Examen première session, théorie des corps, mai 2024

Durée : 3 heures

Exercice 1.

(a) n est une puissance de la caractéristique, et il ne peut pas être une puissance de 2 puisqu'il est impair.

(b) Comme la caractéristique est différente de 2, tout $x \in F\backslash\{0\}$ est différent de son opposé. L'ensemble $F\backslash\{0\}$ se partage donc en ensembles de la forme $\{x, -x\}$, or $x + (-x) = 0$.

(c) Soit G le groupe multiplicatif $F^\times$. L'application $f : G \to G$ définie par $f(x) = x^2$ est un morphisme de groupe (facile). Le noyau a deux éléments ± 1, parce que $x^2 = 1$ si et seulement si $(x-1)(x+1) = 0$, et on a $1 \neq -1$ parce que la caractéristique est non nulle. Par le théorème d'isomorphisme l'image de f a $|F^\times|/2$ éléments. Comme 0 est aussi un carré, il y a $\frac{n-1}{2}+1$ carrés dans F.

Exercice 2. (a) Posons $x := \sqrt{1+\sqrt{3}}$. x vérifie $(x^2-1)^2 = 3$, donc $x^4 - 2x^2 - 2 = 0$. Le polynôme $P(X) := X^4 - 2X^2 - 2$ est irréductible par le critère d'Eisenstein. Comme il est unitaire, c'est le polynôme minimal de x.

Ses quatre racines sont $\pm x$ et $\pm y$ avec $y := i\sqrt{\sqrt{3}-1}$ (se calculent en posant $u := X^2$ et en calculant d'abord les racines de $u^2 - 2u - 2$).

(b) C'est 4 parce que c'est le degré de P.

(c) On a $xy = i\sqrt{2}$, donc $i\sqrt{2} \in E$. La même relation montre que $E = \mathbb{Q}(x, i\sqrt{2})$ contient y, et donc $-x$ et $-y$.

(d) $i\sqrt{2}$ n'appartient pas à $\mathbb{Q}(x)$ parce que ce n'est pas un nombre réel. Donc $X^2 + 2$ est irréductible sur $\mathbb{Q}(x)$, donc $[\mathbb{Q}(x, i\sqrt{2}) : \mathbb{Q}(x)] = 2$. La réponse est donc 8.

(e) Le groupe $Gal(E/\mathbb{Q})$ a 8 éléments parce que c'est le groupe de Galois d'une extension *galoisienne* de degré 8.

Solution courte par la théorie des groupes : puisque E contient une extension non galoisienne de $\mathbb{Q}$ (à savoir $\mathbb{Q}(x)$), la correspondance de Galois nous dit que le groupe de Galois contient un sous-groupe non distingué et on sait que le seul groupe à 8 éléments qui contient un sous-groupe non distingué est le groupe diédral à 8 éléments.

Solution calculatoire : tout élément de $Gal(E/\mathbb{Q})$ est déterminé par l'image de x qui doit appartenir à $\{\pm x, \pm y\}$ et l'image de $z := i\sqrt{2}$ qui doit appartenir à $\pm z$. Donc on a au plus 8 possibilités. Or, $Gal(E/\mathbb{Q})$ a 8 éléments, on a donc toutes les possibilités. Soit σ l'unique élément de $Gal(E/\mathbb{Q})$ qui vérifie $\sigma(x) = y$ et $\sigma(i\sqrt{2}) = -i\sqrt{2}$. Alors $\sigma(xy) = -xy$. Donc $\sigma(y) = -x$. Donc σ n'est pas d'ordre 2. Comme $\sigma^4 = Id$ (facile), σ est d'ordre 4. De plus, si $\tau \in Gal(E/\mathbb{Q})$ est l'unique élément qui vérifie $\tau(x) = x$ et $\tau(z) = -z$, alors on a $\tau(y) = -y$ et un calcul sur x et z montre que $\tau\sigma\tau^{-1}(x) = \sigma^{-1}$. Donc $Gal(E/\mathbb{Q})$ est isomorphe au groupe diédral à 8 éléments.

Exercice 3. (a) Soit $\sigma \in G$. Tout d'abord, on a

$$\{\sigma(\sigma_j(x))\}_{j=1,2,\dots,k} \subset \{\tau(x)\}_{\tau\in G} = \{\sigma_j(x)\}_{j=1,2,\dots,k}.$$

Parce que σ est bijective, le cardial de l'ensemble de gauche est k tout comme le cardinal de l'ensemble de droite, donc $\{\sigma(\sigma_j(x))\}_{j=1,2,\dots,k} = \{\sigma_j(x)\}_{j=1,2,\dots,k}$.

L'application de $E[X]$ dans $E[X]$ qui à un polynôme $P(X) = \sum_{i=0}^m a_i X^i$ associe $\sum_{i=0}^m \sigma(a_i)X^i$ est un K morphisme d'algèbres et envoie donc P_x sur $\prod_{j=1}^k (X - \sigma(\sigma_j(x))) = P_x$ (par le paragraphe précédent), donc tous les coefficients de P_x sont fixés par tout élément de G et se trouvent dans K par définition de K.

(b) Soit $Q \in K[X]$ le polynôme minimal de x sur K. En particulier, Q divise P_x. $Q(x) = 0$, donc $Q(\sigma(x)) = 0$ pour tout $\sigma \in G$. Donc toutes les racines de P_x sont racines de Q. Mais les racines $\sigma_j(x)$, $j = 1, 2, ..., k$ de P_x sont distinctes donc Q est divisible par P_x. Or, Q divise P_x. Comme Q et P_x sont unitaires, on a $Q = P_x$.

(c) D'après ce qui précède, le polynôme minimal sur K de tout élément $x \in E$ est séparable. Doc E/K est séparable.

Soit $P \in K[X]$ un polynôme irréductible qui a une racine x dans E. Alors $P = P_x$ et donc P est scindé sur E. Doc E/K est normale.

On a $[K(x) : K] = \deg(P_x) = k \leq n$.

(d) Attention, on ne sait pas si l'extension est finie, donc on ne peut pas directement dire qu'elle est monogène. Pesez au premier exemple d'extension algébrique infinie vue en cours (avec les racines de 2), elle n'est pas monogène bien que séparable.

Soit p le plus grand entier tel qu'il existe une extension monogène $K(x)$ de K dans E de degré p. Un tel p existe parce que toutes sont de degré $\leq$. Soit alors x justement tel que $[K(x) : K] = p$. Nous affirmons que $K(x) = E$. En effet, supposons par l'absurde qu'il existe $y \in E \backslash K(x)$. Alors y est algébrique sur K par (a), et donc $K(x, y)$ est une extension finie de K, qui de plus est séparable parce que E/K est séparable, et qui est donc monogène par le théorème de l'élément primitif. Or, $[K(x, y) : K] > [K(x) : K]$ parce que $y \notin K(x)$. Contradiction.

(e) On a $G \subset Gal(E/K)$ parce que tous les éléments de G fixent tous les éléments de K par définition de K. Or, $|Gal(E/K)| \leq [E : K]$ par le cours, et donc $n = |G| \leq |Gal(E/K)| \leq [E : K] \leq n$. On a donc des égalités partout, et par inclusion et égalité de cardiaux on a $G = Gal(E/K)$.