Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 10

Exercice 1.
Soit $n > 0$ un entier positif. Montrez que $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont des nombres algébriques sur $\mathbb{Q}$.

Solution.
Comme (formules de partie réelles et imaginaires d'un nombre complexe)

$$\cos(2\pi/n) = \frac{e^{2\pi i/n} + ie^{-2\pi i/n}}{2} \quad \sin(2\pi/n) = \frac{e^{2\pi i/n} - e^{-2\pi i/n}}{2i}$$

on voit que $\cos(2\pi/n), \sin(2\pi/n) \in \mathbb{Q}(i, e^{2\pi i/n})$, ce qui conclut.

Exercice 2. 1. Montrez que $1, \sqrt[3]{2}, \sqrt[3]{4}$ est une $\mathbb{Q}$ base de $\mathbb{Q}(\sqrt[3]{2})$.

2. Écrivez la matrice de la multiplication par

$$1 + \sqrt[3]{2} + \sqrt[3]{4},$$

vue comme application linéaire $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$. Calculez le polynôme caractéristique de cette matrice et déduisez en le polynôme minimal de l'élément ci-dessus.

Solution. Le premier point suit par exemple de l'isomorphisme $\mathbb{Q}[t]/(t^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$ par $t \mapsto \sqrt[3]{2}$. Dans la description par quotient, on voit que l'image de $1, t, t^2$ forme une $\mathbb{Q}$-base.

Pour le deuxième point, la matrice est

$$\begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Le polynôme caractéristique de cette matrice est

$$X^3 - 3X^2 - 3X - 1.$$

Par Cayley-Hamilton l'endomorphisme de multiplication par $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est annulé par ce polynôme. En évaluant en 1 cet endormophisme, on conclut que $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est un zéro de ce polynôme. Comme $1 + \sqrt[3]{2} + \sqrt[3]{4} \notin \mathbb{Q}$ on a forcément que $\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$ car comme $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ il n'y a pas de sous-extensions propres car le degré d'une sous-extension propre diviserait 3. Ainsi le degré du polynôme minimal de $1 + \sqrt[3]{2} + \sqrt[3]{4}$ est 3, ce qui conclut.

Exercice 3.
Soit $\xi = e^{\frac{2\pi i}{n}}$ pour un entier $n > 2$. Démontrez que les corps de décomposition de $x^n - 2$ et de $x^{2n} - 3x^n + 2$ sur $\mathbb{Q}$ sont isomorphes entre eux, et aussi isomorphes à

$$\mathbb{Q}(\xi, \sqrt[n]{2}) \subseteq \mathbb{C}.$$

Solution. Note that the complex roots of $x^2 - 2$ are of the form $e^{\frac{2\pi ik}{n}}\sqrt{2}$ for $0 \leq k < n$. Moreover, note that $x^{2n} - 3x^n + 2$ can be factorized as $x^{2n} - 3x^n + 2 = (x^n - 2)(x^n - 1)$. We can then conclude that the splitting fields are the same and they are given by $\mathbb{Q}(\xi, \sqrt[n]{2})$.

Exercice 4.
Soit $f = x^7 - y^5 \in \mathbb{C}[x, y]$. Le but de cet exercice est de démontrer que f est irréductible dans $\mathbb{C}[x, y]$. Soit $K = \mathbb{C}(y)$ et L le corps de décomposition de f sur K. Soit α une racine de f dans L, et $\beta = \frac{\alpha^3}{y^2}$.

1. Montrez que $[K(\beta) : K] = 7$. *Indication: Trouvez un polynôme sur K dont β est une racine.*
2. Montrez que $K(\beta) = K(\alpha)$.
3. Déduisez que f est irréductible dans $\mathbb{C}[x, y]$.

Solution.

1. We show that the minimal polynomial $m_{\beta,K} = x^7 - y \in K[x]$. It holds that the polynomial vanishes at β, since
$$\beta^7 - y = \left(\frac{\alpha^3}{y^2}\right)^7 - y = \frac{(\alpha^7)^3}{y^{14}} - y \overset{*}{=} \frac{(y^5)^3}{y^{14}} - y = y - y = 0,$$
where in the equation $*$, we use the fact that α is a root of f in L, and hence $\alpha^7 = y^5$. Furthermore, the polynomial is irreducible in $K[x]$: We use Gauss III to deduce that f is irreducible in $K[x] = (\mathbb{C}(y))[x]$ if and only if f is irreducible in $(\mathbb{C}[y])[x]$. Since y is irreducible in $\mathbb{C}[y]$, we may use Eisenstein with $p = y$ to deduce that $x^7 - y$ is irreducible in $(\mathbb{C}[y])[x]$, and hence in $K[x]$. This proves that the minimal polynomial $m_{\beta,K} = x^7 - y \in K[x]$. We conclude that $[K(\beta) : K] = 7$.

2. To show that $K(\alpha) = K(\beta)$, we show that $K(\alpha) \subseteq K(\beta)$ and $K(\beta) \subseteq K(\alpha)$.
We note that
$$\beta^5 = \left(\frac{\alpha^3}{y^2}\right)^5 = \frac{\alpha^{15}}{(y^5)^2} = \frac{\alpha^{15}}{(\alpha^7)^2} = \alpha.$$
From this, it follows that $\alpha = \beta^5 \in K(\beta)$, and hence $K(\alpha) \subseteq K(\beta)$. On the other hand, $\beta = \frac{\alpha^3}{y^2} \in K(\alpha)$, and hence $K(\beta) \subseteq K(\alpha)$.

3. We first remark that by Gauss III, f is irreducible in $\mathbb{C}[x, y] = (\mathbb{C}[y])[y]$ if and only if f is irreducible in $(\mathbb{C}(y))[x] = K[x]$. By the first and second part of this exercise, it holds that $[K(\alpha) : K] = 7$. From this, it follows that the degree of the minimal polynomial $m_{\alpha,K}$ is 7. Now since α is a root of $x^7 - y^5 \in K[x]$, it follows that $m_{\alpha,K} | x^7 - y^5$. Since both polynomials are of degree 7, it follows that $m_{\alpha,K} \sim x^7 - y^5$, and from $m_{\alpha,K}$ being irreducible in $K[x]$ it follows that $x^7 - y^5$ is irreducible in $K[x]$ as well. Applying Gauss III, with $x^7 - y^5$ being primitive, it follows that $x^7 - y^5$ is irreducible in $\mathbb{C}[x, y]$.

Exercice 5. 1. Considérons la situation suivante:

- $\phi : K \to K'$ est un isomorphisme des corps,
- $K \subseteq L$ et $K' \subseteq L'$ sont deux extensions de corps
- $L = K(\alpha)$ et $L' = K'(\alpha')$ avec α et α' algébriques sur K et K' respectivement
- si $\xi : K[x] \to K'[x]$ est l'isomorphisme induit par ϕ, alors $\xi(m_{\alpha,K}) = m_{\alpha',K'}$

Démontrez qu'il existe une extension unique de ϕ à un isomorphisme $\eta : L \to L'$ tel que $\eta(\alpha) = \alpha'$

2. Démontrez que $K(x)[\sqrt{x+1}] \cong K(x)[\sqrt{x+2}]$
3. Démontrez que $K(x, y)[\sqrt{xy}] \cong K(x, y)[\sqrt{x(x+y)}]$

Solution.

1. Use the following isomorphisms to define $\eta : K(\alpha) \to K'(\alpha')$
$$K(\alpha) \cong K[x]/(m_{\alpha,K}) \cong K'[x]/(\xi(m_{\alpha,K})) \cong K'[x]/(m_{\alpha',K'}) \cong K'(\alpha')$$
This shows that $L \cong L'$, so we have proven the existence of η. The uniqueness follows from the fact L is generated by K and α by definition, so knowing the image of K and that of α entirely determines the image of L.

2. Consider the $\phi\colon K(x) \to K(x)$ given by $x \mapsto x+1$. This isomorphism is induced by the universal property of polynomial rings and of fraction fields, and also that it is an isomorphism because it has an inverse given by $x \mapsto x-1$.

   Let $K = K' = K(x)$, $L = K(x)(\sqrt{x+1})$ and $L' = K(x)[\sqrt{x+2}]$. Then ϕ sends the minimal polynomial of $\sqrt{x+1}$ to that of $\sqrt{x+2}$, so by (1) we deduce that $L \cong L'$.

3. Use point (1) and the same idea as in (2) with the automorphism $K(x,y) \to K(x,y)$ given by $x \mapsto x$ and $y \mapsto x+y$, here the inverse is $x \mapsto x$ and $y \mapsto y-x$.

Exercice 6.
Soit $n \geq 1$ un entier. On dit qu'une racine n-ième de l'unité $\xi \in \mathbb{C}$ est primitive si n est le plus petit entier tel que $\xi^n = 1$. On pose,

$$\Phi_n(t) = \prod_{\substack{\xi \text{ racine} \\ \text{primitive} \\ n\text{-ième} \\ \text{de l'unité}}} (t-\xi) \in \mathbb{C}[t].$$

1. Montrer que $t^n - 1 = \prod_{d|n} \Phi_d(t)$ et que $\Phi_n(t) \in \mathbb{Z}[t]$.

2. Soit p un nombre premier et $n \geq 1$. En utilisant le critère d'Eisenstein et le changement de variable $t \mapsto t+1$, montrer que $\Phi_{p^n}(t)$ est irréductible. (*c.f.* changement de variable et Eisentsein vu en cours)

3. Soit $n \geq 1$ un entier et p un premier qui est premier avec n. On note ξ_n une racine primitive n-ième de l'unité. Soit $m(t) \in \mathbb{Q}[t]$ le polynôme minimal de ξ_n. Montrer que $m(t) \in \mathbb{Z}[t]$. Montrer que si ξ est une racine de $m(t)$, alors ξ^p est une racine de $m(t)$. En déduire que $m(t) = \Phi_n(t)$.

   Indication: on pourra montrer par l'absurde que si ξ^p n'est pas une racine de $m(t)$ alors $t^n - 1$ a une racine double modulo p, ce qui est absurde comme $(n,p) = 1$ (Utiliser la dérivée).

4. Soit p un premier et $n \geq 1$ un entier tel que $(n,p) = 1$. Montrer que si $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p[t]$ alors c'est une racine primitive de l'unité dans $\mathbb{F}_p$, c'est à dire un élément dont l'ordre multiplicatif est n.

   Indication: On considère k le corps de décomposition de $t^n - 1$ sur $\mathbb{F}_p$. On utilise la dérivée pour argumenter qu'il y a n-racines distinctes de ce polynôme dans k. On montre ensuite par récurrence sur les diviseurs $d \mid n$ que les racines de $\overline{\Phi_d(t)}$ dans k sont exactement les racines primitives d-ièmes de l'unité dans k.

5. Montrer qu'il existe une infinité de premiers p tel que $\Phi_n(t)$ a une racine dans $\mathbb{F}_p[t]$. En déduire qu'il existe une infinité de premiers p tel que $p \equiv 1 \mod n$.

   Indication: pour tout m suffisamment grand si un nombre premier p divise $\Phi_n(m!)$ alors $p > m$.

Solution.

1. Notons que comme le produit de toutes les racines n-ièmes de l'unité sont égales au produit des racines primitives d-ièmes pour $d \mid n$, on a

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

   On montre par récurence sur n que $\Phi_n(t)$ a coefficients entiers. Pour $n = 1$, on a $\Phi_1(t) = (t-1)$. Pour $n > 1$ notons que $\Phi_n(t)$ est le résultat de la division euclidienne dans $\mathbb{Z}[t]$ de $t^n - 1$ par $\prod_{d|n, d\neq n} \Phi_d(t)$ et ce dernier polynôme est bel et bien à coefficients entiers par récurence.

2. Notons tout d'abord que
$$t^p - 1 = (t-1)\Phi_p(t),$$
et donc que $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + 1$. Notons également que
$$t^{p^n} - 1 = (t^{p^{n-1}} - 1)\Phi_{p^n}(t),$$
et donc que $\Phi_{p^n}(t) = \Phi_p(t^{p^{n-1}})$. Notons que $\Phi_{p^n}(t+1) \equiv (\Phi_p(t+1))^{p^{n+1}} = t^{p^{n+1}} \mod p$ par le raisonnement de l'exemple vu en cours. Comme de plus le coefficient constant de $\Phi_{p^n}(t+1)$ est égal à p, le critère d'Einsenstein permet de conclure à l'irréductibilité de $\Phi_{p^n}(t)$.

3. Écrivons $t^n - 1 = m(t)g(t)$ avec $g(t) \in \mathbb{Q}$. Comme $m(t)$ et $t^n - 1$ ont coefficients dominant 1, g aussi. Dès lors pour $c, d \in \mathbb{Z}$, on a
$$t^n - 1 = \frac{1}{c}(cm(t))\frac{1}{d}(dg(t)))$$
pour $cm(t), dg(t) \in \mathbb{Z}[t]$ primitifs. Par le lemme de Gauss (version II), on a $\frac{1}{cd} \in \mathbb{Z}^\times$. Donc $\frac{1}{d} = \pm c \in \mathbb{Z}$ et donc $c, d = \pm 1$. Ainsi $m(t) \in \mathbb{Z}[t]$.

Soit ξ une racine quelconque de $m(t)$ et par l'absurde supposons que ξ^p ne soit pas une racine de $m(t)$. Alors si $t^n - 1 = m(t)f(t)$ on a que ξ^p est une racine de $f(t)$. Comme $m(t)$ est irréductible dans $\mathbb{Q}[t]$, notons que c'est aussi le poolynôme minimal de ξ. Dès lors $m(t)|f(t^p)$ dans $\mathbb{Q}[t]$ et donc dans $\mathbb{Z}[t]$ comme ces polynômes sont primitifs. En réduisant modulo p (ce qu'on dénote par $\overline{(-)}$ dans la suite), on voit alors que $\overline{m(t)}|\overline{f(t^p)} = (\overline{f(t)})^p$. Dès lors, $\overline{m(t)}$ et $\overline{f(t)}$ ont une racine commune, car les racines (sans compter les multiplicités) de $\overline{f(t)}$ et $(\overline{f(t)})^p$ sont les mêmes. Mais comme $\overline{t^n - 1} = \overline{m(t)f(t)}$ n'as pas de racine multiple comme $(n, p) = 1$, on obtient une contradiction.

Notons que toute racine primitive n-ième de l'unité est de la forme $\xi_n^{p_1 \cdots p_r}$ avec $(p_i, n) = 1$. On obtient par récurence sur r que toute racine primitive n-ième de l'unité est une racine de $m(t)$ et donc que $\Phi_n(t) = m(t)$.

4. Notons k le corps de décomposition de $\overline{t^n - 1} \in \mathbb{F}_p[t]$. On montre par récurence croissante sur les diviseurs d de n que les racines de $\overline{\Phi_d(t)}$ dans k sont exactement les racines primitives d-ième de l'unité. Pour $d = 1$, l'assertion est vérifiée car $\overline{\Phi_1(t)} = \overline{t-1}$. Traitions le pas d'induction. Comme $(p, d) = 1$ le polynôme $\overline{t^d - 1} \in \mathbb{F}_p[t]$ n'a pas de racines multiples. Ainsi le sous-groupe multiplicatif des racines d-ième de l'unité est de cardinal d. Comme tous les éléments de ce sous-groupe multiplicatif sont des racines de $t^e - 1$ pour e l'exposant du groupe, on a forcément $d = e$ sinon $t^e - 1$ aurait trop de racines. Dés lors ce sous-groupe est cyclique d'ordre d. Grâce à la récurence les racines de $\overline{\Phi_{d'}(t)}$ pour tout diviseur $d' \neq d$ de d sont les racines primitives d'-ième de l'unité, c'est à dire les éléments multiplicatifs d'ordre d'. Par suite, en utilisant la formule du point 1., les racines de $\overline{\Phi_d(t)}$ sont forcément les éléments restants du groupe cyclique formé par les racines de $t^d - 1$, c'est à dire les éléments d'ordre d.

Dès lors si $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$, cela implique qu'il existe une racine primitive n-ième de l'unité dans $\mathbb{F}_p$.

5. Soit m suffisamment grand pour que $\Phi_n(m!) \neq 0, 1, -1$. Soit alors p premier tel que $p \mid \Phi_n(m!)$. Alors $p \mid (m!)^n - 1$. Si $p \leq m$, on aurait $p \mid 1$, ce qui est absurde. Ainsi, il suit qu'il existe une infinité de premiers tel que $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$. En effet, on peut prendre un $m' \geq p$ puis appliquer à nouveau l'argument pour m' pour trouver un premier $p' > m' \geq p$ et ainsi de suite pour construire une suite infinie croissante de premiers où $\overline{\Phi_n(t)}$ s'annule. Notons que n est fixé et donc sans perte de généralité $(p, n) = 1$. Ainsi, on utilise le point précédent pour conclure avec Lagrange: $n \mid p - 1$, et donc $p \equiv 1 \mod n$.