Correction feuille 3

1 Extensions de corps, groupes de Galois

Exercice 1. *Montrer que si a et b sont deux éléments non nuls d'un corps K de caractéristique différente de 2, $K(\sqrt{a})$ est égal à $K(\sqrt{b})$ si et seulement si b/a est un carré dans K.*

Preuve : Il est clair que, si $b/a = x^2$ est un carré dans K, on a $\sqrt{b} = \pm x\sqrt{a}$ et $K(\sqrt{a}) = K(\sqrt{b})$. Réciproquement, si ces deux corps sont égaux et différents de K, on peut écrire par exemple $\sqrt{b} = x + y\sqrt{a}$ avec x et y dans K. On en déduit $(b - x^2 - ay^2)^2 = 4x^2y^2a$. Comme a n'est pas un carré dans K, cela implique $2xy = 0$ et $b = x^2 + ay^2$. Comme b n'est pas un carré et la caractéristique n'est pas 2, $2y \neq 0$. On en déduit que $x = 0$ et $b/a = y^2$ est un carré dans K. Reste le cas $K(\sqrt{a}) = K(\sqrt{b}) = K$ pour lequel b et a sont des carrés, et leur quotient aussi.

Exercice 2. *Soit $K = \mathbb{Q}(i + \sqrt{2})$. Montrer que K est galoisien sur $\mathbb{Q}$. Calculer le degré de K sur $\mathbb{Q}$ et le groupe de Galois de $K/\mathbb{Q}$. Donner la liste des sous-corps de K.*

Preuve : Comme $-1/2$ n'est pas un carré dans $\mathbb{Q}$, l'exercice précédent montre que $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont deux extensions quadratiques distinctes de $\mathbb{Q}$. Le composé $L = \mathbb{Q}(i, \sqrt{2})$ est donc une extension galoisienne de degré 4 de $\mathbb{Q}$. On peut décrire l'action du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}) = \{Id, \tau_1, \tau_2, \tau_3\}$ sur i et $\sqrt{2}$:

$$\tau_1(i) = -i,\ \tau_1(\sqrt{2}) = \sqrt{2},\ \tau_2(i) = i,\ \tau_2(\sqrt{2}) = -\sqrt{2},\ \tau_3(i) = -i,\ \tau_3(\sqrt{2}) = -\sqrt{2}.$$

Seul Id laisse fixe l'élément $\alpha = i + \sqrt{2}$ de L. On en déduit que le corps engendré par α est L tout entier, c'est-à-dire $L = K$.

Exercice 3. *Soit $L = \mathbb{Q}(\sqrt{5})$ et $M = \mathbb{Q}(\sqrt{2 + \sqrt{5}})$. Déterminer les degrés des extensions $L/\mathbb{Q}$, $M/\mathbb{Q}$ et M/L. Indiquer lesquelles de ces extensions sont galoisiennes. Déterminer les polynômes minimaux de $\sqrt{2 + \sqrt{5}}$ sur $\mathbb{Q}$ et sur L. Soit a et b deux rationnels tels que $a^2 - 4b$ soit positif mais pas un carré rationnel, et b négatif. Montrer que le polynôme $X^4 + aX^2 + b$ est irréductible sur $\mathbb{Q}$ et que son corps de rupture n'est pas galoisien sur $\mathbb{Q}$.*

Preuve : Comme 5 n'est pas un carré dans $\mathbb{Q}$, $L/\mathbb{Q}$ est une extension quadratique. Montrons que $2 + \sqrt{5}$ n'est pas un carré dans L: en effet, si $(x + y\sqrt{5})^2 = 2 + \sqrt{5}$, son conjugué vérifie $(x - y\sqrt{5})^2 = 2 - \sqrt{5}$ et en faisant le produit, on obtient

$$(x^2 - 5y^2)^2 = 4 - 5 = -1$$

mais -1 n'est pas un carré dans $\mathbb{Q}$, une contradiction. L'extension M/L est donc quadratique, et $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = 4$.. Le générateur $\alpha = \sqrt{2 + \sqrt{5}}$ de M sur $\mathbb{Q}$ vérifie $(\alpha^2 - 2)^2 = 5$, son polynôme minimal sur $\mathbb{Q}$ est donc $(X^2 - 2)^2 - 5 = X^4 - 4X^2 - 1$. Les deux racines imaginaires de ce polynôme ne peuvent appartenir à M qui est inclus dans $\mathbb{R}$. On en déduit que l'extension $M/\mathbb{Q}$ n'est pas galoisienne. D'autre part, une extension quadratique est toujours galoisienne, c'est donc le cas de M/L et $L/\mathbb{Q}$. Le polynôme minimal de α sur L est simplement $X^2 - 2 - \sqrt{5}$.

Comme $a^2 - 4b$ n'est pas un carré, le polynôme $X^4 + aX^2 + b$ n'a pas de racine rationnelle. Pour le factoriser sur $\mathbb{Q}$, il faudrait regrouper les racines imaginaires d'un côté et les deux autres de l'autre, ce qui donnerait une factorisation sur $\mathbb{Q}$ de $Y^2 + aY + b$, qui est impossible puisque $a^2 - 4b$ n'est pas un carré. Le polynôme est irréductible et, ses racines n'engendrant pas le même corps (certaines sont réelles, d'autres non), son corps de rupture n'est donc pas galoisien sur $\mathbb{Q}$.

Exercice 4. *Trouver a et b entiers tels que le polynôme $X^4 + aX^2 + b$ soit irréductible sur $\mathbb{Q}$ et que son corps de rupture soit galoisien sur $\mathbb{Q}$.*

Preuve : Le discriminant $\Delta = a^2 - 4b$ ne doit pas être un carré, sinon le polynôme serait réductible. Le corps quadratique $\mathbb{Q}(\sqrt{\Delta})$ contient alors $(-a + \sqrt{\Delta})/2$ et $(-a - \sqrt{\Delta})/2$, dont les racines carrées sont les racines de $X^4 + aX^2 + b$. Ces racines engendrent des extensions quadratiques de $\mathbb{Q}(\sqrt{\Delta})$ qui coïncident si et seulement si le quotient

$$\frac{-a - \sqrt{\Delta}}{-a + \sqrt{\Delta}} = \frac{a^2 - \Delta}{(-a + \sqrt{\Delta})^2} = b\left(\frac{2}{-a + \sqrt{\Delta}}\right)^2$$

est un carré dans $\mathbb{Q}(\sqrt{\Delta})$, ce qui équivaut à dire que b lui-même est un carré dans $\mathbb{Q}(\sqrt{\Delta})$. L'équation $b = (x+y\sqrt{\Delta})^2$ implique que x ou y est nul, et b est un carré ou Δ fois un carré dans $\mathbb{Q}$. Par exemple, on peut prendre $b = 1$ et $a = -1$: le polynôme $X^4 - X^2 + 1$ est irréductible et son corps de rupture est galoisien sur $\mathbb{Q}$.

Exercice 5. *Soit $K = \mathbb{Q}(\sqrt[3]{2})$, L la clôture galoisienne de K sur $\mathbb{Q}$. Calculer le degré de L sur $\mathbb{Q}$, le groupe de Galois de L/K. Donner la liste des sous-corps de L.*

Preuve : Le corps L est le corps de décomposition de $X^3 - 2$. Comme $X^3 - 2$ est irréductible, K est de degré 3. Les autres racines ne sont pas réelles: le polynôme $X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ est donc irréductible sur K et ses racines engendrent une extension quadratique L de K, et $[L : \mathbb{Q}] = 6$. Le groupe de Galois est un sous-groupe du groupe des permutations des trois racines: c'est $\mathcal{S}_3$ tout entier. Ce groupe a 6 sous-groupes: les deux sous-groupes triviaux, correspondant aux corps $\mathbb{Q}$ et L, les trois sous-groupes d'ordre 2 correspondant aux trois corps cubiques $K = \mathbb{Q}(\sqrt[3]{2})$, $K' = \mathbb{Q}(\rho\sqrt[3]{2})$ et $K'' = \mathbb{Q}(\rho^2\sqrt[3]{2})$, enfin le groupe alterné, d'ordre 3, correspond au corps quadratique $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$.

Exercice 6. *On rappelle que, si L/K est une extension cubique de corps de caractéristique différente de 3, L est engendré par une racine α d'un polynôme de $K[X]$ de la forme $X^3 + pX + q$. Montrer que si la caractéristique est aussi différente de 2, l'extension L/K est galoisienne si et seulement si le discriminant $\Delta = -(4p^3 + 27q^2)$ est un carré dans K.*

Preuve : Notons $L = K(\alpha)$ et $M = K(\alpha, \beta, \gamma)$, où α, β et γ sont les racines de $X^3 + pK + q$. Le corps de rupture $L = K(\alpha)$ est séparable sur K puisque la caractéristique ne divise pas le degré. Sa clôture galoisienne est M. Posons

$$\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma).$$

On a $\delta^2 = \Delta = -(4p^3 + 27q^2) \in K$. Si $M = L$, δ appartient à L et son degré sur K est inférieur ou égal à 2: il appartient en fait à K et Δ est un carré dans K. Au contraire, si $M \neq L$, il existe un automorphisme non trivial σ de M sur K. Cet automorphisme doit laisser fixe α et échanger β et γ, on a donc

$$\sigma(\delta) = (\sigma(\alpha) - \sigma(\beta))(\sigma(\alpha) - \sigma(\gamma))(\sigma(\beta) - \sigma(\gamma)) = (\alpha - \gamma)(\alpha - \beta)(\gamma - \beta) = -\delta.$$

Comme la caractéristique est différente de 2, on a $\sigma(\delta) = -\delta \neq \delta$, et δ n'est pas dans K, c'est-à-dire que Δ n'est pas un carré dans K.

Exercice 7. *Soit G le groupe de Galois de $X^5 - 2$. Quel est le cardinal de G? Est-il abélien, résoluble?*

Preuve : On note $\zeta = e^{\frac{2i\pi}{5}}$ et $\alpha = \sqrt[5]{2}$ dont les polynômes minimaux sont respectivement $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ et $X^5 - 2$. Le corps de décomposition de $X^5 - 2$ est $L = \mathbb{Q}[\zeta, \alpha]$ qui contient entr'autre les corps $\mathbb{Q}[\zeta]$ et $\mathbb{Q}[\alpha]$ qui sont respectivement de degré 4 et 5 sur $\mathbb{Q}$. On en déduit alors que $[L : \mathbb{Q}]$ est divisible par 5 et 4 et donc par 20. Par ailleurs ζ est au plus de degré 4 sur $\mathbb{Q}[\alpha]$ de sorte que $[L : \mathbb{Q}] \leq 20$. Ainsi d'après le théorème de Galois, G est de cardinal 20.

Pour tout $\sigma \in G$, on a $\sigma(\alpha) \in \{\alpha, \zeta\alpha, \zeta^2\alpha, \zeta^3\alpha, \zeta^4\alpha\}$ et $\sigma(\zeta) \in \{\zeta, \zeta^2, \zeta^3, \zeta^4\}$. Comme G est de cardinal 20, alors pour tout $0 \leq k \leq 4$ et $1 \leq l \leq 4$, il existe $\sigma \in G$ tel que $\sigma(\alpha) = \alpha\zeta^k$, $\sigma(\zeta) = \zeta^l$.

Soit alors σ (resp. τ) tel que $\sigma(\alpha) = \alpha\zeta$ (resp. $\tau(\alpha) = \alpha$) et $\sigma(\zeta) = \zeta$ (resp. $\tau(\zeta) = \zeta^2$) de sorte que σ est d'ordre 5 (resp. d'ordre 4) et que tout élément de G s'écrit de manière unique sous la forme $\sigma^k\tau^l$ avec $0 \leq k \leq 4$ et $0 \leq l \leq 3$.

Clairement G n'est pas abélien car $\mathbb{Q}[\alpha]/\mathbb{Q}$ n'est pas galoisien. Par contre il est résoluble car tout groupe de cardinal 20 l'est (le plus petit groupe non résoluble est $\mathcal{A}_5$).
Remarque: En fait $G \simeq \mathbb{Z}/5\mathbb{Z} \ltimes_\psi \mathbb{Z}/4\mathbb{Z}$ où $\psi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times$ avec $\psi(1)$ est la multiplication par 2. On peut déterminer tous les sous-groupes de G et donc toutes les sous-extensions de L, on obtient alors

sous-groupe	corps intermédiaires	degré sur $\mathbb{Q}$
$\{1\}$	$\mathbb{Q}[\zeta, \alpha]$	20
$\{1, \tau^2\}$	$\mathbb{Q}[\alpha, \zeta^2 + \zeta^3]$	10
$\{1, \sigma\tau^2\sigma^{-1}\}$	$\mathbb{Q}[\zeta\alpha, \zeta^2 + \zeta^3]$	10
$\{1, \sigma^2\tau^2\sigma^{-2}\}$	$\mathbb{Q}[\zeta^2\alpha, \zeta^2 + \zeta^3]$	10
$\{1, \sigma^3\tau^2\sigma^{-3}\}$	$\mathbb{Q}[\zeta^3\alpha, \zeta^2 + \zeta^3]$	10
$\{1, \sigma^4\tau^2\sigma^{-4}\}$	$\mathbb{Q}[\zeta^4\alpha, \zeta^2 + \zeta^3]$	10
$< \tau >$	$\mathbb{Q}[\alpha]$	5
$< \sigma\tau\sigma^{-1} >$	$\mathbb{Q}[\zeta\alpha]$	5
$< \sigma^2\tau\sigma^{-2} >$	$\mathbb{Q}[\zeta^2\alpha]$	5
$< \sigma^3\tau\sigma^{-3} >$	$\mathbb{Q}[\zeta^3\alpha]$	5
$< \sigma^4\tau\sigma^{-4} >$	$\mathbb{Q}[\zeta^4\alpha]$	5
$< \sigma >$	$\mathbb{Q}[\zeta]$	4
$< \sigma, \tau^2 >$	$\mathbb{Q}[\zeta^2 + \zeta^3]$	2
G	$\mathbb{Q}$	1

Exercice 8. *Quel est le degré du corps de rupture du polynôme* $(X^3 - 5)(X^3 - 7)$ *sur* $\mathbb{Q}$*?*

Preuve : Si E_1 et E_2 sont deux extensions galoisiennes de F alors E_1E_2 et $E_1 \cap E_2$ sont galoisiennes sur F et on a la suite exacte suivante

$$1 \to \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) \to \mathrm{Gal}(E_1 \cap E_2/F) \to 1$$

Ici on a $E_1 \cap E_2 = \mathbb{Q}[\zeta]$ où ζ est une racine cubique primitive de l'unité de sorte que le degré cherché est 18.

Exercice 9. *Déterminez le groupe de Galois de* $X^6 - 5$ *sur* $\mathbb{Q}$, $\mathbb{R}$.

Preuve : Soit L le corps de décomposition de $X^6 - 5$: $L = \mathbb{Q}[\zeta, \alpha]$ avec $\alpha^6 = 5$, $\alpha \in \mathbb{R}$ et ζ est une racine primitive 3-ième de l'unité de sorte que $-\zeta$ est une racine primitive 6-ième de l'unité. Le degré $[L : \mathbb{Q}]$ est donc égal à 12 et $G \simeq D_6$ engendré par (26)(35) et (123456). Sur $\mathbb{R}$ le groupe de galois est $\mathbb{Z}/2\mathbb{Z}$.

Exercice 10. *Trouvez un élément primitif de* $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$.

Preuve : Soit par exemple $x = \sqrt{3} + \sqrt{7}$. On peut par ailleurs trouver son polynôme minimal en procédant comme suit.

Soit A et B deux polynômes irréductibles unitaires sur $\mathbb{Q}$. Le système en d'équations $A(X) = B(Y - X) = 0$ possède comme solutions les couples $(x_a, x_b + x_a)$ où x_a (resp. x_b) décrit les solutions de $A(X) = 0$ (resp. $B(X) = 0$). On considère alors les polynômes $A(X)$ et $B(Y - X)$ comme des polynômes à valeurs dans $K[Y]$ et on introduit leur résultant qui est un polynôme en Y dont les zéros sont d'après ce qui précède, exactement les sommes des zéros de A avec ceux de B.

Dans notre cas on a $A(X) = X^2 - 3$ et $B(X) = X^2 - 7$. Le résultant en question est donné par le déterminant

$$\begin{vmatrix} 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & -3 \\ 1 & -2Y & Y^2 - 7 & 0 \\ 0 & 1 & -2Y & Y^2 - 7 \end{vmatrix}$$

soit après calcul $Y^4 - 20y^2 + 16$

Exercice 11. *Soit* G *le groupe de Galois de* $(X^3 - 5)(X^4 - 2)$ *sur* $\mathbb{Q}$.

1) Donner un ensemble de générateurs de G *ainsi que l'ensemble de relations entre eux.*

2) G *est-il un groupe cyclique, diédral, symétrique?*

Preuve : Le corps de décomposition de X^4-2 est $E_1=\mathbb{Q}[i,\alpha]$ avec $\alpha^4=2$ qui est de degré 8 sur $\mathbb{Q}$ et de groupe de Galois D_4. Le corps de décomposition de X^3-5 est $E_2=\mathbb{Q}[\zeta,\beta]$ qui est de degré 6 et de groupe de Galois D_3 sur $\mathbb{Q}$. Le groupe de Galois est le groupe produit $D_4\times D_3$: en effet $E_1\cap E_2=\mathbb{Q}$ car la seule autre alternative serait $\mathbb{Q}[\sqrt{3}]$ mais $\sqrt{3}$ n'est pas un carré dans E_1.

Exercice 12. *Trouvez un élément primitif du corps de rupture de* $(X^2-2)(X^2-5)(X^2-7)$.

Preuve : Par exemple $x=\sqrt{2}+\sqrt{5}+\sqrt{7}$.

Exercice 13. *Soit* ζ *un racine primitive* 12*-ième de l'unité. Combien y a-t-il d'extension comprises entre* $\mathbb{Q}[\zeta^3]$ *et* $\mathbb{Q}[\zeta]$.

Preuve : On a $\mathbb{Q}[\zeta]=\mathbb{Q}[\zeta',i]$ où ζ' est une racine primitive 3-ième de l'unité et $\pm i=\zeta^3$ ...

Exercice 14. *Soit* ζ *une racine primitive* 5*-ième de l'unité.*

(1) Décrivez le groupe de Galois de $K=\mathbb{Q}[\zeta]/\mathbb{Q}$ *et montrez que* K *contient un unique sous-corps de degré* 2 *sur* $\mathbb{Q}$ *à savoir* $\mathbb{Q}[\zeta+\zeta^4]$.

(2) Donnez le polynôme minimal de $\zeta+\zeta^4$ *sur* $\mathbb{Q}$.

(3) Donnez le groupe de Galois de $(X^2-5)(X^5-1)$.

(4) Donnez le groupe de Galois de $(X^2+3)(X^5-1)$.

Preuve : (1) Le groupe de galois est $(\mathbb{Z}/5\mathbb{Z})^\times$, cyclique de cardinal 4 engendré par $\sigma_0:=2$; il possède donc un unique sous-groupe H d'indice 2 à savoir le groupe engendré par 2^2. Le sous-corps correspondant est donc engendré par $\sum_{\sigma\in H}\sigma(\zeta)=\zeta+\zeta^4$.

(2) On a $\sigma_0(\zeta+\zeta^4)=\zeta^2+\zeta^3$ et

$$(\zeta+\zeta^4)(\zeta^2+\zeta^3)=-1 \qquad (\zeta+\zeta^4)+(\zeta^2+\zeta^3)=-1$$

de sorte que le polynôme minimal de $(\zeta+\zeta^4$ est X^2+X-1.

(3)

(4) on a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

Exercice 15. *Notons* K *le corps* $\mathbb{Q}(\sqrt{-15})$, f *son automorphisme non trivial, et* α *un élément de* K *tel que le polynôme* $X^3-\alpha$ *soit irréductible sur* K. *Pourquoi existe-t-il de tels* α*? On note* L *le corps de décomposition de ce polynôme, et* $\{\theta,\rho\theta,\rho^2\theta\}$ *ses différentes racines dans* L.

1) Pourquoi sont-elles de cette forme?

2) Montrer que L *est une extension galoisienne de* K *de degré 6, et que* L *contient* $\sqrt{5}$.

3) Montrer qu'il existe deux $K-$*automorphismes* σ *et* τ *de* L *tels que*

$$\sigma(\sqrt{5})=\sqrt{5},\quad \sigma(\theta)=\rho\theta,\quad \tau(\sqrt{5})=-\sqrt{5},\quad \tau(\theta)=\theta.$$

4) Déterminer l'ordre des éléments σ *et* τ *du groupe* $Gal(L/K)$ *et calculer* $\tau\sigma\tau^{-1}$. *Etablir la liste des extensions de* K *contenues dans* L.

5) On suppose désormais que $N_{K/\mathbb{Q}}(\alpha)$ *est le cube d'un nombre rationnel* b *(on admettra que c'est possible). Déterminer les différents conjugués de* θ *sur* $\mathbb{Q}$. *Montrer que l'extension* $L/\mathbb{Q}$ *est galoisienne de degré 12. Prouver qu'il est possible de prolonger l'automorphisme* f *de* K *en un automorphisme* ϕ *de* L *tel que* $\phi(\sqrt{5})=\sqrt{5}$ *et* $\phi(\theta)=b/\theta$. *Calculer* ϕ^2, $\phi\sigma\phi^{-1}$ *et* $\phi\tau\phi^{-1}$. *Montrer que* $\mathbb{Q}(\sqrt{5})$ *admet une extension de degré 3 contenue dans* L *et galoisienne sur* $\mathbb{Q}$.

Preuve : Un polynôme de degré 3 est irréductible si et seulement si il n'a pas de racine. Il s'agit donc de montrer que tous les éléments de $\mathbb{Q}(\sqrt{-15})$ ne sont pas des cubes. Mais si $\alpha = x + y\sqrt{-15} = \theta^3$ avec $\theta \in \mathbb{Q}(\sqrt{-15}$, alors $f(\alpha) = f(\theta)^3$ et la quantité

$$x^2 + 15y^2 = N(\alpha) = \alpha f(\alpha) = N(\theta)^3$$

est le cube d'un rationnel. Il suffit de prendre par exemple $y = 0$ et x non cube pour trouver un α qui convient. Si θ' est une autre racine, on a $(\theta'/\theta)^3 = 1$. Alors θ et θ' différent par une racine cubique de l'unité, ρ ou ρ^2.

Comme L est défini comme corps de décomposition en caractéristique nulle, L/K est forcément galoisienne, et son degré est un multiple de $3 = [K(\theta)/K]$. Mais L contient aussi $\frac{\rho\theta}{\theta} = \rho = \frac{-1+\sqrt{-3}}{2}$ qui est quadratique sur $\mathbb{Q}$. D'après un exercice précédent, $K = \mathbb{Q}(\sqrt{-15})$ et $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$ sont deux extensions quadratiques distinctes de $\mathbb{Q}$. Donc ρ est quadratique sur K, donc pas dans $K(\theta)$, donc quadratique sur $K(\theta)$, et $L = K(\theta)(\rho)$ est de degré 6 sur K. Au passage, on a vu que L contenait $\frac{\sqrt{-15}}{\sqrt{-3}} = \sqrt{5}$.

Le groupe de Galois du corps de décomposition est un sous-groupe du groupe des permutations des racines du polynôme. Ici le groupe est d'ordre 6, et il y a trois racines: $\mathrm{Gal}(L/K)$ s'identifie au groupe des permutations de $\{\theta, \rho\theta, \rho^2\theta\}$. Il existe en particulier σ qui envoie θ sur $\rho\theta$ et $\rho\theta$ sur $\rho^2\theta$. On en déduit $\sigma(\rho) = \sigma(\frac{\rho\theta}{\theta}) = \frac{\rho^2\theta}{\rho\theta} = \rho$, donc aussi $\sigma(\sqrt{-3}) = \sigma(1 + 2\rho) = 1 + 2\sigma(\rho) = \sqrt{-3}$. Comme on a par définition $\sigma(\sqrt{-15}) = \sqrt{-15}$, on en déduit $\sigma(\sqrt{5}) = \frac{\sigma(\sqrt{-15})}{\sigma(\sqrt{-3})} = \sqrt{5}$. De même, la permutation τ qui échange $\rho\theta$ et $\rho^2\theta$ en laissant fixe θ vérifie $\tau(\rho) = \frac{\tau(\rho\theta)}{\tau(\theta)} = \rho^{-1} = \rho^2$, donc $\tau(\sqrt{-3}) = -\sqrt{-3}$ et $\tau(\sqrt{5}) = \frac{\tau(\sqrt{-15})}{\tau(\sqrt{-3})} = -\sqrt{5}$.

La permutation σ est circulaire, elle est d'ordre 3. De même, τ est une transposition, d'ordre 2. On voit que $\tau\sigma\tau^{-1}$ permute les trois racines circulairement, dans l'autre sens: $\tau\sigma\tau^{-1} = \sigma^{-1} = \sigma^2$. On peut écrire

$$\mathrm{Gal}(L/K) = \{Id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Ce groupe a 4 sous-groupes non triviaux, $\{Id, \sigma, \sigma^2\}$ est d'ordre 3 et a pour corps fixe $K(\sqrt{5})$, et les trois groupes d'ordre 2 $\{Id, \tau\}$, $\{Id, \sigma\tau\}$ et $\{Id, \sigma^2\tau\}$ ont pour corps fixes respectifs $K(\theta)$, $K(\rho^2\theta)$ et $K(\rho\theta)$, ce qui complète, avec K et L, la liste des corps intermédiaires entre K et L.

On a $t = \alpha + f(\alpha) \in \mathbb{Q}$ et $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = b^3 \in \mathbb{Q}$. On en déduit que θ est racine du polynôme à coefficients rationnels

$$P(X) = (X^3 - \alpha)(X^3 - f(\alpha)) = X^6 - tX^3 + b^3.$$

Sur K, ce polynôme se décompose en deux facteurs dont on sait qu'ils sont irréductibles (b^3/α n'est pas plus un cube que α dans K). Toute factorisation de P sur $\mathbb{Q}$ serait encore valable sur K, or les facteurs ont des coefficients qui ne sont pas dans $\mathbb{Q}$ (en effet, si α appartenait à $\mathbb{Q}$, on aurait $\alpha^2 = b^6$, donc $\alpha = \pm b^3 = (\pm b)^3$, ce qui contredit le fait que $X^3 - \alpha$ est irréductible sur K); on en déduit que P est irréductible sur $\mathbb{Q}$.

Les racines du polynôme P sont

$$\{\theta, \rho\theta, \rho^2\theta, b/\theta, \rho b/\theta, \rho^2 b/\theta\}$$

et appartiennent toutes à L. D'autre part, le corps de décomposition de P sur $\mathbb{Q}$ contient θ, donc α, donc K, donc $L = K(\theta, \rho\theta)$. On vient de prouver que c'est L, qui est donc une extension galoisienne de degré 12 de $\mathbb{Q}$. $\mathrm{Gal}(L/K)$ est un sous-groupe (distingué) d'indice 2 de $\mathrm{Gal}(L/\mathbb{Q})$. Soit ψ un élément quelconque de $\mathrm{Gal}(L/\mathbb{Q})$ qui n'est pas dans $\mathrm{Gal}(L/K)$. Par construction, la restriction de ψ à K n'est pas l'identité, c'est donc f. On en déduit que ψ échange les deux facteurs de P sur K, et donc l'image $\gamma = \psi(b/\theta)$ de b/θ par ψ est θ, $\rho\theta$ ou $\rho^2\theta$. Choisissons un élément κ de $\mathrm{Gal}(L/K)$ tel que $\kappa(\theta) = \gamma$. Si l'image de $\sqrt{5}$ par $\psi^{-1}\kappa$ est $\sqrt{5}$, $\phi = \psi^{-1}\kappa$ présente les propriétés requises. Sinon, $\phi = \tau\psi^{-1}\kappa$ convient.

On a $\phi^2(\theta) = \phi(b/\theta) = b/\phi(\theta) = \theta$. Donc ϕ^2 est un élément de $\mathrm{Gal}(L/K)$ qui laisse fixe $\sqrt{5}$ et θ: c'est l'identité. On a encore $\phi(\sqrt{-15}) = f(\sqrt{-15}) = -\sqrt{-15}$, donc $\phi(\sqrt{-3}) = \frac{\phi(\sqrt{-15})}{\phi(\sqrt{5})} = -\sqrt{-3}$, d'où $\phi(\rho) = \rho^2$. On en déduit que

$$\phi\sigma\phi^{-1}(\theta) = \phi\sigma(\frac{b}{\theta}) = \phi(\frac{b}{\rho\theta}) = \frac{\theta}{\rho^2} = \rho\theta,$$

donc $\phi\sigma\phi^{-1}$ est un élément de $\mathrm{Gal}(L/K)$ qui envoie $\sqrt{5}$ sur $\sqrt{5}$ et θ sur $\rho\theta$, donc $\phi\sigma\phi^{-1} = \sigma$. De même, on montre que $\phi\tau\phi^{-1} = \tau$, et ϕ commute à tous les éléments de $\mathrm{Gal}(L/K)$, et à lui-même, donc ϕ est dans le centre de $\mathrm{Gal}(L/\mathbb{Q})$: le sous-groupe $\{Id, \phi\}$ est distingué, et le corps fixe de ϕ est un sous-corps M de L galoisien sur $\mathbb{Q}$. Comme $[L : M] = 2$, M est de degré 6 sur $\mathbb{Q}$. Comme $\phi(\sqrt{5}) = \sqrt{5}$, $R = \mathbb{Q}(\sqrt{5})$ est inclus dans M qui est donc une extension de degré 3 de R.

Exercice 16. *Montrer que si K est un corps de caractéristique p non nulle, le corps $M = K(X, Y)$ des fractions rationnelles en deux indéterminées à coefficients dans K est une extension de degré p^2 de son sous-corps $L = K(X^p, Y^p)$. Montrer que si α est un élément de M qui n'est pas dans L, son polynôme minimal sur L est de degré p. En déduire que le mot "séparable" dans l'énoncé du théorème de l'élément primitif n'est pas inutile.*

Preuve : Montrons d'abord que si a est un élément d'un corps L de caractéristique p non nulle qui n'a pas de racine p-ième dans L, le polynôme $U = T^p - a$ est irréductible sur L. En effet, si b est une racine de U dans une extension N de L, le polynôme U se factorise comme $(T - b)^p$ dans $N[T]$. Si donc $U = PQ$ est un factorisation non triviale de U en polynômes unitaires de $L[X]$, on a $P = (T - b)^k$, avec $0 < k < p$. Le coefficient constant $\pm b^k$ de P appartient à L. Comme b^p appartient aussi à L, il en est de même de $b = (b^k)^u.(b^p)^v$, une contradiction.

En reprenant les notations de l'exercice et en posant $N = K(X, Y^p)$, on déduit de ce qui précède que N/L et M/N sont de degré p. Si $\alpha = R(X, Y)$ est un élément quelconque de M, sa puissance p-ième s'écrit $S(X^p, Y^p)$, où S est la fraction rationnelle obtenue en élevant à la puissance p-ième chacun des coefficients de R. Donc α^p est dans L, et le degré de α sur L est au plus p. On en déduit que M/L n'est pas monogène, d'où le résultat.

Exercice 17. *On note L le corps de décomposition dans $\mathbb{C}$ du polynôme $P = T^4 - 3T - 3$.*

a) Montrer que le polynôme P est irréductible sur $\mathbb{Q}$, et qu'il admet dans $\mathbb{C}$ deux racines réelles x et y, et un couple $(z, \overline{z})$ de racines complexes conjuguées l'une de l'autre.

b) Notons $T^2 + aT + b$ et $T^2 - aT + b'$ les polynômes unitaires de degré 2 qui divisent P dans $\mathbb{R}[X]$. Montrer que a est une racine du polynôme $X^6 + 12X^2 - 9$, et calculer le degré de a^2 sur $\mathbb{Q}$.

c) Montrer que $[L : \mathbb{Q}]$ est un multiple de 12.

d) Montrer que le groupe alterné $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 du groupe symétrique $\mathcal{S}_4$.

e) Montrer qu'il existe un automorphisme de L qui échange z et $\overline{z}$ et qui laisse x fixe. Déterminer le groupe de Galois de $L/\mathbb{Q}$. Combien L a-t'il de sous-corps ?

Preuve :

(a) Le critère d'Eisenstein s'applique à P pour le nombre premier $p = 3$, donc P est irréductible sur $\mathbb{Q}$. La dérivée $P'(t) = 4t^3 - 3$ s'annule exactement une fois sur $\mathbb{R}$, au point $\vartheta = \sqrt[3]{\frac{3}{4}}$. Comme $P(\vartheta) = -9\vartheta/4 - 3 < 0$, et $\lim_{t \to \pm\infty} P(t) = +\infty$, la fonction $P(t)$ s'annule exactement deux fois sur $\mathbb{R}$. Les deux autres racines de P dans $\mathbb{C}$ sont conjuguées (au sens habituel...) l'une de l'autre.

(b) La décomposition de P en éléments irréductibles de $\mathbb{R}[T]$, s'écrit

$$(T - x)(T - y)(T^2 + aT + b).$$

Le coefficient de T^2 est nul, donc $(T - x)(T - y) = T^2 - aT + b'$. L'identification donne

$$a^2 = b + b' \qquad a(b - b') = 3 \qquad bb' = -3$$

on tire $a^6 = a^2(b^2 + 2bb' + b'^2)$ de la première équation et $9 = a^2(b^2 - 2bb' + b'^2)$ de la seconde. On a donc $a^6 - 9 = a^2(4bb') = -12a^2$, d'où le résultat. Comme a^2 est racine d'un polynôme de degré 3, il est de degré au plus 3. Pour montrer que a^2 est de degré 3, on peut montrer que le polynôme $X^3 + 12X^2 - 9$ est irréductible sur $\mathbb{Q}$, ce qui résulte du fait qu'aucun des entiers ± 1, ± 3 ou ± 9 qui divisent son coefficient constant n'en est une racine.

(c) Le degré de L est un multiple de celui de chacun de ses éléments. Or x est de degré 4 et a^2 est de degré 3, d'où le résultat.

(d) Les classes de conjugaison de $\mathcal{S}_n$ sont en bijection avec les partitions de l'entier n. Pour $n = 4$, la permutation identique forme la seule classe de conjugaison de cardinal 1, les permutations (12), (123), (1234) et (12)(34) sont des représentants des autres classes, de cardinal respectif 6, 8, 6 et 3. Un sous-groupe d'indice 2 est forcément distingué, et formé de certaines de ces classes. La seule somme qui donne 12 est $1 + 8 + 3$, qui donne le groupe alterné $\mathcal{A}_4$.

(e) Comme L est une extension normale de $\mathbb{Q}$, il est laissé stable par tout automorphisme de $\mathbb{C}$, en particulier la conjugaison complexe, qui laisse x et y et échange z et $\overline{z}$. Cette permutation est une transposition, c'est-à-dire

que considéré comme sous-groupe du groupe des permutations des racines de P, le groupe de Galois de $L/\mathbb{Q}$ n'est pas inclus dans $\mathcal{A}_4$; Or, on a vu au c), que son cardinal $[L:\mathbb{Q}]$ vaut 12 ou 24. la question précédente permet donc de conclure $\mathrm{Gal}(L/\mathbb{Q}) = \mathcal{S}_4$. Reste à compter le nombre de sous-groupes de $\mathcal{S}_4$. Il y en a 1 d'ordre 24, un d'ordre 12, 3 d'ordre 8 (les 2-Sylow sont conjugués entre eux). Il y a 4 sous-groupes d'ordre 6, conjugués à $\mathcal{S}_3$. Les groupes d'ordre ' sont de 3 sortes: les cycliques, au nombre de 3, les conjugués de $\{Id, (12), (34), (12)(34)\}$, au nombre de 3, et le groupe de Klein $\{Id, (12)(34), (13)(24), (14)(23)$. Enfin, il y a 4 groupes d'ordre 3, 9 groupes d'ordre 2 et 1 groupe d'ordre 1, soit un total de $1 + 1 + 3 + 4 + (3 + 3 + 1) + 4 + 9 + 1 = 30$ sous-corps.

Exercice 18. *Montrez en réduisant modulo 2 et 3, que le groupe de Galois G de $X^5 - X - 1$ est $\mathcal{S}_5$.*

Preuve : $X^5 - X - 1$ n'a pas de racines dans $\mathbb{F}_2$ mais il en a dans $\mathbb{F}_4$ comme on peut par exemple le voir calculant le pgcd de $X^5 - X - 1$ avec $X^4 - X$. Ainsi $X^5 - X - 1$ se factorise en un produit de deux facteurs irréductibles de degré 2 et 3. On en déduit alors que G contient une permutation de type $(12)(345)$ et donc en passant au cube, une transposition.

Modulo 3, $X^5 - X - 1$ reste irréductible, de sorte que G contient un 5-cycle. On conclut en remarquant que $\mathcal{S}_n$ est engendré par (12) et $(12\cdots n)$.

Exercice 19. *(1) Soit $E \subset F$ une extension quadratique et soit $x \in F\backslash E$ tel que $x^2 \in E$. Si $a \in F$ est un carré montrez que ou bien a est un carré dans E ou bien ax^2 est un carré dans E.*

(2) Soient $p_1, \cdots, p_n$ des nombres premiers distincts. On considère les propriétés suivantes:

(a_n) le corps $\mathbb{Q}[\sqrt{p}_1, \cdots, \sqrt{p}_n]$ est de degré 2^n sur $\mathbb{Q}$;

(b_n) $x \in \mathbb{Q}$ est un carré dans $\mathbb{Q}[\sqrt{p}_1, \cdots, \sqrt{p}_n]$ si et seulement s'il existe une partie $I \subset \{1, \cdots, n\}$ telle que $x \prod_{i\in I} p_i$ est un carré dans $\mathbb{Q}$.

(i) Montrez que $(a_n) \wedge (b_n) \Rightarrow (a_{n+1})$.

(ii) Montrer que $(a_n) \wedge (b_{n-1}) \Rightarrow (b_n)$.

(iii) En déduire que (a_n) et (b_n) sont vraies pour tout n.

(iv) Montrez que la famille $\sqrt{2}, \sqrt{3}, \cdots$ des racines carrées des nombres premiers, est libre sur $\mathbb{Q}$.

Preuve : (1) On a $F = E[x]$; supposons donc $a = \alpha^2$ avec $\alpha x \notin E$. On a alors $F = E[\alpha x]$ et il existe $e_1, e_2 \in E$ tels que $x = e_1(\alpha x) + e_2$ et donc $(x - e_2)^2 \in E$ soit $e_2 = 0$ ce qui implique $\alpha \in E$.

(2) (i) c'est trivial

(ii) Cela découle directement de (1)

(iii) (iv) immédiat.

Exercice 20. *Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{C}[X]$; on veut prouver que P est totalement décomposé dans $\mathbb{C}[X]$.*

(1) Montrer que $Q(X) = (X^2 + 1)P(X)\bar{P}(X) \in \mathbb{R}[X]$.

(2) On note D le corps de décomposition sur $\mathbb{R}$ de Q et on note G le groupe de Galois de $D/\mathbb{R}$ de cardinal $2^n m$ avec m impair.

(i) Montrer que $n \geq 1$.

(ii) En notant que tout polynôme réel de degré impair admet au moins une racine réelle, montrer, en utilisant le théorème de Sylow, que $m = 1$.

(iii) En notant que tout nombre complexe est le carré d'un nombre complexe, montrer, en utilisant le théorème de Sylow, que $n = 1$.

(iv) Montrer que $D = \mathbb{C}$ et conclure.

Preuve : (1) C'est clair.

(2) (i) D contient $\mathbb{C}$ et donc 2 divise $[D:\mathbb{R}]$.

(ii) Un polynôme de degré impair possède toujours une racine réelle d'après le théorème des valeurs intermédiaires en remarquant qu'en $\pm\infty$ les limites sont infinies de signes opposés. Soit d'après le théorème de

Sylow, le 2-Sylow G_2: l'extension $L = D^{G_2}/\mathbb{R}$ est donc de degré m sur $\mathbb{R}$, le polynôme minimal d'un élément primitif est de degré m et irréductible sur $\mathbb{R}$ d'où $m = 1$.

(iii) Soit H le groupe de Galois de $D/\mathbb{C}$; c'est un 2-groupe que nous supposons non trivial. Or dans un 2-groupe non trivial il existe $Q \subset H$ tel que $H/Q \simeq \mathbb{Z}/2\mathbb{Z}$ de sorte que D^Q est une extension de degré 2 de $\mathbb{C}$ et donc de la forme $\mathbb{C}[\alpha]$ avec $\alpha^2 \in \mathbb{C}$. Or tout nombre complexe a une racine carrée complexe et donc $\alpha \in \mathbb{C}$, contradiction.

(iv) On en déduit donc que $D = \mathbb{C}$ i.e. $\mathbb{C}$ est algébriquement clos.

2 Nombres transcendants

Exercice 1. e **est irrationnel**: *on considère la suite* (u_n) *définie par récurrence:* $u_0 = 1$ *et* $u_{n+1} = u_n + \frac{1}{(n+1)!}$.

(a) Montrez que (u_n) *converge; on notera e sa limite.*

(b) On suppose qu'il existe $a, b \in \mathbb{N}$ *tels que* $e = a/b$ *(*$b \neq 0$ *avec* a *et* b *premiers entre eux). En étudiant* $\alpha = (k!)(e - u_k)$ *pour* $k > b$*, montrez que l'on aboutit à une contradiction.*

Preuve : (a) évident (b) $\alpha = (k+1)^{-1} + (k+1)^{-1}(k+2)^{-1} + \cdots \leq \sum_{i=1}^{+\infty}(k+1)^{-i} = 1/k \notin \mathbb{N}$.

Exercice 2. π^2 **est irrationnel**: *Soit* $f_n(x) = \frac{x^n(1-x)^n}{n!}$.

(a) Montrez que pour tout $m \geq 0$, $f_n^{(m)}(0) \in \mathbb{Z}$.

(b) On suppose qu'il existe $a, b \in \mathbb{N}$ *premiers entre eux et* $b \neq 0$ *tels que* $\pi^2 = a/b \in \mathbb{Q}$ *et on pose*

$$G_n(x) = b^n[\pi^{2n} f_n(x) - \pi^{2n-2} f_n''(x) + \cdots + (-1)^n f_n^{(2n)}(x)].$$

Montrez que $G_n(0)$ *et* $G_n(1)$ *sont des entiers.*

(c) Montrez que

$$\pi \int_0^1 a^n \sin(\pi x) f_n(x) dx = G_n(0) + G_n(1)$$

et conclure.

Preuve : (a) $f_n^{(m)}(0) = 0$ pour $m < n$ et $m > 2n$. En écrivant $x^n(1-x)^n = \sum_k c_k x^k$, on a $f^{(m)}(0) = \frac{m!}{n!} c_m$ pour $m \geq n$.

(b) En remarquant que $f_n(1-x) = f_n(x)$ on a le même résultat en 1 d'où le résultat.

(c) C'est une simple intégration par parties et la conclusion découle de la majoration de l'intégrale par $\pi a^n/n!$ dont la limite est nulle pour n tendant vers l'infini ($0 < f(x) \leq 1/n!$). Un entier plus petit que $1/2$ est nul ce qui ne se peut pas car l'intégrale n'est pas nulle pour n fixé.

Exercice 3. e **est transcendant**: *(a) Soit* $P \in \mathbb{R}[X]$ *de degré* m*; montrez que*

$$I_P(t) = \int_0^t e^{t-u} P(u) du = e^t \sum_{i=0}^{m} P^{(i)}(0) - \sum_{i=0}^{m} P^{(i)}(t).$$

(b) Soient $a_0, \cdots, a_n \in \mathbb{Z}$ *tels que* $a_0 + a_1 e + \cdots + a_n e^n = 0$ *avec* $a_0 \neq 0$ *et* $a_n \neq 0$*. On pose pour tout* $0 < p \in \mathbb{N}$*:* $f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p$ *ainsi que* $J_p = a_0 I_f(0) + \cdots + a_n I_f(n)$*. Montrez que* $J_p \in \mathbb{Z}$ *puis que si* p *est un nombre premier assez grand,* J_p *est divisible par* $(p-1)!$ *mais pas par* $p!$.

(c) Montrez qu'il existe une constante c *indépendante de* p*, telle que* $|J_p| \leq c^p$ *et conclure.*

Preuve : (a) On traite le cas d'un monôme (évidemment) puis on conclura par linéarité:

$$\begin{aligned} \int_0^t e^{t-u} u^n du &= e^t[-e^{-u}u^n]_0^t + e^t \int_0^t e^{-u} n u^{n-1} du \\ &= -t^n + n \int_0^t e^{t-u} u^{n-1} du \end{aligned}$$

On peut par exemple raisonner par récurrence sur n, on obtient alors $\int_0^t e^{t-u} u^n du = e^t \sum_{k=0}^n [\frac{d^k}{dt^k} t^n]_0 - \sum_{k=0}^n \frac{d^k}{dt^k} t^n$ et on conclut par linéarité. (remplacer m par $+\infty$).

(b) On pose $m = np + p - 1$ de sorte que $J_p = \sum_{j=0}^m f^{(j)}(0)(a_0 + a_1 e + \cdots + a_n e^n) - \sum_{j=0}^m \sum_{k=0}^n f^{(j)}(k)$. Le résultat se déduit des faits suivants: le premier terme dans l'écriture de J_p ci-dessus est nul et les $f^{(j)}(k) \in \mathbb{Z}$.

En outre si $k > 0$, $f^{(j)}(k) = 0$ pour $j < p$ et $f^{(j)}(k)$ est un multiple de $p!$ pour $j \geq p$. Pour $k = 0$, $f^{(j)}(0) = 0$ pour $j < p-1$ et $f^{(j)}(0)$ est divisible par $p!$ pour $j \geq p$ alors que $f^{(p-1)}(0) = (p-1)!(n!)^p(-1)^{np}$ qui ne sera pas divisible par p si $p > n$, d'où le résultat.

En particulier J_p n'est pas nul.

(c) On a $|f(x)| \leq (2n)^m$ pour $0 \leq x \leq n$ de sorte que

$$J_p \leq \sum_{k=0}^{n} |a_k| \int_0^k e^{k-u}|f(u)|du \leq \sum_k |a_k|(2n)^m(e^k - 1) \leq c[(2n)^{n+1}]^p$$

avec $c = e^n \sum |a_k|$, d'où le résultat.

Au final on a donc $|J_p| \geq (p-1)!$ car J_p est non nul et divisible par $(p-1)!$ et $|J_p| \leq c^p$. La contradiction provient du fait que $c^p/(p-1)!$ tend vers 0 lorsque p tend vers $+\infty$.

Exercice 4. Approximation des réels par des rationnels

(i) Soient $p/q \neq a/b$ des rationnels distincts. Montrez que $|p/q - a/b| \geq 1/bq$.

(ii) (a) Soit $P \in \mathbb{Z}[X]$ un polynôme de degré n ne possédant aucune racine rationnelle (i.e. $\forall x \in \mathbb{Q}$, $P(x) \neq 0$). Soit $x \in \mathbb{R}$ un irrationnel tel que $P(x) = 0$. Montrez que pour tout $\delta > 0$ et tout $p/q \in \mathbb{Q}$ avec p et q premiers entre eux et $q > 0$, tel que $|p/q - x| \leq \delta$, il existe une constante $K(x, \delta)$ qui ne dépend que de x et de δ telle que $|p/q - x| \geq K(x)/q^n$.

*(b) Soit $x = \sum_{i=1}^{+\infty} 10^{-i!}$. Justifiez cette écriture et montrez que x est irrationnel. On considère alors $I_x = \{P \in \mathbb{Q}[X],\ P(x) = 0\} = (\mu_x)$ avec $\mu_x \in \mathbb{Z}[X]$ qu'on appelle le polynôme minimal de x sur $\mathbb{Q}$. **On suppose** que μ_x est non nul et on note n son degré. Montrez que μ_x n'a pas de racines rationnelles. En considérant les rationnels $x_k = \sum_{i=1}^{k} 10^{-i!}$ pour $k \geq n$, montrez que l'on aboutit à une contradiction.*

(iii) Soit $x \in \mathbb{R}$ un irrationnel. Soit alors (p_n/q_n) une suite de rationnels écrite sous forme réduite (i.e. p_n et q_n premiers entre eux et $q_n > 0$), convergeant vers x. Montrez que (q_n) tend vers l'infini.

Preuve : (1) $|pb - qa|$ est un entier non nul donc supérieur ou égal à 1.

(2) (a) L'inégalité des AF s'écrit: $|P(p/q) - P(x)| \leq K|x - p/q|$ où K est un majorant de la dérivée de P sur $[x - \delta, x + \delta]$. Comme $P(x) = 0$ et $P(p/q) \neq 0$, on obtient en réduisant au même dénominateur $1/q^n \leq |a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n| \leq K|p/q - x|$ d'où le résultat.

(b) Si μ_x avait une racine, en factorisant, on obtiendrait un polynôme de $\mathbb{Q}[X]$ qui s'annule en x et de degré strictement plus petit que celui de μ_x alors qu'il doit être divisible par ce dernier !

On a $0 \leq x - x_k \leq 210^{-(k+1)!}$ (on prend des 1 partout au lieu de les prendre espacés). On doit donc avoir $210^{n(k!)} \geq K10^{(k+1)!}$ pour tout k ce qui ne se peut pas. (x est donc transcendant)

(3) Soit M, d'après l'indication, on choisit 2ϵ égal au minimum des $x - p_n/q_n$ où $p_n/q_n \in [x-1, x+1]$ (si l'ensemble est vide, on prend $2\epsilon = 1$). Soit alors n_0 tel que pour tout $n \geq n_0$, $|p_n/q_n - x| \leq \epsilon$. On a alors pour tout $n \geq n_0$, $q_n \geq M$, d'où le résultat.

Le dénominateur q^n est alors un facteur cohérent d'estimation de la facilité avec laquelle un réel se laisse approcher par des rationnels. En particulier dans 2-a, le δ n'est pas important car si on se rapproche de x, les dénominateurs q grandissent de sorte que K/q^n sera plus petit que δ ...

(4) C'est le principe des tiroirs et des chaussettes; les chaussettes sont les x_q pour $1 \leq q \leq q_0$ ce qui donne q_0 chaussette. Si une de ces chaussettes est rangée dans tiroir I_0 il n'y a rien à faire. Dans le cas contraire, q_0 chaussettes rangées dans $q_0 - 1$ tiroirs cela donne 2 chaussettes dans le même tiroir, soit $x_{q_1}, x_{q_2} \in I_k$. On écrit $x_{q_1} - x_{q_2} = qx - p$ avec $q = q_1 - q_2$ et $p = E(q_2 x) - E(q_1 x)$. On a bien $0 \leq q \leq q_0$.

3 Construction à la règle et au compas

Soit Σ un ensemble de points du plan $\mathbb{R}^2$; on dit qu'un point P est constructible à la règle et au compas à partir de Σ s'il existe un entier n et une suite de points $P_1, \cdots, P_n = P$ tels que pour tout $i \in \{1, \cdots, n\}$, notant $\Sigma_i = \Sigma \cup \{P_1, \cdots, P_{i-1}\}$, il existe 4 points $A, B, A', B' \in \Sigma_i$ tels que l'une des propriétés suivantes soit vérifiée:

- P_i est le point d'intersection des droites non parallèles (AB), $(A'B')$;
- P_i est l'un des deux points d'intersection de la droite (AB) et du cercle de centre A' passant par B';
- P_i est l'un des points d'intersection des cercles centrés en A, A' et passant respectivement par B, B'.

Un réel x est dit constructible à partir de Σ si le point $(x, 0)$ de $\mathbb{R}^2$ l'est. Un nombre complexe z est dit constructible à partir de Σ si le point si sa partie réelle et imaginaire l'est.

(1) Soit Σ une partie de $\mathbb{R}^2$ contenant $0, 1$ et soit C_Σ l'ensemble des points constructibles à partir de Σ. Montrez que si $x, y \in C_\Sigma$ alors $x + y, x - y, xy, x/y, \sqrt{x}$ sont aussi dans C_Σ.

(2) Désormais $\Sigma = \{0, 1\}$. Montrez qu'un réel x est constructible si et seulement s'il existe un entier n et une suite de sous-corps de $\mathbb{R}$: $\mathbb{Q} = E_0 \subset E_1 \subset \cdots, E_n$ tels que pour tout i, $[E_i : E_{i-1}] = 2$ et $x \in E_n$.

(3) En déduire que si x est constructible, alors x est algébrique de degré une puissance de 2.

(4) Que pensez-vous des problèmes de la duplication du cube, de la trisection des angles et de la quadrature du cercle.

(5) Montrez que $x \in \mathbb{R}$ est constructible si et seulement si le sous-corps de $\mathbb{C}$ engendré par x et ses conjugués est de degré une puissance de 2: autrement dit si le corps de décomposition de x est de degré une puissance de 2.

(6) Montrez que les polygones réguliers constructibles sont les $2^s p_1 \cdots p_r$ où les p_i sont des nombres premiers de Fermat.

Preuve : (1) Ce sont des constructions classiques

(2) Rappelons qu'une équation d'une droite est de la forme $ax + by + c = 0$ tandis que celle d'un cercle est de la forme $x^2 + y^2 + Ax + By + C = 0$. Le point d'intersection de deux droites d'équations $ax + by + c = 0$ et $a'x + b'y + c' = 0$ avec $a, b, c, a', b', c' \in K$ est un point $(x, y) \in K^2$. Le point d'intersection d'une droite d'équation $ax + by + c = 0$ et d'un cercle $x^2 + y^2 + Ax + By + C = 0$ avec $a, b, c, A, B, C \in K$ est un point $(x, y) \in L^2$ où L est une extension de degré au plus deux de K. Le point d'intersection de deux cercles se ramène à celui d'une droite et d'un cercle, l'équation de la droite étant obtenue par soustraction des deux équations des cercles (c'est l'axe radial du faisceau de cercle engendré par ces deux cercles).

(3) C'est clair en utilisant la multiplicativité des degrés.

(4) Le polynôme $X^3 - 2$ n'a pas de racines dans $\mathbb{Q}$, il est donc irréductible et $\sqrt[3]{2}$ est donc de degré 3.

Le point $\sin\alpha$ est constructible à partir de $\cos\alpha$ car $\sin^2\alpha\alpha = 1 - \cos^2\alpha$. La question est donc de savoir si $\cos\alpha/3$ est constructible sur le corps $\mathbb{Q}[\cos\alpha]$. Or comme $\cos(3x) = 4\cos^3 x - 3\cos x$, alors $2\cos(\alpha/3)$ est racine du polynôme $X^3 - 3X + 2\cos\alpha$ les autres racines étant $\cos(\alpha/3 + 2\pi/3)$ et $\cos(\alpha/3 + 4\pi/3)$. Ainsi α est trisectable si et seulement si $X^3 - 3X + 2\cos\alpha$ est réductible sur $\mathbb{Q}[\cos\alpha]$, i.e. a une racine dans $\mathbb{Q}[\cos\alpha]$.

Considérons par exemple $\alpha = \pi/3$ et donc le polynôme $X^3 - 3X - 1$ et soit $a/b \in \mathbb{Q}$ une éventuelle racine. On obtient après réduction au même dénominateur avec $a \wedge b = 1$: $a^3 - 3a^2b - b^3 = 0$ soit $b = 1$ et $a = \pm 1$ ce qui n'est pas.

Le nombre π étant transcendant, la quadrature du cercle est impossible.

(5) Remarquons déjà que si z est constructible alors tout conjugué z' de z l'est aussi. Soit en effet $\mathbb{Q} \subset K_1 \subset \cdots, \subset K_n$ est tour d'extensions quadratiques avec $z \in K_n$ et soit $L/\mathbb{Q}$ une extension galoisienne de $\mathbb{Q}$ contenant K_n. Il existe alors $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $\sigma(z) = z'$ et alors $\mathbb{Q} \subset \sigma(K_1) \subset \cdots \subset \sigma(K_n)$ est une tour d'extension quadratiques avec $z' \in \sigma(K_n)$ et z' est donc constructible.

Soit alors L l'extension de $\mathbb{Q}$ engendrée par z et ses conjugués. D'après ce qui précède tout élément de L est constructible. Or d'après le théorème de l'élément primitif on a $L = \mathbb{Q}[\alpha]$ avec donc α constructible de sorte que $[L : \mathbb{Q}]$ est une puissance de 2.

Réciproquement soit $L/\mathbb{Q}$ une extension galoisienne de degré 2^n. Son groupe de Galois est donc d'ordre 2^n de sorte qu'il existe une suite de sous-groupe distingué

$$(0) = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

avec $G_i/G_{i-1} \simeq \mathbb{Z}/2\mathbb{Z}$. On en déduit alors que la tour $\mathbb{Q} = L^{G_n} \subset L^{G_{n-1}} \subset \cdots \subset L^{G_0} = L$ est une tour d'extensions quadratiques.

Remarque: Pour voir l'existence de la suite de composition formée par les G_i, on raisonne par récurrence sur le cardinal de G. Le centre Z de G n'est pas trivial car G est un p-groupe pour $p = 2$. Si $Z \neq G$, on construit à partir d'une suite de composition de Z et de G/Z une pour G. Si $Z = G$, on considère $2G \neq G$ ainsi que $G/2G$ qui est une $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel, et on procède de même.

(6) Notons $\mathcal{C}$ l'ensemble des nombres n tels que $e^{2i\pi/n}$ soit constructible. De manière élémentaire on a les propriétés suivantes:

- si $n \in \mathcal{C}$ alors $2n \in \mathcal{C}$;
- si $n \in \mathcal{C}$ et $m|n$ alors $m \in \mathcal{C}$;
- si $n, m \in \mathcal{C}$ et $n \wedge m = 1$ alors $nm \in \mathcal{C}$ (utiliser une relation de Bezout).

Il nous reste alors à montrer que si p impair appartient à $\mathcal{C}$ alors p est un nombre de Fermat et que pour tout p premier impair $p^2 \notin \mathcal{C}$: cela découle simplement de l'irréductibilité sur $\mathbb{Q}$ des polynômes cyclotomiques: $e^{2i\pi/p}$ (resp. $e^{2i\pi/p^2}$) est de degré $p-1$ (resp. $p(p-1)$) sur $\mathbb{Q}$ de polynôme minimal $\Phi_p(X) = \frac{X^p-1}{X-1}$ (resp. $\Phi_{p^2}(X) = \frac{X^{p^2}-1}{X^p-1}$.