

Algèbre 2^e année

Corrigé 13

1. Soit E le corps de rupture de $t^n - a$ sur F . Soit p la caractéristique de F . Puisque $p \nmid n$, les éléments $\omega, \dots, \omega^{n-1}$ sont distincts. Si $0 \leq k \leq n-1$, alors $(\alpha\omega^k)^n - a = 0$. Par conséquent, $\alpha, \alpha\omega, \dots, \alpha\omega^{n-1}$ sont n racines distinctes de $t^n - a$. Il s'ensuit que

$$t^n - a = \prod_{j=0}^{n-1} (t - \alpha\omega^j)$$

et donc $E \subset F(\alpha, \omega)$. Par contre, E contient toute racine de $t^n - a$, alors $\alpha \in E$. De plus, $\alpha\omega$ est une racine, donc il appartient à E . Donc $\omega = (\alpha\omega)\alpha^{-1} \in E$. Par conséquent, $E = F(\alpha, \omega)$.

2. (a) $t^2 - 3 = (t + i\sqrt{3})(t - i\sqrt{3})$ alors $\mathbf{Q}(i\sqrt{3})$ est le corps de rupture de degré 2.
- (b) $\mathbf{Q}(i)$ est le corps de rupture de $t^2 + 1$ sur \mathbf{Q} . Soit ω une racine cubique primitive. On note $\alpha = \sqrt[3]{2}$. Par l'exercice 1, $[\mathbf{Q}(i)](\alpha, \omega)$ est le corps de rupture de $(t^3 - 2)$ sur $\mathbf{Q}(i)$, donc $E = \mathbf{Q}(i, \alpha, \omega)$ est le corps de rupture de $(t^3 - 2)(t^2 + 1)$. Pour trouver le degré, on remarque que $t^3 - 2$ est irréductible sur $\mathbf{Q}(i)$, $t^3 - 2 = (t - \alpha)(t^2 + \alpha t + \alpha^2)$, et $t^2 + \alpha t + \alpha^2$ est irréductible sur $\mathbf{Q}(\alpha, i)$. Donc $[E : \mathbf{Q}] = [E : \mathbf{Q}(\alpha, i)][\mathbf{Q}(\alpha, i) : \mathbf{Q}(i)][\mathbf{Q}(i) : \mathbf{Q}] = 2 \cdot 3 \cdot 2 = 12$.
- (c) Si on met $x = t^3$, on trouve le polynôme $x^2 - 2x + 3 = (x - 1)^2 + 2$. Les racines sont $\beta = 1 + i\sqrt{2}$ et $\bar{\beta} = 1 - i\sqrt{2}$. Soit ω une racine cubique d'unité et soit $\alpha \in \mathbf{C}$ tel que $\alpha^3 = \beta$. Il s'ensuit que $\bar{\alpha}^3 = \bar{\beta}$. Alors $\alpha, \alpha\omega, \alpha\omega^2, \bar{\alpha}, \bar{\alpha}\omega, \bar{\alpha}\omega^2 = \overline{\alpha\omega^2}$, $\bar{\alpha}\omega^2 = \overline{\alpha\omega}$ sont six racines distinctes de $t^6 - 2t^3 + 3$. Donc $E \subset \mathbf{Q}(\alpha, \bar{\alpha}, \omega)$ où E est le corps de rupture. Puisque α et $\bar{\alpha}$ sont des racines du polynôme, $\mathbf{Q}(\alpha, \bar{\alpha}) \subset E$. Puisque $\bar{\alpha}$ et $\bar{\alpha}\omega$ sont des racines, $\bar{\alpha}^{-1}\bar{\alpha}\omega = \omega \in E$. Par conséquent, $E = \mathbf{Q}(\alpha, \bar{\alpha}, \omega)$.
- On remarque que $\mathbf{Q} \subset \mathbf{Q}(\beta) \subset \mathbf{Q}(\alpha)$. Les polynômes minimaux de $\mathbf{Q}(\beta)$ sur \mathbf{Q} et de $\mathbf{Q}(\alpha)$ sur $\mathbf{Q}(\beta)$ sont $t^2 - 2t + 3$ et $t^3 - \beta$, respectivement. Alors $[\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}(\beta)][\mathbf{Q}(\beta) : \mathbf{Q}] = 3 \cdot 2 = 6$.
- Sur $\mathbf{Q}(\alpha)$, $t^3 - \bar{\beta}$ est irréductible. (Pourquoi?) Alors $[\mathbf{Q}(\alpha, \bar{\alpha}) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \bar{\alpha}) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = 3 \cdot 6 = 18$. Donc $[E : \mathbf{Q}] = [\mathbf{Q}(\alpha, \bar{\alpha}, \omega) : \mathbf{Q}(\alpha, \bar{\alpha})][\mathbf{Q}(\alpha, \bar{\alpha}) : \mathbf{Q}] = 3 \cdot 18 = 54$.
3. (a) Soit $f_n(t) = t^{p^n} - t$. Alors la dérivée de $f(t)$ est $Df(t) = -1$. Or, $f(t)$ a une racine multiple ssi il existe $g(t)$ tel que $\deg g(t) > 0$ et $g(t) \mid f(t)$ et $g(t) \mid Df(t)$. Puisque $\deg Df(t) = 0$, il s'ensuit que toute racine de $f(t)$ est simple.

- (b) Soit $\eta : \mathbf{Z} \rightarrow K$ l'homomorphisme d'anneaux défini par $\eta(1) = 1$. Alors $\ker \eta = (p)$ pour un certain premier p . L'homomorphisme η détermine une extension de corps $\bar{\eta} : \mathbf{F}_p \cong \mathbf{Z}/p\mathbf{Z} \rightarrow K$. On pose $n = [K : \mathbf{F}_p]$, d'où $\sharp(K) = p^n$. Si $\alpha \in K^*$, alors $\alpha^{p^n-1} = 1$. Par conséquent, α est une racine de $f_n(t)$. Il s'ensuit que

$$f_n(t) = \prod_{\alpha \in K} (t - \alpha).$$

Donc K est le corps de rupture de $f_n(t)$ et chaque élément de K est une racine de $f_n(t)$.

- (c) Posons $V = V_K(f_n)$. C'est clair que 0 et $1 \in V$. Puisque la caractéristique de K est p , on a $(u+v)^p = u^p + v^p$ pour tous $u, v \in K$. Alors $u-v \in V$ si $u, v \in V$ et V est un sous-groupe additif de K . Si $u, v \in V$, alors $u = u^{p^n}$ et $v = v^{p^n}$. Donc $uv = u^{p^n}v^{p^n} = (uv)^{p^n}$ et $uv \in V$. Par conséquent V est un sous-anneau de K . Si $u \in \mathbf{F}_p$, alors $u^p = u$, donc $u^{p^n} = u$ et $u \in V$. Alors $\mathbf{F}_p \subset V \subset K$. Par l'exercice 6 de la série 12, V est un corps. Puisque f_n est un polynôme de degré p^n duquel toute racine est simple, et K en est le corps de rupture, V a p^n éléments. Les corps V et K sont tous les deux corps de rupture donc $V = K$. Évidemment, $[K : \mathbf{F}_p] = n$. Si K' est un autre corps de rupture, alors $V_{K'}(f_n) = K' \cong K = V_K(f_n)$.
- (d) Soit K un corps fini. Par (b) il existe un premier p et un entier n tel que K est un corps de rupture de $f_n \in \mathbf{F}_p[t]$. Par (c), $K \cong \mathbf{F}_{p^n}$.
4. (a) On utilise l'exercice 1. Pour trouver une racine de $t^4 - 3$, il faut la construire. Le polynôme n'a aucune racine dans \mathbf{F}_7 . Si $t^4 - 3$ est réductible alors c'est le produit de deux polynômes irréductible de degré deux et on vérifie directement que cela n'est pas le cas. Alors $E = \mathbf{F}_7[t]/(t^4 - 3)$ est un corps et l'image canonique α de t dans E est une racine de $t^4 - 3$. On écrit $E = \mathbf{F}_7(\alpha)$. Ensuite il faut trouver une quatrième racine primitive d'unité, mais c'est facile : $t^2 + 1$ est irréductible dans E . On pose ω l'image de t dans le corps $E[t]/(t^2 + 1)$. Alors le corps de rupture de $t^4 - 3$ est $\mathbf{F}_7(\alpha, \omega)$.
- (b) $t^3 + t^2 + t + 1 = (t+1)(t^2 + 1)$. Le corps de rupture est $\mathbf{F}_{13}(\omega) = \mathbf{F}_{13}[t]/(t^2 + 1)$.
5. (a) On écrit $f(t) = a_0 + a_1t + \dots + a_nt^n$. Puisque α est une racine de $f(t)$, $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. En y appliquant σ ,

$$\begin{aligned} \sigma(a_0 + a_1\alpha + \dots + a_n\alpha^n) &= \sigma(0) \\ a_0 + a_1\sigma(\alpha) + \dots + a_n\sigma(\alpha)^n &= 0 \end{aligned}$$

puisque σ est un homomorphisme d'anneaux qui fixe F . Par conséquent, $f(\sigma(\alpha)) = 0$, c-à-d $\sigma(\alpha)$ est une racine de $f(t)$.

- (b) $\sigma : \mathbf{C} \rightarrow \mathbf{C}$, $\sigma(z) = \bar{z}$, est un automorphisme de \mathbf{C} qui fixe \mathbf{Q} (en fait, il fixe \mathbf{R}). Alors le résultat s'ensuit de (a).