Partiel 2012

Le résultat de cet exercice est important, mais il n'est pas essentiel d'en connaître la preuve. Soit  $L/K$  une extension algébrique de corps. On suppose que tout polynôme de  $K[X]$  a une racine dans  $L$ . On veut montrer que  $L$  est une clôture algébrique de  $K$ .

1. Montrer la conclusion si on suppose de plus que tout polynôme de  $K[X]$  est scindé dans  $L$ .
2. Montrer la conclusion si on suppose de plus que  $K$  est parfait.
3. On suppose à partir de maintenant que la caractéristique de  $K$  est  $p > 0$ . Montrer que  $M = \{x \in L \mid \exists n \in \mathbb{N}^*, x^{p^n} \in K\}$  est un sous-corps parfait de  $L$ .
4. En déduire que  $L$  est un corps parfait.
5. Montrer que tout polynôme de  $M[X]$  a une racine dans  $L$ . Conclure.

**Indications :** Voir le corrigé du partiel 2012.

### Exercice 13 : Produits tensoriels de corps dans le cas non séparable

Calculer  $\mathbb{F}_p(t^{1/p}) \otimes_{\mathbb{F}_p(t)} \mathbb{F}_p(t^{1/p})$ .

**Indications :** On a :

$$\begin{aligned} \mathbb{F}_p(t^{1/p}) \otimes_{\mathbb{F}_p(t)} \mathbb{F}_p(t^{1/p}) &\cong \mathbb{F}_p(t)[X]/(X^p - t) \otimes_{\mathbb{F}_p} \mathbb{F}_p(t)[X]/(X^p - t) \\ &\cong \mathbb{F}_p(t)[X, Y]/(X^p - t, Y^p - t) \cong \mathbb{F}_{p^p}[Z]/(Z^p). \end{aligned}$$

**Bonne vacances et bonnes fêtes !**