Christian Maire

CORPS

Christian Maire
E-mail : christian.maire@univ-fcomte.fr
Institut FEMTO-ST, Université de Franche-Comté, 15B Avenue des Montboucons - 25030 Besançon.

21 août 2021

CORPS

Christian Maire

TABLE DES MATIÈRES

1. Extensions de corps 1
1.1. Introduction 1
1.2. Extension engendrée par une partie 2
1.3. Le degré d'une extension 5
1.4. Algébricité et transcendance 6
1.5. Disjonction linéaire 11
1.6. Exercices 15

2. Clôture algébrique d'un corps 27
2.1. Racine d'un polynôme 27
2.2. Théorèmes d'existence 28
2.3. Prolongement des isomorphismes 32
2.4. Exercices 37

3. Groupe des automorphismes d'une extension finie 41
3.1. Rappels 41
3.2. Extensions algébriques normales 42
3.3. Extensions algébriques séparables 44
3.4. Dérivée formelle d'un polynôme. Application à la séparabilité 48
3.5. Extensions galoisiennes 51
3.6. Exercices 53

4. Théorie de Galois 65
4.1. Corps fixes 65
4.2. Correspondance de Galois 69
4.3. Propriétés élémentaires 73
4.4. Norme et trace 75

4.5. Exercices 78

5. Corps finis 91
5.1. La classification 91
5.2. L'automorphisme de Frobenius 93
5.3. Polynômes primitifs 95
5.4. Groupe de Galois sur $\mathbb{Q}$ et réduction modulo p 96
5.5. Exercices 102

6. Corps cyclotomiques - Théorie de Kummer 113
6.1. Racines de l'unité dans un corps 113
6.2. Corps cyclotomiques sur $\mathbb{F}_q$ 117
6.3. Corps cyclotomiques sur $\mathbb{Q}$ 117
6.4. Théorie de Kummer 125
6.5. Exercices 130

7. Constructions à la règle et au compas 153
7.1. Définitions 153
7.2. Les constructions fondamentales 155
7.3. Extensions et CRCA 158
7.4. Exemples 163
7.5. Exercices 166

8. Devoirs maison et Annales 169

CHAPITRE 1

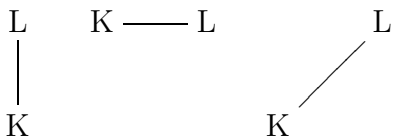
EXTENSIONS DE CORPS

1.1. Introduction

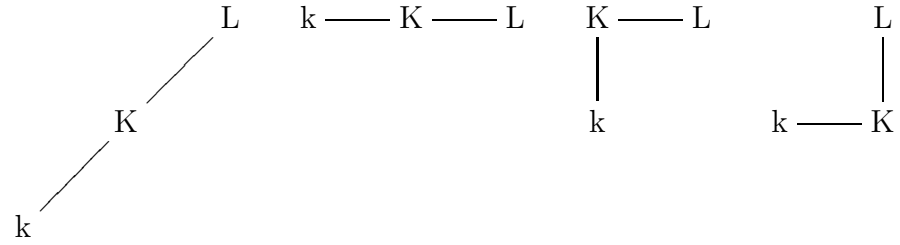
Nous entendons par *corps*, un anneau commutatif K non trivial (contenant donc deux éléments privilégiés : 0 le neutre pour l'addition, et 1 le neutre pour la mutiplication) tel que tout élément non nul est inversible. Commençons par rappeler un fait bien connu pour les corps.

Théorème 1.1.1. — *Soient* K *et* L *deux corps et* $\varphi : \mathrm{K} \to \mathrm{L}$ *un homomorphisme de corps. Alors* φ *est injectif.*

En effet, puisque φ est un homomorphisme de corps $\varphi(1) = 1$. Par conséquent l'image de φ n'est pas réduite à l'idéal (0). Mais d'un autre coté, le noyau de φ est un idéal de K. C'est donc l'idéal nul ou bien K tout entier. Ce dernier est à exclure (car $\mathrm{Im}(\varphi) \neq (0)$) et ainsi $\ker(\varphi) = (0)$.
Ainsi, $\mathrm{K} \hookrightarrow \mathrm{L}$. Par conséquent K peut-être vu comme un sous-corps de L : le corps K est un sous-ensemble de L et les opérations de K coïncident avec celles de L. On dit alors que le corps L est une extension du corps K et on note L/K.
Par la suite, des schémas représentant des extensions permettent de comprendre plus facilement certaines situations. Ainsi, si L/K est une extension de corps, on la représente par l'un des schémas suivants :



Si K/k et L/K sont deux extensions de corps, alors L/k est également une extension de corps. Cette situation peut être représentée par l'un des schémas suivants :



On parle alors de tours d'extensions. Dans ce cas, on dit que L/K est une extension relative de L/k et que K/k est une *sous-extension* de L/k.

Rappelons ensuite comment l'on définit la caractéristique d'un corps K. Pour cela, considérons l'homomorphisme h d'anneaux de $\mathbb{Z}$ dans K défini par $h(1) = 1$. L'image $\mathrm{Im}(h)$ est un anneau intégre et ainsi, $\ker(h)$ est un idéal premier de $\mathbb{Z}$. C'est donc ou bien (0) ou bien $p\mathbb{Z}$, p étant un nombre premier. Le corps K est de caractéristique 0 si l'homomorphisme h est injectif. Dans ce cas, l'homomorphisme h se prolonge en un morphisme de corps de $\mathbb{Q}$ vers K et ainsi K est une extension de $\mathbb{Q}$. Si le noyau de h est de la forme $p\mathbb{Z}$, par factorisation, h induit un morphisme de corps de $\mathbb{F}_p$ $(= \mathbb{Z}/p\mathbb{Z})$ vers K, et ainsi K est une extension de $\mathbb{F}_p$.
En conclusion, nous venons de montrer que tout corps est une extension d'un *sous-corps premier* $\mathbb{Q}$ ou $\mathbb{F}_p$.

Exemple 1.1.2. — 1) Le corps des nombres complexes $\mathbb{C}$ est une extension de $\mathbb{Q}$ mais aussi du corps des nombres réels $\mathbb{R}$; $\mathbb{C}/\mathbb{R}$ est une extension relative de $\mathbb{C}/\mathbb{Q}$ et $\mathbb{R}/\mathbb{Q}$ est une sous-extension de $\mathbb{C}/\mathbb{Q}$.
2) Si K_1/K et K_2/K sont deux extensions de K, alors $\mathrm{K}_1 \cap \mathrm{K}_2$ est un corps contenant K, c'est donc aussi une extension de K. Le corps $\mathrm{K}_1 \cap \mathrm{K}_2$ est une sous-extension de K_1/K.

1.2. Extension engendrée par une partie

Définition 1.2.1. — Soit K/k une extension de corps et soit A une partie de K. On note par $\mathrm{k}(A)$ l'intersection de toutes les sous-extensions

F/k de K/k contenant A. On dit que $\mathrm{k}(A)$ est la sous-extension de K/k engendrée par A.

Le sous-ensemble $\mathrm{k}(A)$ de K est bien un corps (cf. exemple 1.1.2) qui contient k et est contenu dans K. Le corps $\mathrm{k}(A)$ est le corps engendré par $\mathrm{k} \cup A$.
Nous allons donner une première réduction montrant que l'étude de $\mathrm{k}(A)/\mathrm{k}$ se ramène à A fini.

Proposition 1.2.2. — *Soit* K/k *une extension de corps et soit* A *une partie de* K. *Alors*

$$\mathrm{k}(A) = \bigcup_{\substack{B \subset A \\ B \text{ fini}}} \mathrm{k}(B).$$

Démonstration. — Soit $B \subset A$. Alors $\mathrm{k}(B) \subset \mathrm{k}(A)$ ce qui prouve l'inclusion $\bigcup_{\substack{B \subset A \\ B \text{ fini}}} \mathrm{k}(B) \subset \mathrm{k}(A)$.
Pour l'inclusion inverse, il suffit de noter que $\bigcup_{\substack{B \subset A \\ B \text{ finie}}} \mathrm{k}(B)$ est un corps contenant A et k : il contient donc $\mathrm{k}(A)$. □

Si $A = \{\alpha_1, \cdots, \alpha_n\}$, on note alors $\mathrm{k}(A) = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$. Si $A = \{\alpha\}$, on dit que $\mathrm{k}(\alpha)$ est une sous-extension simple de K/k.
Lorsque A est fini, la description de $\mathrm{k}(A)$ est alors aisée :

Théorème 1.2.3. — *Soit* K/k *une extension de corps et soit* $A = \{\alpha_1, \cdots, \alpha_n\}$ *une famille d'éléments de* K. *Alors*

$$\mathrm{k}(\alpha_1, \cdots, \alpha_n) = \{\frac{P(\alpha_1, \cdots, \alpha_n)}{Q(\alpha_1, \cdots, \alpha_n)}, P, Q \in \mathrm{k}[X_1, \cdots, X_n], Q(\alpha_1, \cdots, \alpha_n) \neq 0\}.$$

Démonstration. — L'ensemble de droite est clairement contenu dans $\mathrm{k}(\alpha_1, \cdots, \alpha_n)$. Il suffit alors de noter que cet ensemble (de droite donc) est un corps, ce qui est immédiat. □

Proposition 1.2.4. — *Soient* K/k *une extension de corps et,* A *et* B *deux ensembles d'éléments de* K. *Alors* $\mathrm{k}(A)(B) = \mathrm{k}(A \cup B) = \mathrm{k}(B)(A)$. *En particulier, si* α *et* β *sont deux éléments de* K, *il vient*

$$\mathrm{k}(\alpha)(\beta) = \mathrm{k}(\alpha, \beta) = \mathrm{k}(\beta)(\alpha).$$

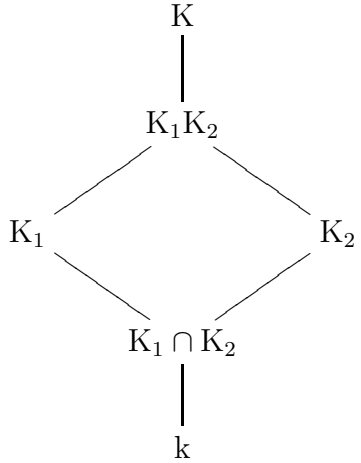
Démonstration. — Comme $A \subset A \cup B$, il vient $\mathrm{k}(A) \subset \mathrm{k}(A \cup B)$. Maintenant le corps $\mathrm{k}(A \cup B)$ est une extension de $\mathrm{k}(A)$ contenant B. Par minimalité de $\mathrm{k}(A)(B)$, il vient $\mathrm{k}(A)(B) \subset \mathrm{k}(A \cup B)$.
Réciproquement. Le corps $\mathrm{k}(A)(B)$ contient k et $A \cup B$. Par minimalité de $\mathrm{k}(A \cup B)$, il vient $\mathrm{k}(A \cup B) \subset \mathrm{k}(A)(B)$. □

Définition 1.2.5. — Soient $(\mathrm{K}_i)_{i \in I}$ une famille de sous-extensions de K/k. Alors le compositum des $\mathrm{K}_i, i \in I$, est défini par

$$\prod_{i \in I} \mathrm{K}_i := \mathrm{k}(\bigcup_{i \in I} \mathrm{K}_i).$$

Le compositum des $(\mathrm{K}_i)_{i \in I}$ est donc la plus petite sous-extension de K/k contenant les corps K_i, $i \in I$.

Pour un compositum de deux extensions K_1/k et K_2/k, on obtient le schéma suivant :



.

Le compositum $\mathrm{K}_1\mathrm{K}_2$ contient bien K_1 et K_2, et c'est la plus petite sous-extension de K contenant K_1 et K_2. À noter que l'intersection $\mathrm{K}_1 \cap \mathrm{K}_2$ est bien une sous-extension de K/k contenue dans K_1 et K_2.

Proposition 1.2.6. — *Soient* K/k *une extension et* A, B *deux ensembles d'éléments de* K. *Alors*

$$\mathrm{k}(A)\mathrm{k}(B) = \mathrm{k}(A \cup B).$$

En particulier $\mathrm{k}(\alpha_1)\cdots\mathrm{k}(\alpha_n) = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$.

Démonstration. — Le compositum $\mathrm{k}(A)\mathrm{k}(B)$ est la plus petite sous-extension de K/k contenant $\mathrm{k}(A)$ et $\mathrm{k}(B)$. Ces deux corps sont contenus dans $\mathrm{k}(A \cup B)$, ainsi $\mathrm{k}(A)\mathrm{k}(B) \subset \mathrm{k}(A \cup B)$.
Réciproquement. Comme $A \subset \mathrm{k}(A)$ et $B \subset \mathrm{k}(B)$, il vient $A \cup B \subset \mathrm{k}(A)\mathrm{k}(B)$, et ainsi $\mathrm{k}(A \cup B) \subset \mathrm{k}(A)\mathrm{k}(B)$. □

1.3. Le degré d'une extension

Soit K/k une extension. La multiplication dans K définie une loi externe de k sur K permettant de considérer K comme un k-espace vectoriel.

Définition 1.3.1. — Soit K/k une extension. Le degré de K/k, noté [K : k], est par définition la dimension du k-espace vectoriel K. Le degré est un entier, à l'exception du cas où le k-espace vectoriel K est infini.

Remarque 1.3.2. — [K : k] = 1 si et seulement si K = k.

Remarque 1.3.3. — Si $[\mathrm{k}(\alpha) : \mathrm{k}] = n$, on dit que α est de degré n sur k.

Remarque 1.3.4. — Quand [K : k] = 2, on dit que K/k est une extension quadratique.

Exemple 1.3.5. — $[\mathbb{C} : \mathbb{R}] = 2$; $[\mathbb{R} : \mathbb{Q}] = \infty$ (provient du fait que $\mathbb{R}$ n'est pas dénombrable) ; $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (une $\mathbb{Q}$-base étant $(1, \sqrt{2})$).

***Théorème 1.3.6* (Transitivié du degré)**. — *Soient* L/K *et* K/k *deux extensions de corps. Alors*

$$[\mathrm{L} : \mathrm{k}] = [\mathrm{L} : \mathrm{K}][\mathrm{K} : \mathrm{k}].$$

Démonstration. — La preuve repose sur le lemme suivant :

Lemme 1.3.7. — *Si* $(e_i)_{i\in I}$ *forme une* k*-base de* K *et* $(\varepsilon_j)_{j\in J}$ *une* K*-base de* L, *alors* $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ *forme une* k*-base de* L.

Démonstration. — Montrons que la famille $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est génératrice pour le k-espace vectoriel L. Soit $x \in$ L. Alors il existe une partie finie J_0 de J telle que

$$x = \sum_{j\in J_0} a_j\varepsilon_j,$$

avec $a_j \in$ K. Pour chaque a_j, il existe une partie finie $I_0^{(j)}$ telle que

$$a_j = \sum_{i\in I_0^{(j)}} \lambda_i e_i,$$

et au total

$$x = \sum_{j\in J_0}\sum_{i\in I_0^{(j)}} \lambda_i e_i\varepsilon_j.$$

Montrons que la famille $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre. Il suffit de montrer que pour tout sous-ensemble fini I_0 et J_0 de I et de J, la famille $(e_i\varepsilon_j)_{(i,j)\in I_0\times J_0}$ est k-libre. Soient $\lambda_{i,j} \in$ k tels que

$$\sum_{(i,j)\in I_0\times J_0} \lambda_{i,j}e_i\varepsilon_j = 0.$$

Alors utilisant la liberté de $(\varepsilon_j)_{j\in J_0}$, il vient :

$$\forall j,\ \sum_{i\in I_0} \lambda_{i,j}e_i = 0.$$

Puis, utilisant la liberté de $(e_i)_{i\in I_0}$, il vient $\lambda_{i,j} = 0$, d'où le résultat. □

La preuve du théorème 1.3.6 est alors immédiate. Si I ou J sont infinis, alors [L : k] $= \infty$. Sinon, [L : k] $= |I||J| =$ [L : K][K : k]. □

1.4. Algébricité et transcendance

1.4.1. Nombres algébriques, nombres transcendants. — Soit K/k une extension et soit $\alpha \in$ K. Notons par φ_α l'homomorphisme (d'anneaux) d'evaluation :

$$\begin{array}{rcl} \varphi_\alpha : \mathrm{k}[X] & \to & \mathrm{K} \\ P & \mapsto & P(\alpha) \end{array}$$

Comme $\mathrm{Im}(\varphi_\alpha)$ est un sous-anneau de K qui est intègre, le noyau de φ_α est un idéal premier de $\mathrm{k}[X]$. C'est soit l'idéal nul (0), soit un idéal maximal (P), P étant ici un polynôme irréductible de $\mathrm{k}[X]$.

Définition 1.4.1. — L'élément α est dit transcendant sur k si $\ker(\varphi_\alpha) = (0)$.
L'élément α est dit algébrique sur k si $\ker(\varphi_\alpha) = (P)$, P étant un polynôme irréductible de $\mathrm{k}[X]$.

Remarque 1.4.2. — L'élement α est transcendant sur k si et seulement si aucun polynôme non nul de $\mathrm{k}[X]$ ne s'annule en α.

Exemple 1.4.3. — Les éléments i et $\sqrt[3]{3}$ sont algébriques sur $\mathbb{Q}$.

Théorème 1.4.4. — *Soit* K/k *une extension.*
1) Soit $\alpha \in \mathrm{K}$ *algébrique sur* k. *Alors il existe un polynôme irréductible* $P \in \mathrm{k}[X]$ *tel que*

$$\mathrm{k}[X]/(P) \simeq \mathrm{k}(\alpha).$$

De plus $[\mathrm{k}(\alpha) : \mathrm{k}] = \deg(P) = n$ *et* $(1, \alpha, \cdots, \alpha^{n-1})$ *forme une* k*-base de* $\mathrm{k}(\alpha)$. *On a ainsi* $\mathrm{k}(\alpha) = \mathrm{k}[\alpha]$, *où* $\mathrm{k}[\alpha] = \{Q(\alpha), Q \in \mathrm{k}[X]\}$.
2) Soit $\alpha \in \mathrm{K}$ *transcendant sur* k. *Alors*

$$\mathrm{k}(\alpha) \simeq \mathrm{k}(X),$$

et $[\mathrm{k}(\alpha) : \mathrm{k}] = \infty$.

Démonstration. — 1) Puisque α est algébrique sur k, $\ker(\varphi_\alpha) = (P)$, avec P un polynôme irréductible de $\mathrm{k}[X]$. Le théorème de factorisation indique que $\mathrm{k}[\alpha] = \mathrm{Im}(\varphi_\alpha) \simeq \mathrm{k}[X]/(P)$. L'idéal (P) étant maximal, le quotient $\mathrm{k}[X]/(P)$ est un corps et il en est de même pour $k[\alpha]$. Par minimalité de $\mathrm{k}(\alpha)$, on obtient $k(\alpha) = \mathrm{k}[\alpha]$.
Soit n le degré de P. Soit $Q \in \mathrm{k}[X]$. Effectuons la division euclidienne de Q par P :

$$Q = PB + R,$$

avec $\deg(R) < n$. Alors $Q(\alpha) = P(\alpha)B(\alpha) + R(\alpha) = R(\alpha)$ et ainsi la famille $(1, \alpha, \cdots, \alpha^{n-1})$ engendre $\mathrm{k}[\alpha] = \mathrm{k}(\alpha)$ comme k-espace vectoriel.

Supposons cette famille liée. Il existe un entier $i < n$, des éléments $a_0, \cdots, a_i \in \mathrm{k}$ tels que

$$a_i\alpha^i + a_{i-1}\alpha^{i-1} + \cdots + a_1\alpha + a_0 = 0.$$

Soit $R = a_iX^i + \cdots a_1X + a_0 \in \mathrm{k}[X]$. La relation précédente indique que $R(\alpha) = 0$ ou encore que $R \in \ker(\varphi_\alpha) = (P)$. Ainsi $P|R$. Comme $\deg(R) < \deg(P)$, alors $R = 0$, ou encore $a_i = \cdots = a_0 = 0$.
2) Supposons α transcendant. Alors $\ker(\varphi_\alpha) = (0)$ et ainsi $\mathrm{k}[X] \simeq \mathrm{k}[\alpha] \subset \mathrm{k}(\alpha)$. Comme pour tout polynôme non nul $Q \in \mathrm{k}[X]$, on a $Q(\alpha) \neq 0$, l'homomorphisme φ_α se prolonge en un homomorphisme injectif φ'_α de $\mathrm{k}(X)$ vers $\mathrm{k}(\alpha)$. Le théorème 1.2.3 montre ensuite que ce morphisme φ'_α est surjectif et c'est donc un isomorphisme. □

Corollaire 1.4.5. — *L'élément α est algébrique sur* k *si et seulement si l'espace vectoriel* $\mathrm{k}[\alpha]$ *est de dimension finie sur* k.

Définition 1.4.6. — Si $\alpha \in \mathrm{K}$ est algébrique sur k, le polynôme P (qui engendre $\ker(\varphi_\alpha)$) est unique si on le choisit unitaire. Dans ce cas, on l'appelle le polynôme irréductible de α sur k et on le note $\mathrm{Irr}(\alpha, \mathrm{k})$.

Remarque 1.4.7. — Si $Q \in \mathrm{k}[X]$ s'annule en $X = \alpha$, alors $\mathrm{Irr}(\alpha, \mathrm{k})$ divise Q dans $\mathrm{k}[X]$.

Proposition 1.4.8. — *Soit la tour d'extensions* $\mathrm{k} \text{ —— } \mathrm{K} \text{ —— } \mathrm{L}$.
Si $\alpha \in \mathrm{L}$ est algébrique sur k*, alors α est algébrique sur* K *et*

$$[\mathrm{K}(\alpha) : \mathrm{K}] \leq [\mathrm{k}(\alpha) : \mathrm{k}].$$

Par contre si α est transcendant sur K*, alors α est transcendant sur* k.

Démonstration. — Si α est algébrique sur k, alors α annule $\mathrm{Irr}(\alpha, \mathrm{k})$. Ce polynôme peut être vu dans $\mathrm{K}[X]$ et ainsi α et algébrique sur K et $\mathrm{Irr}(\alpha, K)|\mathrm{Irr}(\alpha, \mathrm{k})$, d'où l'assertion sur le degré.
Si α est transcendant sur K, aucun polynôme non nul à coefficients dans K, en l'occurence dans k, ne s'annule en α. Ainsi α est transcendant sur k. □

Remarque 1.4.9. — L'ensemble des nombres algébriques sur $\mathbb{Q}$ est dénombrable. En particulier, il existe des nombres réels transcendants.

Exemple 1.4.10. — L'élément $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$. En effet l'élément $\sqrt[3]{2}$ est racine du polynôme X^3-2 qui est irréductible sur $\mathbb{Q}$ (critère d'Eisenstein appliqué au premier 2), c'est donc le polynôme irréductible de $\sqrt[3]{2}$: $\mathrm{Irr}(\sqrt[3]{2},\mathbb{Q}) = X^3-2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(X^3-2) = 3$.

Exemple 1.4.11. — Montrons que $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}] = 4$. Le corps $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$, ce qui n'est pas le cas de $\mathbb{Q}(i,\sqrt{2})$ (car $i \notin \mathbb{R}$). Ainsi le corps $\mathbb{Q}(i,\sqrt{2})$ contient strictement le corps $\mathbb{Q}(\sqrt{2})$ et donc $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(\sqrt{2})] > 1$.
Notons ensuite que $\mathrm{Irr}(i,\mathbb{Q}) = X^2+1$, par conséquent $\mathrm{Irr}(i,\mathbb{Q}(\sqrt{2}))$ divise X^2+1 et ainsi $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Au total, $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(\sqrt{2}] = 2$ et $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2} : \mathbb{Q}] = 4$. Au passage, on note que $(1,i)$ forme une $\mathbb{Q}(\sqrt{2})$-base de $\mathbb{Q}(i,\sqrt{2})$.

1.4.2. Extensions algébriques, extensions transcendantes. —

Définition 1.4.12. — L'extension K/k est dite algébrique si **tous** les éléments de K sont algébriques sur k. Sinon, elle est dite transcendante.

Commençons par donner une conséquence immédiate du corollaire 1.4.5.

Proposition 1.4.13. — *Toute extension* K/k *de degré fini est algébrique.*

Démonstration. — En effet, soit $\beta \in$ K. Alors k$[\beta] \subset$ K et ainsi k$[\beta]$ est un sous-k-espace vectoriel de K. La dimension de k$[\beta]$ sur k est donc plus petite que celle de K sur k qui est finie. Ainsi, d'après le corollaire 1.4.5, l'élément β est algébrique sur k. □

Corollaire 1.4.14. — *Soient* $\alpha_1,\cdots,\alpha_n \in$ K *des éléments quelconques. Alors* k$(\alpha_1,\cdots,\alpha_n)$/k *est une extension algébrique si et seulement si tous les éléments* α_i *sont algébriques sur* k.

Démonstration. — Un sens est évident. Si k$(\alpha_1,\cdots,\alpha_n)$/k est une extension algébrique, alors les éléments α_i sont algébriques sur k.
Réciproquement. Supposons les éléments α_i tous algébriques sur k. D'après la proposition 1.4.8, [k$(\alpha_1,\cdots,\alpha_i,\alpha_{i+1})$: k$(\alpha_1,\cdots,\alpha_i)$] est fini, et au total

$$[\mathrm{k}(\alpha_1,\cdots,\alpha_n) : \mathrm{k}] = [\mathrm{k}(\alpha_1,\cdots,\alpha_n) : \mathrm{k}(\alpha_1,\cdots,\alpha_{n-1})]\cdots[\mathrm{k}(\alpha_1) : \mathrm{k}],$$

l'est aussi. La proposition 1.4.13 s'applique. □

On peut aller un peu plus loin que la proposition 1.4.13.

Théorème 1.4.15. — *Soit* K/k *une extension quelconque. Tout compositum d'extensions quelconques* $K_i, i \in I$, *de* k *(contenues dans* K*) est une extension algébrique de* k *si et seulement si toutes les extensions* K_i/k, $i \in I$, *sont algébriques.*

Démonstration. — Un sens est immédiat : si le compositum est algébrique, alors toutes les extensions sont algébriques.
Réciproquement. Commençons par montrer que l'ensemble E des éléments algébriques de K sur k contenus dans K forme un corps. C'est assez immédiat. Soit $\alpha \neq 0$ et β dans E. Alors $\alpha^{-1} \in k(\alpha)$ et est donc algébrique et $\alpha - \beta$, $\alpha\beta$, $\alpha^{-1}\beta$ sont dans $k(\alpha, \beta)$ et sont donc algébriques par le corollaire 1.4.14. Ainsi E est un sous-corps de K contenant k : c'est donc une extension algébrique de k. Toute extension algébrique de k contenue dans K est contenue dans E. Le compositum F d'extensions algébriques de k est donc contenu dans E (par minimalité) et ainsi tout élément de F est contenu dans E et est donc algébrique sur k : l'extension F/k est algébrique. □

Définition 1.4.16. — Soit K/k une extension quelconque. Le corps E constitué de tous les éléments algébriques sur k est la plus grande extension algébrique de k contenue dans K. C'est aussi le compositum de toutes les extensions algébriques de k contenues dans K. Le corps E est la fermeture algébrique de k dans K.

Proposition 1.4.17. — *Les extensions* L/K *et* K/k *sont algébriques si et seulement* L/k *est algébrique.*

Démonstration. — Un sens est immédiat. Supposons L/k algébrique. Alors tout élément α de L est algébrique sur k donc sur K (voir par exemple que $\mathrm{Irr}(\alpha, k) \in K[X]$!) et tout élément α de K est algébrique sur k (car $\alpha \in L$!) : L/K et K/k sont donc algébriques.
Réciproquement. Soit α un élément de L. Par hypothèse, α est algébrique sur K : $[K(\alpha) : K] = n$. Il existe $P = a_0 + \cdots a_{n-1}X^{n-1} + X^n \in K[X]$ tel que $P(\alpha) = 0$ (en fait $P = \mathrm{Irr}(\alpha, K)$). Considérons l'extension k′ =

$\mathrm{k}(a_0, \cdots, a_n)$. Comme l'extension K/k est algébrique, les éléments a_i sont algébriques sur k et ainsi l'extension k′/k est algébrique et est même finie (cf. corollaire 1.4.14 et sa preuve). L'élément α est algébrique sur k′ et au total $[\mathrm{k}'(\alpha) : \mathrm{k}]$ est fini. Il en est de même pour $[\mathrm{k}(\alpha) : \mathrm{k}]$ (car $\mathrm{k}(\alpha) \subset \mathrm{k}'(\alpha)$). □

Si l'ensemble A est constitué d'éléments de l'extension K/k, notons par $\mathrm{k}[A]$ le sous-anneau de $\mathrm{k}(A)$ dont les éléments sont des polynômes en plusieurs variables sur k évalués en A. Si $A = \{\alpha\}$ et que α est algébrique, nous savons que $\mathrm{k}[\alpha] = \mathrm{k}(\alpha)$. Pour le cas général, nous avons :

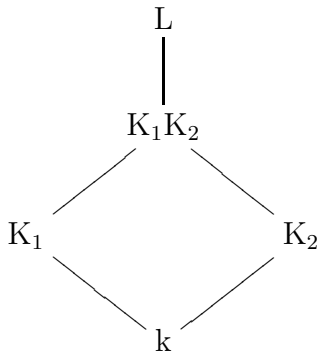
Corollaire 1.4.18. — *Soit* K/k *une extension et soit* A *une partie de* K. *Si* $\mathrm{k}(A)/\mathrm{k}$ *est algébrique alors* $\mathrm{k}(A) = \mathrm{k}[A]$.

Démonstration. — D'après la proprosion 1.2.2, il suffit de considérer le cas où A est fini. Cela va simplement être une récurrence. Si $|A| = 1$, alors d'après le théorème 1.4.4, on a bien $\mathrm{k}(\alpha) = \mathrm{k}[\alpha]$. Supposons $A = \{\alpha_1, \cdots, \alpha_{n+1}\}$. Alors $\mathrm{k}(A) = \mathrm{k}(\alpha_1, \cdots, \alpha_n)(\alpha_{n+1})$. L'élément α_{n+1} est algébrique sur k donc sur $\mathrm{k}(\alpha_1, \cdots, \alpha_n)$ et ainsi $\mathrm{k}(A) = \mathrm{k}(\alpha_1, \cdots, \alpha_n)[\alpha_{n+1}]$. Appliquons ensuite l'hypothèse de récurrence, pour aboutir à $\mathrm{k}(A) = \mathrm{k}[\alpha_1, \cdots, \alpha_n][\alpha_{n+1}] = \mathrm{k}[\alpha_1, \cdots, \alpha_n, \alpha_{n+1}]$. □

1.5. Disjonction linéaire

Pour simplifier, dans cette partie nous supposons que les extensions considérées sont toutes algébriques.

Proposition 1.5.1. — *Soient les sous-extensions* K_1/k *et* K_2/k *de l'extension algébrique* L/k



Alors toute famille d'éléments $(e_i)_{i\in I}$ *de* K_2 *engendrant* K_2 *comme* k*-espace vectoriel, engendre* $\mathrm{K}_1\mathrm{K}_2$ *comme* K_1*-espace vectoriel. En particulier, si* $[\mathrm{K}_2 : \mathrm{k}]$ *est fini,* $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{K}_1] \leq [\mathrm{K}_2 : \mathrm{k}]$.

Démonstration. — Soit $(e_i)_{i\in I}$ des éléments de K_2 engendrant K_2 comme k-espace vectoriel. Alors $\mathrm{K}_2 = \mathrm{k}((e_i)_{i\in I})$ et ainsi $\mathrm{K}_1\mathrm{K}_2 = \mathrm{K}_1\mathrm{k}((e_i)_{i\in I}) = \mathrm{K}_1((e_i)_{i\in I})$. Les éléments e_i sont algébriques sur k, ils sont aussi algébriques sur K_1 et d'après le corollaire 1.4.18, $\mathrm{K}_1\mathrm{K}_2 = \mathrm{K}_1[(e_i)_{i\in I}]$. Comme pour tout j et tout entier n, $e_j^n \in \sum_{i\in I} \mathrm{k}e_i$, on obtient $\mathrm{K}_1\mathrm{K}_2 = \mathrm{K}_1[(e_i)_{i\in I}] = \sum_{i\in I} \mathrm{K}_1 e_i$. □

Définition 1.5.2. — Soient les sous-extensions K_1/k et K_2/k de L/k. Alors l'extension K_2 est linéairement disjointe de K_1 sur k si toute famille de K_2 libre sur k est libre sur K_1 (lorsque celle-ci est vue dans le compositum $\mathrm{K}_1\mathrm{K}_2$).

Remarque 1.5.3. — Grâce au théorème de la base adaptée, dans la définition précédente, on peut remplacer "libre" par "base" : toute k-base de K_2 est une K_1-base de $\mathrm{K}_1\mathrm{K}_2$.

Remarque 1.5.4. — Si K_2 est linéairement disjointe de K_1 sur k, alors $\mathrm{K}_1 \cap \mathrm{K}_2 = \mathrm{k}$. En effet, sinon il existe $x \in \mathrm{K}_1 \cap \mathrm{K}_2$ qui n'est pas dans k et donc la famille $(1, x)$ libre sur k ne l'est plus sur K_1.

Proposition 1.5.5. — *Supposons l'extension* K_2 *de degré fini sur* k. *Alors l'extension* K_2 *est linéairement disjointe de* K_1 *sur* k *si et seulement si* $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{K}_1] = [\mathrm{K}_2 : \mathrm{k}]$.

Démonstration. — Immédiat. □

Remarque 1.5.6. — Lorsque K_1/k est aussi de degré fini, il est immédiat de voir (grâce à la transitivité du degré) que l'extension K_2 est linéairement disjointe de K_1 sur k si et seulement si l'extension K_1 est linéairement disjointe de K_2 sur k. Dans ce cas (où les degrés sont finis), on obtient ainsi en conclusion que l'extension K_2 est linéairement disjointe de K_1 sur k si et seulement si $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}] = [\mathrm{K}_1 : \mathrm{k}][\mathrm{K}_2 : \mathrm{k}]$.

Pour le cas général, nous avons aussi la symétrie :

Proposition 1.5.7. — *L'extension* K_2 *est linéairement disjointe de* K_1 *sur* k *si et seulement si l'extension* K_1 *est linéairement disjointe de* K_2 *sur* k.

Remarque 1.5.8. — Cette proposition nous permet alors de parler d'extensions K_1/k et K_2/k linéairement disjointes (sur k).

Démonstration. — Supposons l'extension K_2 linéairement disjointe de K_1 sur k. Soit $(e_i)_{i\in I}$, I fini, une famille de K_1 libre sur k. On veut montrer que $(e_i)_{i\in I}$ est libre sur K_2. Raisonnons par l'absurde. Supposons la famille $(e_i)_{i\in I}$ liée sur K_2. Soit $I' \subset I$ de cardinal minimal n tel que $(e_i)_{i\in I'}$ est liée sur K_2. Nommons les éléments de $I' : 1, \cdots, n$. Il existe une famille $(a_i)_{i\in I'}$ d'éléments de K_2 telle que

$$\sum_{i=1}^{n} a_i e_i = 0. \tag{1}$$

Par minimalité de I', les éléments a_i sont tous non nuls. La famille $(a_i)_{i\in I'}$ n'étant pas libre sur K_1, elle n'est donc pas libre sur k. Il existe une famille d'éléments $(\lambda_i)_{i\in I'}$ de k telle que $\sum_{i=1}^{n} \lambda_i a_i = 0$, avec au moins un élément λ_{i_0} non nul. Quitte à revoir la numérotation, on peut supposer $i_0 = 1$ et $\lambda_1 = 1$. En isolant a_1, on obtient $a_1 = -\sum_{i=2}^{n} \lambda_i a_i$. En reportant dans la

relation (1), il apparaît

$$\sum_{i=2}^{n} a_i(e_i - \lambda_i e_1) = 0.$$

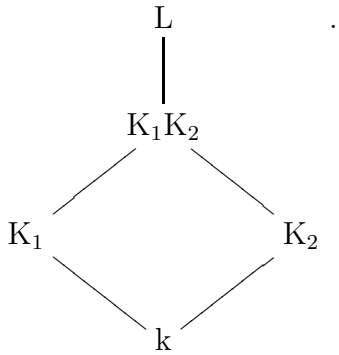
Comme $(e_i)_{i\in I'}$ est k-libre, pour $i = 2, \cdots, n$, $e_i \neq \lambda_i e_1$. La famille $(a_i)_{i=2,\cdots,n}$ est donc liée sur K_1, elle l'est aussi sur k. Quitte à renuméroter, on peut supposer que a_2 appartient au k-espace vectoriel engendré par $a_3, \cdots, a_n$. Il en est de même pour a_1. Bref, en continuant le processus, on obtient que les a_i, $i = 1, \cdots, n$, sont propotionnels à a_n : il existe $x_i \in \mathrm{k}$ tels que $a_i = x_i a_n$. En reportant dans (1), on obtient

$$a_n \sum_{i=1}^{n} x_i e_i = 0.$$

Comme a_n est non-nul, on a une relation linéaire non nulle sur k entre les éléments e_i, ce qui est en contradiction avec l'une des hypothèses initiales. □

Voici un critère utile dans la pratique :

Proposition 1.5.9. — *Soient les sous-extensions finies* K_1/k *et* K_2/k *de* L/k



Alors si les entiers $[\mathrm{K}_1 : \mathrm{k}]$ *et* $[\mathrm{K}_2 : \mathrm{k}]$ *sont premiers entre eux, les extensions* K_1/k *et* K_2/k *sont linéairement disjointes.*

Démonstration. — La transitivité du degré indique que $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}]$ est divisible par $[\mathrm{K}_1 : \mathrm{k}]$ et par $[\mathrm{K}_2 : \mathrm{k}]$: ainsi $[\mathrm{K}_1 : \mathrm{k}][\mathrm{K}_2 : \mathrm{k}] \mid [\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}]$. Comme $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}] \leq [\mathrm{K}_1 : \mathrm{k}][\mathrm{K}_2 : \mathrm{k}]$, on obtient $[\mathrm{K}_1\mathrm{K}_2 : \mathrm{k}] = [\mathrm{K}_1 : \mathrm{k}][\mathrm{K}_2 : \mathrm{k}]$, on conclut avec la remarque 1.5.6. □

Remarque 1.5.10. — Soient K_1/k et K_2/k deux extensions quadratiques contenues dans K/k et telles que $K_1 \cap K_2 = k$. Alors les extensions K_1/k et K_2/k sont linéairement disjointes (voir l'exercice 5). Le compositum K_1K_2 est de degré 4 sur k. On dit que l'extension K_1K_2/k est une extension biquadratique.

Terminons cette partie par la proposition suivante.

Proposition 1.5.11. — *Considérons le schéma d'extensions finies*

$$\begin{array}{ccccccc} K_2 & \text{——} & K_2K_1 & \text{——} & K_2K_1' & \text{——} & L \\ | & & | & & | & & \\ k & \text{——} & K_1 & \text{——} & K_1' & & \end{array}$$

Alors K_2 *et* K_1' *sont linéairement disjointes sur* k *si et seulement si*

(i) K_1 *et* K_2 *sont linéairement disjointes sur* k *;*

(ii) K_1K_2 *et* K_1' *sont linéairement disjointe sur* K_1*.*

Démonstration. — Le point (i) équivaut à $[K_2K_1 : K_1] = [K_2 : k]$ et le point (ii) équivaut à $[K_2K_1' : K_1'] = [K_2K_1 : K_1]$. On voit ainsi que si (i) et (ii) sont satisfaits alors $[K_2K_1' : K_1'] = [K_2 : k]$ ce qui équivaut à la disjonction linéaire entre K_2 et K_1'.
Réciproquement. Supposons les extensions K_2 et K_1' linéairement disjointes sur k ou encore $[K_2K_1' : K_1'] = [K_2 : k]$. Alors $[K_2K_1' : k] = [K_2K_1' : K_2K_1][K_2K_1 : K_2][K_2 : k]$ mais aussi $[K_2K_1' : k] = [K_2K_1' : K_1'][K_1' : K_1][K_1 : k]$. Il vient au total

$$[K_2K_1' : K_2K_1][K_2K_1 : K_2] = [K_1' : K_1][K_1 : k],$$

tout en sachant que $[K_2K_1' : K_2K_1] \leq [K_1' : K_1]$ et $[K_2K_1 : K_2] \leq [K_1 : k]$. On obtient les égalités souhaitées. □

1.6. Exercices

Nous désignons par $j = \dfrac{-1 + i\sqrt{3}}{2} \in \mathbb{C}$ une racine cubique de l'unité.

1.6.1. Énoncés. —

Exercice 1. — *Énoncer puis montrer le critère d'irréductibilité d'Eisenstein (sur* $\mathbb{Z}$*).*

Exercice 2. — *Soit* $P = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$*,* $a \neq 0$*. Montrer que* P *est irréductible sur* $\mathbb{Q}$ *si et seulement si* $P(n/m) \neq 0$*, pour toute fraction* $n/m \in \mathbb{Q}$*,* $n \in \mathbb{Z}$*,* $m \in \mathbb{N}$*,* $(n, m) = 1$*,* $n|d$ *et* $m|a$*.*

Exercice 3. — *Calculer* $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$*.*

Exercice 4. — *Montrer que le degré de* $\mathbb{R}/\mathbb{Q}$ *est infini.*

Exercice 5. — *Soit* K/k *une extension de degré* 2 *et soit* L/k *une extension algébrique quelconque. Montrer que* L/k *et* K/k *sont linéairement disjointes si et seulement si* $\mathrm{K} \cap \mathrm{L} = \mathrm{k}$*.*

Exercice 6. — *Déterminer le diagramme des extensions en les corps* $\mathbb{Q}(X, Y)$*,* $\mathbb{Q}(X, Y^2)$*,* $\mathbb{Q}(X^2, Y)$*,* $\mathbb{Q}(X^2, Y^2)$ *tout en indiquant les degrés.*

Exercice 7. — *Soit* $F(a)/F$ *une extension de degré impair. Montrer que* $F(a) = F(a^2)$*.*

Exercice 8. — *Soient* α *et* β *deux nombres complexes vérifiant* $\alpha^3 = 2$ *et* $\beta^4 + 6\beta + 2 = 0$*. Déterminer le degré de* $\mathbb{Q}(\alpha, \beta)$ *sur* $\mathbb{Q}$*. L'élément* $\alpha + \beta$ *est-il algébrique sur* $\mathbb{Q}$ *?*

Exercice 9. — *Soit* $\mathrm{k}/\mathbb{Q}$ *une sous-extension de* $\mathbb{C}/\mathbb{Q}$ *contenue dans* $\mathbb{R}/\mathbb{Q}$ *(ou encore* $\mathrm{k} \subset \mathbb{R}$*). Déterminer* $[\mathrm{k}(i) : \mathbb{Q}]$*.*

Exercice 10. — *Déterminer* $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ *pour les nombres complexes suivants :* $\alpha = i + \sqrt{2}$*,* $\alpha = \sqrt[4]{5} + \sqrt{5}$*,* $\alpha = \sqrt{n + 2\sqrt{2}}$*, avec* $n \in \mathbb{N} - \{0\}$*.*

Exercice 11. — *Soit* α *une racine réelle de* $X^3 - 2$*. Montrer que les extensions* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *et* $\mathbb{Q}(j\alpha)/\mathbb{Q}$ *ne sont pas linéairement disjointes. Que vaut* $[\mathbb{Q}(\alpha, j\alpha) : \mathbb{Q}]$ *? Montrer que* $\mathbb{Q}(\alpha, j\alpha) = \mathbb{Q}(\alpha, j)$*.*

Exercice 12. — *Soient* K/k *une extension,* $t \in K$ *et* $n \in \mathbb{Z} - \{0\}$*. Montrer que* t *est transcendant sur* k *si et seulement si* t^n *l'est.*

Exercice 13. — *Soit* $\alpha = \sqrt[3]{2} + j\sqrt[3]{4}$.
1) Déterminer un polynôme $P \in \mathbb{Q}[X]$ *de degré* 6 *ayant pour racine* α.
2) Montrer que $j \in \mathbb{Q}(\alpha)$ *et* $\sqrt[3]{2} \in \mathbb{Q}(\alpha, j)$.
3) Montrer que $\mathbb{Q}(\alpha) = \mathbb{Q}(j, \sqrt[3]{2})$ *puis que* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.
4) En déduire que $P = \mathrm{Irr}(\alpha, \mathbb{Q})$.

Exercice 14. — *Soit* $k = \mathbb{Q}(\dfrac{X^4 - 1}{X})$ *le corps des fractions rationnelles en* $Y = (X^4 - 1)/X$.
Montrer que $\mathbb{Q}(X)$ *est une extension algébrique de* k, *puis déterminer* $[\mathbb{Q}(X) : \mathrm{k}]$.

Exercice 15 **(Le nombre de Liouville)**. —
1) Soit $P = a_n X^n + \cdots a_1 X + a_0 \in \mathbb{Z}[X]$, $a_n \neq 0$, *ayant* α *comme racine réelle de* P.

a) Soit $M = \max_i \left|\dfrac{a_i}{a_n}\right|$. *Montrer que* $|\alpha| \leq 1 + M$.

b) En déduire que pour $x \in \mathbb{R}$, *avec* $|x - \alpha| < 1$, *il existe une constante* κ *ne dépendant que des coefficients* a_i, *telle que* $|P'(x)| \leq \kappa$.
2) Soit $\alpha \in \mathbb{R}$, $\alpha \notin \mathbb{Q}$, α *racine de* P. *On suppose que* α *est de degré* n *sur* $\mathbb{Q}$. *En appliquant le théorème des accroissements finis, montrer que quelque soit le rationnel* p/q, $q > 0$, $p/q \in [\alpha - 1, \alpha + 1]$, *on a* $|\alpha - p/q| \geq \dfrac{1}{\kappa q^n}$.
3) Soit $\alpha = \displaystyle\sum_{k \geq 1} \frac{1}{10^{k!}}$.

a) Montrer que $\alpha \notin \mathbb{Q}$.

b) Soit $\alpha_k = \dfrac{1}{10} + \cdots + \dfrac{1}{10^{k!}}$. *Majorer* $|\alpha - \alpha_k|$. *En déduire que* α *est transcendant (sur* $\mathbb{Q}$*).*

1.6.2. Solutions. —

Exercice 1. Soit $P = X^n + a_{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. Supposons qu'il existe un nombre premier ℓ tel que $a_i \equiv 0 (\mathrm{mod}\ \ell)$, pour tout $i = 0, \cdots, n-1$ et tel que $a_0 \not\equiv 0 (\mathrm{mod}\ \ell^2)$. Alors P est irréductible dans $\mathbb{Q}[X]$.
Comme le contenu de P est trivial, l'irréductibilité de P sur $\mathbb{Q}$ équivaut à l'irréductibilité de P sur $\mathbb{Z}$. Supposons que $P = QR$, avec $Q, R \in \mathbb{Z}[X]$,

$\deg(Q) \geq 1$, $\deg(R) \geq 1$; $Q = X^r + b_{r-1}X^{r-1} + \cdots + b_0$; $R = X^s + c_{s-1}X^{s-1} + \cdots + c_0$. Comme ℓ divise $c_0 b_0$, le nombre premier ℓ divise par exemple c_0. Mais comme ℓ^2 ne divise pas $c_0 b_0$, alors ℓ ne divise pas b_0. Soit i_0 le plus grand entier tel que pour $i < i_0$, ℓ divise c_i. Alors i_0 est bien défini et $1 \leq i_0 \leq s$. Regardons alors le terme a_{i_0} :

$$a_{i_0} = \sum_{k=0}^{i_0} b_k c_{i_0-k} \equiv b_0 c_{i_0} \not\equiv 0 (\text{mod } \ell),$$

ce qui contredit l'hypothèse sur la divisibilité de a_{i_0} par ℓ.

Exercice 2.
Le polynôme $P = aX^3 + bX^2 + cX + d$ de degré 3 est irréductible sur $\mathbb{Q}$ si et seulement si P n'a pas de racine dans $\mathbb{Q}$. Cherchons la forme des racines de P dans $\mathbb{Q}$. Soit $\alpha = n/m \in \mathbb{Q}$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$, $(n, m) = 1$, une racine de P. Alors $m^3 P(n/m) = an^3 + bmn^2 + cm^2 n + dm^3 = 0$. Ainsi $n(an^2 + bnm + cm^2) = -dm^3$. Alors n divise dm^3, et comme $(m, n) = 1$, n divise d. De même, on a

$$m(bn^2 + cmn + dm^2) = -an^3,$$

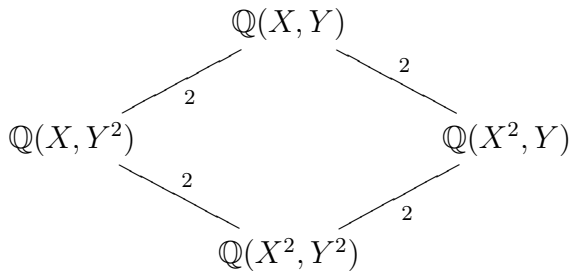
et ainsi m divise a

Exercice 3. L'élément $\sqrt{5}$ est racine de $X^2 - 5$ qui est irréductible sur $\mathbb{Q}$ (critère d'Eisenstein en $p = 5$). Ainsi $[\mathbb{Q}(\sqrt{5} : \mathbb{Q}] = \deg(X^2 - 5) = 2$.

Exercice 4.
Supposons que $[\mathbb{R} : \mathbb{Q}] = n$. Il existe une $\mathbb{Q}$-base $e_1, \cdots, e_n$ de $\mathbb{R}$. Or $\mathbb{Q}e_1 + \cdots + \mathbb{Q}e_n$ est dénombrable mais $\mathbb{R}$ ne l'est pas. Contradiction.

Exercice 5.
Nous savons déja que si L/k et K/k sont linéairement disjointes alors $\mathrm{K} \cap \mathrm{L} = \mathrm{k}$.
Réciproquement. Partons de $\mathrm{L} \cap \mathrm{K} = \mathrm{k}$. Raisonnons par l'absurde en supposant les extensions K/k et L/k non linérairement disjointes. Alors $[\mathrm{LK} : \mathrm{L}] < [\mathrm{K} : \mathrm{k}] = 2$ et ainsi $\mathrm{LK} = \mathrm{L}$, ou encore $\mathrm{K} \subset \mathrm{L}$. Par conséquent, $\mathrm{L} \cap \mathrm{K} = \mathrm{K} \neq \mathrm{k}$ car $[\mathrm{K} : \mathrm{k}] = 2$, ce qui aboutit à une contradiction.

Exercice 6.
Comparons les corps $\mathbb{Q}(X,Y)$ et $\mathbb{Q}(X,Y^2)$.
L'élément Y^2 se trouve dans le corps $\mathbb{Q}(X,Y)$, ainsi $\mathbb{Q}(X,Y) = \mathbb{Q}(X,Y^2,Y)$ est une extension de $\mathbb{Q}(X,Y^2)$. Soit P le polynôme dans $\mathbb{Q}(X,Y^2)[Z]$ défini par $P(Z) = Z^2 - Y^2$. Alors $P(Y) = 0$, ce qui signifie que $[\mathbb{Q}(X,Y^2,Y) : \mathbb{Q}(X,Y^2)] \leq 2$. Le corps $\mathbb{Q}(X,Y^2)$ est le corps des fractions rationnelles en X et Y^2, en particulier, $Y \notin \mathbb{Q}(X,Y^2)$. Ainsi $[\mathbb{Q}(X,Y) : \mathbb{Q}(X,Y^2)] = 2$ (et P est irréductible sur $\mathbb{Q}(X,Y)$).
Au total, on obtient le schéma d'extensions



Comme $X \notin \mathbb{Q}(X^2,Y)$, $\mathbb{Q}(X,Y^2) \cap \mathbb{Q}(X^2,Y)$ est un sous-corps strict de $\mathbb{Q}(X^2,Y)$, donc de degré sur $\mathbb{Q}(X^2,Y^2)$ strictement plus petit que 2 : ainsi $\mathbb{Q}(X,Y^2) \cap \mathbb{Q}(X^2,Y) = \mathbb{Q}(X^2,Y^2)$. Il y a disjonction linéaire entre $\mathbb{Q}(X,Y^2)/\mathbb{Q}(X^2,Y^2)$ et $\mathbb{Q}(X^2,Y)/\mathbb{Q}(X^2,Y^2)$, et $[\mathbb{Q}(X,Y) : \mathbb{Q}(X^2,Y^2)] = 4$.

Exercice 7.
On a la tour d'extensions

$$\mathrm{F} \text{ —— } \mathrm{F}(a^2) \text{ —— } \mathrm{F}(a) \ .$$

Ainsi $[\mathrm{F}(a) : \mathrm{F}(a^2)]|[\mathrm{F}(a) : \mathrm{F}]$. Mais a est racine de $P = X^2 - a^2 \in \mathrm{F}(a^2)[X]$, ce qui signifie que $[\mathrm{F}(a) : \mathrm{F}(a^2)] \leq 2$. Comme $[\mathrm{F}(a) : \mathrm{F}]$ est impair, on en déduit que $[\mathrm{F}(a) : \mathrm{F}(a^2)] = 1$, d'où le résultat.

Exercice 8.
Le nombre complexe α est racine de $P = X^3 - 2$ et β est racine de $Q = X^4 + 6X + 2$. Les polynômes P et Q sont irréductibles sur $\mathbb{Q}$ (critère d'Eisenstein en $p = 2$). Ainsi $[\mathbb{Q}(\alpha);\mathbb{Q}] = 3$ et $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Comme $(3,4) = 1$, les extensions $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$ sont linéairement disjointes sur

$\mathbb{Q}$ et ainsi le compositum $\mathbb{Q}(\alpha)\mathbb{Q}(\beta)$, qui coïncide avec $\mathbb{Q}(\alpha,\beta)$, est de degré 12 sur $\mathbb{Q}$.
L'élément $\alpha+\beta$ appartient à l'extension $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ qui est finie (donc algébrique) : l'élément $\alpha+\beta$ est algébrique sur $\mathbb{Q}$.

Exercice 9.
Comme $\mathrm{k}\subset\mathbb{R}$, $i\notin\mathrm{k}$. Ainsi $1<[\mathrm{k}(i):\mathrm{k}]\leq[\mathbb{Q}(i):\mathbb{Q}]=2$, et par conséquent $[\mathrm{k}(i):\mathrm{k}]=2$. Par transitivité du degré on obtient $[\mathrm{k}(i):\mathbb{Q}]=2[\mathrm{k}:\mathbb{Q}]$.

Exercice 10.
• $\alpha=i+\sqrt{2}$. L'élément α se trouve dans le corps $\mathbb{Q}(i,\sqrt{2})$ Comme $\mathbb{Q}(\sqrt{2})\subset\mathbb{R}$, d'après l'exercice 9, $[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}]=4$. Ainsi $[\mathbb{Q}(\alpha):\mathbb{Q}]|4$. De $(\alpha-i)^2=2$, il vient $\alpha^2-2i\alpha-1=2$ puis $\alpha^2-3=-2i\alpha$ et ainsi $i=\dfrac{-\alpha^2+3}{2\alpha}\in\mathbb{Q}(\alpha)$. De $\alpha=i+\sqrt{2}$, on en déduit ensuite que $\sqrt{2}\in\mathbb{Q}(\alpha)$ et donc au total que $\mathbb{Q}(\alpha)=\mathbb{Q}(i,\sqrt{2})$. L'élément α est de degré 4 sur $\mathbb{Q}$.

• $\alpha=\sqrt[4]{5}+\sqrt{5}$. Comme $\sqrt[4]{5}^2=\sqrt{5}$, $\alpha\in\mathbb{Q}(\sqrt[4]{5})$. L'élément $\sqrt[4]{5}$ est de degré 4 sur $\mathbb{Q}$. Ensuite $(\alpha-\sqrt{5})^2=\alpha^2-2\alpha\sqrt{5}+5=\sqrt{5}$. On en déduit (noter que $1+2\alpha>0$ et est donc non nul) : $\sqrt{5}=\dfrac{\alpha^2+5}{1+2\alpha}$ et ainsi $\mathbb{Q}(\sqrt{5})\subset\mathbb{Q}(\alpha)$. On a la tour d'extensions

$$\mathbb{Q}\overset{2}{\longrightarrow}\mathbb{Q}(\sqrt{5})\longrightarrow\mathbb{Q}(\alpha)\longrightarrow\mathbb{Q}(\sqrt[4]{5})\ .$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{4}$$

Donc $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{5})]=1$ ou 2. Mais si ce degré vaut 1, alors $\alpha\in\mathbb{Q}(\sqrt{5})$, puis $\sqrt[4]{5}=\alpha-\sqrt{5}\in\mathbb{Q}(\sqrt{5})$, ce qui est en contradiction avec $[\mathbb{Q}(\sqrt[4]{5}:\mathbb{Q}]=4$.

• $\alpha=\sqrt{n+2\sqrt{2}}$. On élève au carré : $\alpha^2=n+2\sqrt{2}$. Ainsi on obtient deux informations : $\sqrt{2}=\dfrac{\alpha^2-n}{2}\in\mathbb{Q}(\alpha)$ et $\alpha^4-2n\alpha^2+n^2-8=0$. Au total, on obtient la tour d'extensions

$$\mathbb{Q}\overset{2}{\longrightarrow}\mathbb{Q}(\sqrt{2})\longrightarrow\mathbb{Q}(\alpha)$$

avec $[\mathbb{Q}(\alpha):\mathbb{Q}] \leq 4$. Ainsi $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})]$ est égal à 1 ou à 2. Supposons que $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha)$. Alors $\alpha \in \mathbb{Q}(\sqrt{2})$. Comme $(1, \sqrt{2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$, il existe $a, b \in \mathbb{Q}$ tels que $\alpha = a + b\sqrt{2}$. On élève au carré pour obtenir $n + 2\sqrt{2} = a^2 + 2b^2 + 2ab\sqrt{2}$. Comme $(1, \sqrt{2})$ est une $\mathbb{Q}$-base, on en déduit : $a^2 + 2b^2 = n$ et $ab = 1$. Il vient alors l'équation $a^4 - 3a^2 + 2 = 0$, c'est-à-dire a est racine de $P = X^4 - nX^2 + 2$. En notant que les seules racines possibles de P dans $\mathbb{Q}$ sont ± 1 et ± 2, on calcule : $P(1) = P(-1) = 3 - n$ et $P(2) = P(-2) = 18 - 4n$. On voit donc que si $n \neq 3$, alors on aboutit à une contradiction c'est-à-dire $\alpha \notin \mathbb{Q}(\sqrt{2})$ et donc $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$. À noter que dans ce cas, $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^4 - 2nX^2 + n^2 - 8$.
Pour $n = 3$, on obtient $\alpha^2 = (1 + \sqrt{2})^2$ et ainsi $\alpha = 1 + \sqrt{2}$, d'où $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2$.

Exercice 11.
La famille $(1, \alpha, \alpha^2)$ est $\mathbb{Q}$-libre.
Maintenant partons de la relation $1 + j + j^2 = 0$: Alors

$$\begin{aligned} 0 &= 1 + j + j^2 \\ &= \alpha^3(1 + j + j^2) \\ &= 2 + (j\alpha)\alpha^2 + (j\alpha)^2\alpha \end{aligned}$$

Ceci montre que la famille $(1, \alpha, \alpha^2)$ est liée sur $\mathbb{Q}(j\alpha)$.
On note ensuite que $j = j\alpha/\alpha \in \mathbb{Q}(j, j\alpha)$. Comme $\mathbb{Q}(\alpha)$ est réel et $j \notin \mathbb{R}$, il vient $[\mathbb{Q}(j\alpha, \alpha):\mathbb{Q}(\alpha)] > 1$. Mais d'un autre coté, comme les extensions $\mathbb{Q}(j\alpha)/\mathbb{Q}$ et $\mathbb{Q}(\alpha)/\mathbb{Q}$ ne sont pas linéairement disjointes, $[\mathbb{Q}(j\alpha, \alpha):\mathbb{Q}(\alpha)] < [\mathbb{Q}(\alpha):\mathbb{Q}] = 3$, d'où au total $[\mathbb{Q}(j\alpha, \alpha):\mathbb{Q}(\alpha)] = 2$ puis $\mathbb{Q}(\alpha, j\alpha):\mathbb{Q}] = 2 * 3 = 6$
Au passage, on a vu que $j \in \mathbb{Q}(\alpha, j\alpha)$, $\mathbb{Q}(j, \alpha) \subset \mathbb{Q}(\alpha, j\alpha)$ et ainsi $\mathbb{Q}(j, \alpha) \subset \mathbb{Q}(\alpha, j\alpha) \subset \mathbb{Q}(j, \alpha)$ d'où l'égalité souhaitée.

Exercice 12.
Soit le corps $\mathrm{F} = \mathrm{k}(t^n)$. Pour $n > 0$, l'élément t est racine du polynôme $P(X) = X^n - t^n \in \mathrm{F}[X]$. Pour $n < 0$, l'élément t^{-1} est racine du polynôme $P(X) = X^{-n} - t^n \in \mathrm{F}[X]$. Comme $\mathrm{F}(t) = \mathrm{F}(1/t)$, il vient au total

$[\mathrm{k}(t) : \mathrm{k}(t^n)] \leq n$ et la tour d'extensions

$$\mathrm{k} \text{ —— } \mathrm{k}(t^n) \text{ —— } \mathrm{k}(t)$$

Supposons t algébrique sur k. Alors l'extension $\mathrm{k}(t)/\mathrm{k}$ est algébrique et ainsi t^n est algébrique sur k.
Réciproquement. Supposons t^n algébrique sur k. Les extensions $\mathrm{k}(t^n)/\mathrm{k}$ et $\mathrm{k}(t)/\mathrm{k}(t^n)$ étant algébriques, par transitivité de l'algébricité, on en déduit que $\mathrm{k}(t)/\mathrm{k}$ est algébrique.

Exercice 13.
1) On a $\alpha = \sqrt[3]{2}(1+j\sqrt[3]{2})$ et ainsi $\alpha^3 = 6(1+j\sqrt[3]{2}+j^2\sqrt[3]{4}) = 6(1+j\alpha)$. Par conséquent, $\alpha^3 - 6j\alpha - 6 = 0$. Comme $2j = -1+\sqrt{-3}$ on a $\alpha^3+3\alpha-6 = 3\alpha\sqrt{-3}$. On élève au carré pour obtenir la relation de degré 6 sur $\mathbb{Q}$:

$$\alpha^6 + 6\alpha^4 - 12\alpha^3 + 36\alpha^2 - 36\alpha + 36 = 0.$$

2) De la relation $\alpha^3 = 6(1 + j\alpha)$, on en déduit que $j \in \mathbb{Q}(\alpha)$.
On élève ensuite au carré la relation $\alpha = \sqrt[3]{2}(1 + j\sqrt[3]{2})$, pour obtenir $\alpha^2 = \sqrt[3]{4} + 4j + 2j\sqrt[3]{2}$ puis $\sqrt[3]{4} = \alpha^2 - 4j - 2j^2\sqrt[3]{2}$. On reporte alors dans la relation initiale définissant α : $\sqrt[3]{2} = -\alpha + j\alpha^2 - 4j^2 \in \mathbb{Q}(\alpha, j)$.
3) La définition de α montre que $\alpha \in \mathbb{Q}(j, \sqrt[3]{2})$ et ainsi $\mathbb{Q}(\alpha) \subset \mathbb{Q}(j, \sqrt[3]{2})$. D'après la question 2), $j, \sqrt[3]{2} \in \mathbb{Q}(\alpha, j) = \mathbb{Q}(\alpha)$, car $j \in \mathbb{Q}(\alpha)$.
Au total, on trouve $\mathbb{Q}(\alpha) = \mathbb{Q}(j, \sqrt[3]{2})$.
4) On a $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ et $[\mathbb{Q}(j) : \mathbb{Q}] = 2$. Comme 2 et 3 sont premiers entre eux, les extensions $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(j)/\mathbb{Q}$ sont linéairement disjointes et ainsi $[\mathbb{Q}(j, \sqrt[3]{2}) : \mathbb{Q}] = 6$.
L'élément α est donc de degré 6 sur $\mathbb{Q}$, par conséquent $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^6 + 6X^4 - 12X^3 + 36X^2 - 36X + 36$.

Exercice 14.
Soit $Y = (X^4-1)/X$. Alors $X^4 - XY - 1 = 0$, ce qui signifie que l'élément X est racine de $P(Z) = Z^4 - YZ - 1 \in \mathrm{k}[Z]$. Ainsi, X est algébrique sur k et $[\mathrm{k}(X) : \mathrm{k}] \leq 4$.
Nous allons montrer que P est irréductible sur k.
Notons que $\mathrm{k} = \mathbb{Q}(Y)$ est le corps des fractions de l'anneau principal $\mathbb{Q}[Y]$. Le polynôme P est à coefficients dans $\mathbb{Q}[Y]$ (de contenu 1), il suffit alors de montrer l'irréductibilité de P sur $\mathbb{Q}[Y]$.

Soit ensuite le morphisme d'évaluation φ de $\mathbb{Q}[Y,Z]$ vers $\mathbb{Q}[Z]$ obtenu en posant $Y=1$; $\varphi : a_n(Y)Z^n+\cdots+a_1(Y)Z+a_0(Y) \mapsto a_n(1)Z^n+\cdots+a_0(1)$. C'est un morphisme d'anneaux de noyau $(Y-1)$. Nous allons montrer que le polynôme $\varphi(P)=Z^4-Z-1$ est irréductible dans $\mathbb{Q}[Z]$ (il suffit de montrer qu'il l'est sur $\mathbb{Z}$). Tout d'abord $\varphi(P)$ n'a pas de racine dans $\mathbb{Q}$ (les seules possibles étant ± 1). Ensuite supposons que $\varphi(P)=(aZ^2+bZ+c)(a'Z^2+b'Z+c')$ dans $\mathbb{Z}[Z]$, $a>0$. Alors, par identification, il vient les équations : $aa'=1, cc'=-1, ab'+a'b=0, a'c+ac'+bb'=0, bc'+b'c=1$. Ainsi les trois premières équations donnent : $a=a'=1$, $b=-b'$, $c=-c'=\pm 1$. On reporte dans la 4ème équation pour obtenir $bb'=0$ d'où $b=b'=0$. En comparant avec la dernière équation, on aboutit à une contradiction.
Supposons que $P=RS$, $R,S \in \mathbb{Q}[Y,Z]$. Alors $\varphi(P)=\varphi(R)\varphi(S)$ est irréductible dans $\mathbb{Q}[Z]$. Ainsi, par exemple, $\varphi(R)=\alpha \in \mathbb{Q}^\times$, c'est-à-dire $R-\alpha \in \ker(\varphi)$: il existe $Q_0 \in \mathbb{Q}[Y,Z]$ tel que $R-\alpha=(Y-1)Q_0$. Comme $R|P$, $\deg_Y(R) \leq 1$. On a donc $\deg_Y(R)=1$ si et seulement si $Q_0 \neq 0$.
Montrons que Q_0 est forcément nul. En effet sinon, $0 \neq Q_0 \in \mathbb{Q}[Z]$ et également $S \in \mathbb{Q}[Z]$. Dans ce cas, il vient $Z^4-YZ-1=(Y-1)Q_0S+S$, d'où par identification (dans l'anneau $\mathbb{Q}[Z,Y]$) : $Q_0S=-Z$ et $S(1-Q_0)=Z^4-1$. Ainsi, la seconde relation indique que $S \in \mathbb{Q}^\times$. Mais alors, $\varphi(SR)=\varphi(S)\varphi(R) \in \mathbb{Q}$, ce qui est absurde.
Donc $Q_0=0$ et $R=\alpha$.
En conclusion, nous avons montré que $P=RS$ implique que R ou S est dans $\mathbb{Q}^\times$, d'où l'irréductibilité de P sur k. Ainsi $P=\mathrm{Irr}(X,\mathrm{k})$ et $[\mathrm{k}(X):\mathrm{k}]=4$.

Exercice 15.

1) a) On peut supposer $|\alpha| > 1$ (sinon, c'est immédiat !). Partons de la relation $\alpha^n = \sum_{i=0}^{n-1} \frac{a_i}{a_n}\alpha^i$. Alors

$$\begin{aligned} |\alpha|^n &\leq M\sum_{i=0}^{n-1}|\alpha|^i \\ &= M\frac{1-|\alpha|^n}{1-|\alpha|} \\ &\leq M\frac{|\alpha|^n}{|\alpha|-1} \end{aligned}$$

On simplifie par $|\alpha|^n$ pour obtenir $1 \leq \frac{M}{|\alpha|-1}$, d'où le résultat.
b) De $|x-\alpha| < 1$, il vient $|x| < 1 + |\alpha| \leq M + 2$. Alors $|P'(x)| = |na_n x^{n-1} + \cdots a_1| \leq n|a_n|M^{n-1} + \cdots + |a_1| = \kappa$.
2) Commençons par la remarque suivante. Comme α est de degré n sur $\mathbb{Q}$, $P = a_n \mathrm{Irr}(\alpha, \mathbb{Q})$ et $n > 1$ (car $\alpha \notin \mathbb{Q}$). Ainsi $P(p/q) \neq 0$. Par conséquent $a_n p^n + a_{n_1} p^{n-1}q + \cdots + a_1 pq^{n-1} + q^n$ est un entier non nul et $|a_n p^n + a_{n_1} P^{n-1}q + \cdots + a_1 pq^{n-1} + q^n| \geq 1$.
On applique ensuite le théorème des accroissement finis entre α et p/q pour obtenir $|P(p/q)| = |P(\alpha) - P(p/q)| = |P'(c)||\alpha - p/q| \leq \kappa|\alpha - p/q|$, avec $c \in]\alpha - p/q, \alpha + p/q[$.
On multiplie ensuite le tout par q^n, pour obtenir $\kappa q^n|\alpha - p/q| \geq q^n P(p/q) \geq 1$, d'aprés la remarque précédente. Ainsi, $|\alpha - p/q| \geq 1/(\kappa q^n)$.
3) a) À noter que α est bien défini (la série converge dans $\mathbb{R}$). On rappelle qu'un nombre réel est rationnel si et seulement si, son développement décimal est périodique à partir d'un certain rang. Ce qui n'est pas le cas pour α.
b) $|\alpha - \alpha_k| \leq \frac{1}{10^{(k+1)!}}\left(1 + \frac{1}{10} + \frac{1}{100} + \cdots\right) \leq \frac{2}{10^{(k+1)!}}$.
Supposons alors α algébrique sur $\mathbb{Q}$. L'élément α n'est pas dans $\mathbb{Q}$ et écrivons $\alpha_k = p_k/q_k$, avec $q_k = 10^{k!}$. Soit alors $P = \mathrm{Irr}(\alpha, \mathbb{Q})$ et $n = \deg(P)$. On applique les résultats des questions précédentes. Il existe κ, ne dépendant que de P tel que pour k ≥ 1, $|\alpha - \alpha_k| \geq \frac{1}{\kappa 10^{nk!}}$. On obtient

ainsi, pour tout entier $k \geq 1$

$$\frac{2}{10^{(k+1)!}} \geq \frac{1}{\kappa 10^{nk!}},$$

d'où une contradiction.

CHAPITRE 2

CLÔTURE ALGÉBRIQUE D'UN CORPS

L'objectif de ce chapitre est de définir rigoureusement la notion de clôture algébrique d'un corps k puis de montrer qu'une fois celle-ci fixée, le problème de l'étude des extensions algébriques de k est alors figé.

2.1. Racine d'un polynôme

Définition 2.1.1. — Soit K/k une extension et $P \in \mathrm{k}[X]$. Un élément $\alpha \in \mathrm{K}$ est racine de P (dans K) si $P(\alpha) = 0$.

Remarque 2.1.2. — Si α est racine de $P \in \mathrm{k}[X]$ dans K, alors α est algébrique sur k et $\mathrm{Irr}(\alpha, \mathrm{k})$ divise P dans $\mathrm{k}[X]$.

Définition 2.1.3. — Soit une extension K/k et soit $P \in \mathrm{k}[X]$, P non nul. Alors le corps K est dit de rupture pour P, s'il existe une racine α de P dans K telle que $\mathrm{K} = \mathrm{k}(\alpha)$.
Le corps K est dit corps de décomposition pour P si dans $\mathrm{K}[X]$, le polynôme P se factorise en produit de polynômes de degré 1 :

$$P = a_n X^n + \cdots + a_1 X + a_0 = a_n \prod_{i=1}^{n} (X - \alpha_i),$$

avec $\alpha_i \in \mathrm{K}$.

Remarque 2.1.4. — Soit K un corps de décomposition de P. Alors P a au plus $n = \deg(P)$ racines dans K.

Définition 2.1.5. — Soit K/k une extension et soit $P \in \mathrm{k}[X]$ (non constant). Le corps K est dit corps des racines de P si K est corps de décomposition pour P et est minimal pour cette propriété : $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$, avec $\alpha_i \in \mathrm{K}$ et $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$.

Remarque 2.1.6. — Étant donné un corps de décomposition L d'un polynôme $P \in \mathrm{k}[X]$, il existe une unique sous-extension K/k de L/k pour laquelle K est un corps des racines de P : si $P = a_n \prod_{i=1}^{n}(X-\alpha_i) \in \mathrm{L}[X]$, $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$. Se pose alors la question de l'existence et de l'unicité du corps de racines d'un polynôme P.

Exemple 2.1.7. — Soit l'extension $\mathbb{C}/\mathbb{Q}$.
Le corps des racines sur $\mathbb{Q}$ de $X^2 + 1$ est le corps $\mathbb{Q}(i)$.
Le corps $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture du polynôme $P = X^3-2$. Vérifier que le corps des racines sur $\mathbb{Q}$ de $X^3 - 2$ est le corps $\mathbb{Q}(\sqrt[3]{2}, j)$, j étant une racine primitive cubique de 1.

Proposition 2.1.8. — *Si le corps* K *est corps des racines du polynôme* $P \in \mathrm{k}[X]$, *alors* $[\mathrm{K} : \mathrm{k}] \leq n!$, *où* $n = \deg(P)$.

Démonstration. — Notons $\alpha_1, \cdots, \alpha_n$ les racines de P dans K. Pour simplifier supposons P unitaire. Remarquons que $\mathrm{Irr}(\alpha_1, \mathrm{k})|P$ et donc $[\mathrm{k}(\alpha_1) : \mathrm{k}] \leq n$. Il vient ensuite $P = (X - \alpha_1)Q$, avec $Q \in \mathrm{k}(\alpha_1)[X]$. L'élément α_2 est racine de Q, ainsi $\mathrm{Irr}(\alpha_2, \mathrm{k}(\alpha_1))|Q$ et par conséquent $[\mathrm{k}(\alpha_1, \alpha_2) : \mathrm{k}(\alpha_1)] \leq d - 1$. On continue le processus pour aboutir à

$$[\mathrm{k}(\alpha_1, \cdots, \alpha_n) : \mathrm{k}] = [\mathrm{k}(\alpha_1, \cdots, \alpha_n) : \mathrm{k}(\alpha_1, \cdots, \alpha_{n-1})] \cdots [\mathrm{k}(\alpha_1) : \mathrm{k}] \leq d!.$$

□

2.2. Théorèmes d'existence

Nous commençons par montrer le théorème fondamental suivant :

Théorème 2.2.1. — *Soit* k *un corps et soit* $P \in \mathrm{k}[X]$, *non constant. Alors il existe un corps de rupture* K *pour* P.

Démonstration. — Soit $P = X^n + a_{n-1}X^{n-1} \cdots + a_1X + a_0$, $a_i \in \mathrm{k}$. Il faut donc construire une extension K/k contenant une racine α de P. Il suffit de montrer ce résultat pour un facteur irréductible de P.

Pour la suite, on suppose donc que P est irréductible dans $\mathrm{k}[X]$. L'idéal $P\mathrm{k}[X]$ est maximal, le quotient $\mathrm{k}[X]/(P)$ est un corps, notons-le K'.
Soit l'homomorphisme de réduction $\varphi : \mathrm{k}[X] \to \mathrm{k}[X]/(P)$. Notons $\mathrm{k}' = \varphi(\mathrm{k})$. Il est immédiat que $\varphi_{|\mathrm{k}}$ est injectif et ainsi $\mathrm{k} \overset{\varphi}{\simeq} \mathrm{k}'$. Par conséquent K'/k' est une extension de corps.
Soit le polynôme

$$\overline{P} := Y^n + \varphi(a_{n-1})Y^{n-1} + \cdots + \varphi(a_0) \in \mathrm{k}'[Y].$$

Alors $\overline{P}(\varphi(X)) = \varphi(P(X)) = 0$: le corps K' contient une racine de $\overline{P}$. Il faut maintenant revenir à k. On va effectuer un transport de structure.
Soit $S = \mathrm{K}' - \mathrm{k}'$, et considérons le réunion disjointe $\mathrm{K} = \mathrm{k} \cup S$.
On définit alors l'application f par

$$\begin{array}{rcl} f : \mathrm{K} & \to & \mathrm{K}' \\ x & \mapsto & \left\{ \begin{array}{lll} x & \text{si} & x \in S \\ \varphi(x) & \text{si} & x \in \mathrm{k} \end{array} \right. \end{array}$$

L'application f est clairement bijective, notons f^{-1} son application réciproque.
Cette application f nous permet de munir K de deux lois $+$ et $\cdot$. Pour $x, y \in \mathrm{K}$, on pose

$$x + y = f^{-1}(f(x) + f(y)),$$
$$x \cdot y = f^{-1}(f(x)f(y)).$$

Alors il est facile de voir que $(\mathrm{K}, +, \cdot)$ est un corps puis que f est un isomorphisme de corps. L'homomorphisme f restreint à k est un isomorphisme de corps et les deux lois définies précédemment sur K coïncident sur k avec celles de k. En clair, K/k est un extension de corps. Enfin, notons que $\varphi(X) \in S$. Posons alors $\alpha = f^{-1}(\varphi(X))$. Alors

$$\begin{array}{rcl} P(\alpha) & = & P(f^{-1}(\varphi(X))) \\ & = & (f^{-1}(\varphi(X)))^n + a_{n-1}(f^{-1}(\varphi(X)))^{n-1} + \cdots + a_0 \\ & = & f^{-1}\left(\varphi(X)^n + \varphi(a_{n-1})\varphi(X)^{n-1} + \cdots + \varphi(a_1)\varphi(X) + \varphi(a_0)\right) \\ & = & f^{-1}\left(\overline{P}(\varphi(X))\right) \\ & = & f^{-1}(0) \\ & = & 0. \end{array}$$

Ainsi α est une racine de P dans K : le corps $\mathrm{k}(\alpha)$ est un corps de rupture pour P. □

Corollaire 2.2.2. — *Soit* $P \in \mathrm{k}[X]$ *non nul. Alors le polynôme* P *admet un corps de décomposition.*

Démonstration. — C'est immédiat, par induction. □

Corollaire 2.2.3. — *Si* K *et* K′ *sont deux corps de rupture sur* k *de* $P \in \mathrm{k}[X]$, *alors* $\mathrm{K} \simeq \mathrm{k}[X]/(P) \simeq \mathrm{K}'$.

Démonstration. — C'est immédiat en considérant l'homomorphisme d'évaluation en $X = \alpha : \mathrm{k}[X] \to \mathrm{k}(\alpha)$, où α est une racine de P. □

Définition 2.2.4. — Un corps K est dit algébriquement clos si tout polynôme non constant $P \in \mathrm{K}[X]$ admet une racine dans K.

Si K est un corps algébriquement clos, alors tout polynôme P non constant de $\mathrm{K}[X]$ se factorise, dans $\mathrm{K}[X]$, en produit de polynômes de degré 1. Ou encore, tout élément algébrique sur K se trouve dans K.
Se pose alors la question de l'existence de tels corps....

Théorème 2.2.5. — *Soit* k *un corps. Alors* k *possède une extension algébriquement close (il existe une extension* K/k, *avec* K *algébriquement clos).*

En fait, nous allons être plus précis en montrant le

Théorème 2.2.6. — *Soit* k *un corps. Il existe une extension algébrique* $\overline{\mathrm{k}}$ *de* k *qui est algébriquement close.*

Démonstration. — Commençons par la remarque suivante. Soient $P_1, \cdots, P_r \in \mathrm{k}[X]$ des polynomes non constants. On peut trouver un corps K scindant chaque polynôme P_i : il suffit de prendre un corps des racines de $P_1 \cdots P_r$.
La preuve du théorème va reposer sur le lemme suivant :

Lemme 2.2.7. — *Il existe une extension algébrique* K/k *telle que tout polynôme non constant* $P \in \mathrm{k}[X]$ *est scindé dans* K.

Démonstration. — À chaque polynôme $P \in \mathrm{k}[X]$ unitaire (non constant) de degré d, on associe d indeterminées $X_{P,1}, \cdots, X_{P,d}$, puis l'on considère

l'algèbre polynomiale $\mathrm{k}[(X_{P,i})_{P,i}]$. Soit alors l'idéal $\mathcal{I}$ de $\mathrm{k}[(X_{P,i})_{P,i}]$ engendré par les coefficients des polynômes

$$S(P) := P(X) - (X - X_{P,1}) \cdots (X - X_{P,d}),$$

$P \in \mathrm{k}[X]$ non constant.
L'élément 1 n'est pas dans $\mathcal{I}$: sinon, il existe $Q_1 \cdots, Q_r \in \mathrm{k}[(X_{P,i})]$ et $P_j \in \mathrm{k}[X]$ tels que

$$Q_1 a(P_1) + \cdots + Q_r a(P_r) = 1,$$

où $a(P_i)$ est un coefficient de $S(P_i)$. Notons que cette égalité ne fait intervenir qu'un nombre fini d'interminées et que l'on peut la voir dans toute extension K/k.
Soit alors K/k un corps scindant les polynômes $P_1, \cdots, P_r$. Dans K, notons $\alpha_{i,j}$ les racines de P_i.
Posons alors pour $i = 1, \cdots, r$, et $j = 1, \cdots, \deg(P_i)$, $X_{P_i,j} = \alpha_{i,j}$ puis, par exemple, 0 pour les autres variables.
En cette spécialisation, le polynôme $S(P_i)$ est le polynôme nul, ce qui signifie que les coefficients $a(P_i)$, après spécialisation, sont nuls.
On évalue alors l'identité initiale en la précédente spécialisation pour aboutir à la contradiction $0 = 1$.
Soit alors $\mathfrak{M}$ un idéal maximal contenant $\mathcal{I}$ (ceci a un sens car $\mathcal{I} \neq (1)$) et soit K′ le quotient $\mathrm{k}[(X_{P,i})_{P,i}]/\mathfrak{M}$: c'est un corps. Soit $\varphi : \mathrm{k}[(X_{P,i})_{P,i}] \to \mathrm{k}[(X_{P,i})_{P,i}]/\mathfrak{M}$. Alors $\varphi_{|\mathrm{k}}$ est injectif et induit un isomorphisme de corps entre k et $\mathrm{k}' := \varphi(\mathrm{k})$.
Pour finir, soit $P = \sum_i a_i X^i \in \mathrm{k}[X]$ unitaire (non constant). Posons $\overline{P} = \sum_i \varphi(a_i) Y^i \in \mathrm{k}'[Y]$. Alors, comme les coefficients de $S(P)$ sont nuls dans K′, l'image de $S(P)$ dans $\mathrm{K}'[X]$ est nulle, c'est-à-dire :

$$\overline{P} = (Y - \varphi(X_{P,1})) \cdots (Y - \varphi(X_{P,d})),$$

et ainsi $\overline{P}$ est scindé sur K′.
On applique ensuite la même opération que celle utilisée dans la preuve du théorème 2.2.1 : on effectue un transport de structure pour obtenir l'existence d'une extension K/k qui scinde tout polynôme de k.
Au passage, on note que K′ est engendré sur k′ par les éléments $\varphi(X_{P,i})$ qui sont algébriques sur k′. Ainsi, l'extension K′/k′ est algébrique et il en est de même pour K/k. □

La fin de la preuve du théorème 2.2.6 est alors immédiate. Soit K/k une extension algébrique satisfaisant les conditions du lemme 2.2.7. Montrons que K/k est une extension algébriquement close.
Soit $P \in \mathrm{K}[X]$ un polynôme irréductible. Alors P admet une racine α dans L, où L/K est une extension qui contient une racine de chaque polynôme de $\mathrm{K}[X]$ (cf. la construction précédente). L'élément α est algébrique sur K donc sur k (car K/k est algébrique). Soit $R = \mathrm{Irr}(\alpha, \mathrm{k})$. Alors R est scindé sur $\mathrm{K} \subset \mathrm{L}$ et ainsi $\alpha \in \mathrm{K}$. □

Définition 2.2.8. — Soit k un corps. Le corps $\overline{\mathrm{k}}$ s'appelle une clôture algébrique pour (de) k.

Proposition 2.2.9. — *Soit* K/k *une extension algébrique. Alors le corps* $\overline{\mathrm{k}}$ *est une clôture algébrique pour* k *si et seulement si* $\overline{\mathrm{k}}$ *est une clôture algébrique pour* K.

Démonstration. — Cela provient de la transitivité de l'algébricité. □

2.3. Prolongement des isomorphismes

Définition 2.3.1. — Soient k un corps, L/k une extension algébriquement close et L′ un corps algébriquement clos. Soit K/k une extension algébrique contenue dans L/K. Soit σ un homomorphisme de corps de k vers L′ et $\overline{\sigma}$ un homomorphisme de K vers L′. On dit que $\overline{\sigma}$ prolonge σ si $\overline{\sigma}_{|\mathrm{k}} = \sigma$.

$$\begin{array}{ccc} \mathrm{L} & & \mathrm{L}' \\ | & & | \\ \mathrm{K} & \xrightarrow[\simeq]{\overline{\sigma}} & \overline{\sigma}(\mathrm{K}) \\ | & & | \\ \mathrm{k} & \xrightarrow[\simeq]{\sigma} & \sigma(\mathrm{k}) \end{array}$$

Théorème 2.3.2. — *Soient* k *un corps,* L/k *une extension algébriquement close et* L′ *un corps algébriquement clos. Soit* σ *un isomorphisme de* k *vers un sous-corps* k′ *de* L′. *Soit* $P \in \mathrm{k}[X]$ *un polynôme irréductible sur* k. *Soit* α *une racine de* P *dans* L *et soit* $\mathrm{K} = \mathrm{k}(\alpha)$. *Alors l'ensemble des homomorphismes* $\overline{\sigma}$ *de* K *dans* L′ *qui prolongent* σ *est en bijection*

avec l'ensemble des racines distinctes de $P' = \sigma(P)$ dans L'*. La correspondance est donnée par :* $\overline{\sigma}(\alpha) = \alpha'$*, où* α' *est une racine de* P' *dans* L'*.*

Démonstration. — • Construisons l'homomorphisme de corps $\overline{\sigma}$ qui va vérifier : $\overline{\sigma}(\alpha) = \alpha'$ et $\overline{\sigma}_{|\mathrm{k}} = \sigma$.
Par abus, notons encore σ :

$$\begin{array}{rcl} \sigma : \mathrm{k}[X] & \to & \mathrm{k}'[X] \\ a_i X^i & \mapsto & \sigma(a_i) X^i \end{array}$$

l'isomorphisme d'anneaux prolongeant l'isomorphisme entre k et k′ puis, toujours par abus, par passage au quotient :

$$\sigma : \mathrm{k}[X]/(P) \to \mathrm{k}'[X]/(P').$$

L'homomorphisme d'anneaux σ est là aussi un isomorphisme, et en particulier P' est irréductible sur k′. Notons ensuite que par évaluation en α et α', il vient $\mathrm{k}[X]/(P) \simeq \mathrm{k}(\alpha)$ et $\mathrm{k}'[X]/(P') \simeq \mathrm{k}'(\alpha')$ car $\mathrm{Irr}(\alpha, \mathrm{k}) = P$ et $\mathrm{Irr}(\alpha', \mathrm{k}') = P'$. Donc au total, on obtient un isomorphisme $\overline{\sigma} : \mathrm{k}(\alpha) \xrightarrow{\simeq} \mathrm{k}'(\alpha')$. Il faut simplement s'assurer que l'isomorphisme entre ces corps prolonge bien σ et envoie α sur α' :

$$\mathrm{k}(\alpha) \xrightarrow{\simeq} \mathrm{k}[X]/(P) \xrightarrow{\sigma} \mathrm{k}'[X]/(P') \xrightarrow{\simeq} \mathrm{k}'(\alpha')$$
$$\mathrm{k}(\alpha) \xrightarrow[\overline{\sigma}]{} \mathrm{k}'(\alpha')$$

Il est clair que pour $a \in \mathrm{k}$, $\overline{\sigma}(a) = \sigma(a)$. Ensuite $\overline{\sigma}(\alpha)$ a pour image l'évaluation en α' de X .... d'où le résultat.
• Il reste à déterminer tous les prolongements $\overline{\sigma}$ de σ. C'est assez immédiat. Soit $\alpha' = \overline{\sigma}(\alpha)$. Alors

$$\begin{array}{rcl} P'(\alpha') & = & \sigma(P)(\overline{\sigma}(\alpha)) \\ & = & \overline{\sigma}(P(\alpha)) \\ & = & 0. \end{array}$$

Ainsi α' est une racine de P'. Pour conclure, il suffit de noter que $\overline{\sigma}(\alpha)$ caractérise $\overline{\sigma}$. □

Remarque 2.3.3. — Il y a au plus n prolongements $\overline{\sigma}$, où $n = \deg(P) = \deg(P')$. En particulier, si K/k une sous-extension de degré finie de $\overline{\mathrm{k}}$/k, alors tout plongement σ de k dans $\overline{\mathrm{k}}$ admet au plus n prolongements (en

effet, il suffit d'écrire $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_m)$, puis d'itérer l'observation du début de la remarque).

Remarque 2.3.4. — Il se pose alors la question suivante. Soit $P \in \mathrm{k}[X]$ irréductible. Combien le polynôme P a-t'il de racines dans $\overline{\mathrm{k}}$? Il y en a au plus $n = \deg(P)$, mais cela peut-être moins.

Exemple 2.3.5. — Notons $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps à 2 élément et soit $\mathrm{k} = \mathbb{F}_2(X)$ le corps des fractions rationnelles sur $\mathbb{F}_2$. Considérons $P = Y^2 - X \in \mathrm{k}[Y]$. Alors P est irréductible dans $\mathrm{k}[Y]$ (critère d'Eisenstein appliqué à X dans l'anneau factoriel $\mathrm{k}[X, Y]$). Soit α une racine de P dans une clôture algébrique $\overline{\mathrm{k}}$ de k. Alors $\alpha^2 = X$ et $P = (Y - \alpha)^2$. L'élément α est donc racine double ! Ainsi, si l'on prend σ l'homorphisme identité, il n'existe qu'un seul homomorphisme de corps de $\mathrm{k}(\alpha)$ dans $\overline{\mathrm{k}}$ prolongeant σ : l'identité.

Définition 2.3.6. — Soit $\overline{\mathrm{k}}$ une clôture algébrique de k. Si $P \in \mathrm{k}[X]$ est irréductible et si α est une racine de P dans $\overline{\mathrm{k}}$, alors toute racine β de P dans $\overline{\mathrm{k}}$ s'appelle un k-conjugué de α.

Remarque 2.3.7. — L'élément β est un k-conjugué de α si et seulement si β est une racine de $\mathrm{Irr}(\alpha, \mathrm{k})$ dans $\overline{\mathrm{k}}$.

Théorème 2.3.8. — *Soient* k *un corps,* L/k *une extension algébriquement close et* L′ *un corps algébriquement clos. Soit* σ *un isomorphisme de* k *sur un sous-corps* k′ *de* L′*. Soit* K/k *une extension algébrique. Alors il existe un homomorphisme* $\overline{\sigma}$ *de* K *dans* L′ *qui prolonge* σ*.*

Démonstration. — On veut montrer que le schéma suivant existe :

$$\begin{array}{ccc} \mathrm{L} & & \mathrm{L}' \\ | & & | \\ \mathrm{K} & \xrightarrow[\simeq]{\overline{\sigma}} & \mathrm{K}' \\ | & & | \\ \mathrm{k} & \xrightarrow[\simeq]{\sigma} & \mathrm{k}' \end{array}$$

La preuve est purement algébrique. Soit $\mathcal{F}$ l'ensemble des couples $(\mathrm{F}, \overline{\sigma})$, où F/k est une sous-extension de K/k et $\overline{\sigma}$ un prolongement de σ à F en

un isomorphisme de F sur une sous-extension F′ de L′/k. L'ensemble $\mathcal{F}$ est ordonné de la manière suivante (issu de l'inclusion) :

$$(\mathrm{F}_1, \sigma_1) \leq (\mathrm{F}_2, \sigma_2)$$

si et seulement si

$$\mathrm{F}_1 \subset F_2 \quad \text{et} \quad \sigma_{2|\mathrm{F}_1} = \sigma_1.$$

L'ensemble $\mathcal{F}$ est non-vide (il contient le couple (k, σ)).
Montrons ensuite que toute chaîne d'élément $(\mathrm{F}_i, \overline{\sigma}_i)_{i\in I}$ de $\mathcal{F}$ (i.e. partie de $\mathcal{F}$ totalement ordonnée) admet un élément maximal. Soit $\mathrm{E} = \cup_i \mathrm{F}_i$. Alors E/k est une extension de corps. Pour $x \in \mathrm{F}_i$, posons $\overline{\sigma}_{\mathrm{E}}(x) := \overline{\sigma}_i$: cette définition ne dépend pas du choix de $i \in I$. Alors $\overline{\sigma}_{\mathrm{E}}$ est un homomorphisme de corps de K vers L′ prolongeant σ. Ainsi $(\mathrm{E}, \overline{\sigma}_{\mathrm{E}})$ est un majorant.
On peut appliquer le lemme de Zorn. La famille $\mathcal{F}$ admet un élément maximal $(\mathrm{F}, \overline{\sigma})$. Il nous suffit de montrer que F = K. Supposons qu'il existe $\alpha \in \mathrm{K}$ ne se trouvant pas dans F. L'élément α est algébrique sur k. Par le théorème 2.3.2, on en déduit l'existence d'un homomorphisme τ de $\mathrm{F}(\alpha)$ dans L′ prolongeant $\overline{\sigma}$. L'homomorphisme τ prolonge alors aussi σ et ainsi $(\mathrm{F}(\alpha), \tau) \in \mathcal{F}$, avec $(\mathrm{F}(\alpha), \tau) > (\mathrm{F}, \overline{\sigma})$, ce qui contredit la maximalité de $(\mathrm{F}, \overline{\sigma})$. □

Remarque 2.3.9. — Quand $\overline{\mathrm{k}}$ est dénombrable (par exemple quand $\mathrm{k} = \mathbb{Q}$, $\mathrm{k} = \mathbb{Z}/p\mathbb{Z}$, $\mathrm{k} = \mathbb{Q}(T)$, ...), on peut procéder d'une façon plus directe. Notons $(\alpha_i)_{i\in\mathbb{N}}$ les éléments de $\overline{\mathrm{k}}$ et soit $\mathrm{K}_i = \mathrm{k}(\alpha_1, \cdots, \alpha_i)$. On vérifie facilement que

$$\overline{\mathrm{k}} = \bigcup_i \mathrm{K}_i.$$

Pour K_0, posons $\sigma_0 = \sigma$. D'après le théorème 2.3.2, tout isomorphisme σ_i de K_i vers un sous-corps de $\overline{\mathrm{k}}$ se prolonge en un morphisme σ_{i+1} de K_{i+1} vers $\overline{\mathrm{k}}$. Définissons alors τ sur $\overline{\mathrm{k}}$ par : pour $x \in \mathrm{K}_i$, $\tau(x) = \sigma_i(x)$. L'isomorphisme τ est bien défini et prolonge σ. La restriction $\overline{\sigma}$ de τ à K donne le prolongement de σ recherché.

On en arrive à la notion de k-isomorphisme.

Définition 2.3.10. — Soit K/k et K′/k deux extensions de corps. On dit que $\sigma : \mathrm{K} \to \mathrm{K}'$ est un k-isomorphisme si σ est un isomorphisme de

corps dont la restriction à k est l'identité (ou encore σ prolonge l'identité). On parle aussi de k-plongements de K dans $\overline{\mathrm{k}}$. Quand k est un sous-corps premier ($\mathrm{k} = \mathbb{F}_p$ ou $\mathrm{k} = \mathbb{Q}$), on parle de plongements de K dans $\overline{\mathrm{k}}$.
Enfin, lorsque $\mathrm{K} = \mathrm{K}'$, on parle alors de k-automorphisme.

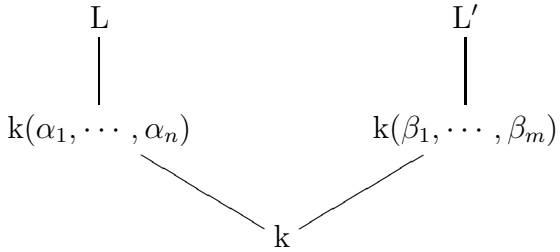
Remarque 2.3.11. — Les extensions K/k et K′/k sont k-isomorphes via σ si et seulement si, σ est un isomorphisme de corps, et σ est un isomorphisme de k-espaces vectoriels entre K et K′.

Corollaire 2.3.12. — *Soit* L/k *une extension algébriquement close de* k. *Soient* K_1 *et* K_2 *deux clôtures algébriques de* k *dans* L. *Alors il existe un* k*-isomorphisme de* K_1 *vers* K_2.

Démonstration. — On applique le théorème 2.3.8 avec $\sigma = \mathrm{id}$, l'identité, $\mathrm{K} = \mathrm{K}_1$ et $\mathrm{L}' = \mathrm{K}_2$. Il existe un k-isomorphisme $\overline{\sigma}$ de K_1 vers $\overline{\sigma}(\mathrm{K}_1) \subset \mathrm{K}_2$. Comme $\overline{\sigma}$ est un isomorphisme, il est facile de voir que $\overline{\sigma}(\mathrm{K}_1)$ est algébriquement clos. D'autre part $\mathrm{K}_2/\overline{\sigma}(\mathrm{K}_1)$ est algébrique. Ainsi $\overline{\sigma}(\mathrm{K}_1) = \mathrm{K}_2$. □

Corollaire 2.3.13. — *Soit* P *un polynôme de* $\mathrm{k}[X]$ *et soient* K *et* K′ *deux corps de racines pour* P *(dans deux extensions algébriquement closes* L *et* L′*). Alors il existe un* k*-isomorphisme de* K *vers* K′.

Démonstration. — Soient $\{\alpha_1, \cdots, \alpha_n\}$ (respectivement $\{\beta_1, \cdots, \beta_m\}$) les racines de P dans K (respectivement dans K′). Alors $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$ et $\mathrm{K}' = \mathrm{k}(\beta_1, \cdots, \beta_m)$. On a le schéma d'extensions suivant :



D'après le théorème 2.3.8, il existe donc un k-isomorphisme de corps $\overline{\sigma}$ de L vers $\overline{\sigma}(\mathrm{L}) \subset \mathrm{L}'$. Or $\overline{\sigma}(P) = P$. Ainsi, $\overline{\sigma}(\{\alpha_1, \cdots, \alpha_n\}) = \overline{\sigma}(\{\beta_1, \cdots \beta_m\})$, ce qui montre que $n = m$ et, quitte à revoir la numérotation, $\overline{\sigma}(\alpha_i) = \beta_i$. □

Remarque 2.3.14. — Dans la pratique, on se fixe toujours une clôture algébrique $\overline{\mathrm{k}}$ de k. Soit alors par exemple un polynôme $P \in \mathrm{k}[X]$ unitaire et non constant. Dans $\overline{\mathrm{k}}$, P s'écrit $P = (X - \alpha_1) \cdots (X - \alpha_n)$ et alors **le** corps des racines de P s'ecrit $\mathrm{k}(\alpha_1, \cdots, \alpha_n)$.

2.4. Exercices

2.4.1. Énoncés. —

Exercice 16. — *1) Donner un exemple d'un corps fini.*
2) Montrer qu'un corps fini n'est pas algébriquement clos.

Exercice 17. — *Dans cet exercice, prenons* $\mathbb{C}$ *comme corps de décomposition. Déterminer le corps des racines* k *sur* $\mathbb{Q}$ *des polynômes suivants :* $P = X^4 - 1$ *;* $P = X^3 - 2$. *Déterminer dans chaque cas* $[\mathrm{k} : \mathbb{Q}]$.

Exercice 18. — *Soit la tour d'extension*

$$\mathbb{Q} \text{ —— } \mathbb{Q}(\sqrt{2}) \text{ —— } \mathbb{Q}(\sqrt[4]{2}) \text{ —— } \mathbb{C}$$

1) Montrer qu'il existe deux $\mathbb{Q}$*-isomorphismes* σ_0 *et* σ_1 *de* $\mathbb{Q}(\sqrt{2})$ *dans* $\mathbb{C}$.
2) a) Déterminer tous les isomorphismes de $\mathbb{Q}(\sqrt[4]{2})$ *dans* $\mathbb{C}$ *prolongeant* σ_0.
b) Déterminer tous les isomorphismes de $\mathbb{Q}(\sqrt[4]{2})$ *dans* $\mathbb{C}$ *prolongeant* σ_1.
c) En déduire tous les $\mathbb{Q}$*-isomorphismes de* $\mathbb{Q}(\sqrt[4]{2})$ *dans* $\mathbb{C}$.
3) Parmi les $\mathbb{Q}$*-isomorphismes de* $\mathbb{Q}(\sqrt[4]{2})$ *dans* $\mathbb{C}$*, lesquels sont des* $\mathbb{Q}$*-automorphismes ?*

Exercice 19. — *Soit* $a \in \mathbb{C}$ *une racine de* $X^6 + X^3 + 1$. *Déterminer tous les* $\mathbb{Q}$*-plongements de* $\mathbb{Q}(a)$ *dans* $\mathbb{C}$. *(Noter que* a *est racine de* $X^9 - 1$*). Parmi ces* $\mathbb{Q}$*-plongements, déterminer les* $\mathbb{Q}$*-automorphismes de* $\mathbb{Q}(a)$ *puis reconnaître le groupe des* $\mathbb{Q}$*-automorphismes de* $\mathbb{Q}(a)$.

2.4.2. Solutions. — *Exercice 16.*

1) Soit p un nombre premier. Alors $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps fini.
2) Soient $\mathrm{k} = \{\alpha_1, \cdots, \alpha_n\}$ un corps fini. Alors le polynôme $P = (X - \alpha_1) \cdots (X - \alpha_n) + 1 \in \mathrm{k}[X]$ et pour tout i, $P(\alpha_i) = 1 \neq 0$. Ainsi k n'est pas algébriquement clos.

Exercice 17.
(i) $P = X^4 - 1 = (X^2 - 1)(X^2 + 1)$. Le corps des racines de P est le corps $\mathbb{Q}(i)$ et $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
(ii) $P = (X^3 - 2)$. Les racines de P dans $\mathbb{C}$ sont $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$.
Soit k le corps des racines de P. Alors, $\sqrt[3]{2}$ et j sont dans k, par conséquent, $\mathbb{Q}(j, \sqrt[3]{2}) \subset$ k. On peut ensuite noter que les trois racines de P s'expriment en fonction de j et de $\sqrt[3]{2}$, et ainsi, k $\subset \mathbb{Q}(j, \sqrt[3]{2})$ d'où k $= \mathbb{Q}(j, \sqrt[3]{2})$ et $[\text{k}; \mathbb{Q}] = 6$ (voir aussi l'exercice 11).

Exercice 18.
1) D'après le théorème 2.3.2, les isomorphismses de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{C}$ qui prolongement l'identité sur $\mathbb{Q}$ sont en correspondance avec les $\mathbb{Q}$-conjugués de $\sqrt{2}$, ou encore les racines de $\text{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$. On a ainsi deux $\mathbb{Q}$-isomorphismes : $\sigma_0 : \sqrt{2} \mapsto \sqrt{2}$ et $\sigma_1 : \sqrt{2} \mapsto -\sqrt{2}$.
2) Remarquons tout d'abord que $\text{Irr}(\sqrt[4]{2}, \mathbb{Q}) = X^4 - 2$ et ainsi $\sqrt[4]{2}$ est de degré 2 sur $\mathbb{Q}(\sqrt{2})$. Alors $P = \text{Irr}(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})) = X^2 - \sqrt{2}$.
a) Les isomorphismes de $\mathbb{Q}(\sqrt[4]{2})$ dans $\mathbb{C}$ prolongeant σ_0 sont en correspondance avec les racines de $\sigma_0(P) = X^2 - \sqrt{2}$. On a alors deux prolongements : $\sigma_{0,0} = \sqrt[4]{2} \mapsto \sqrt[4]{2}$ et $\sigma_{0,1} = \sqrt[4]{2} \mapsto -\sqrt[4]{2}$.
b) Les isomorphismes de $\mathbb{Q}(\sqrt[4]{2})$ dans $\mathbb{C}$ prolongeant σ_1 sont en correspondance avec les racines de $\sigma_1(P) = X^2 + \sqrt{2}$. On a alors deux prolongements : $\sigma_{1,0} = \sqrt[4]{2} \mapsto i\sqrt[4]{2}$ et $\sigma_{1,1} = \sqrt[4]{2} \mapsto -i\sqrt[4]{2}$.
c) Soit σ un $\mathbb{Q}$-isomorphisme de $\mathbb{Q}(\sqrt[4]{2})$ dans $\mathbb{C}$. Alors, $\tau := \sigma_{|\mathbb{Q}(\sqrt{2})}$ est un $\mathbb{Q}$-plongement de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{C}$ et par conséquent $\tau = \sigma_0$ ou $\tau = \sigma_1$. Comme σ prolonge τ, on obtient au total $\sigma \in \{\sigma_{i,j}, i = 0, 1,\ j = 0, 1\}$.
3) Clairement $\sigma_{0,0}(\sqrt[4]{2}) \in \mathbb{Q}(\sqrt[4]{2})$ et $\sigma_{0,1}(\sqrt[4]{2}) \in \mathbb{Q}(\sqrt[4]{2})$ et ainsi $\sigma_{0,0}$ et $\sigma_{0,1}$ sont des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\sqrt[4]{2})$. Par contre, comme $i\sqrt[4]{2} \notin \mathbb{R}$, $\sigma_{1,0}(\sqrt[4]{2}) \notin \mathbb{Q}(\sqrt[4]{2})$ et $\sigma_{0,1}(\sqrt[4]{2}) \notin \mathbb{Q}(\sqrt[4]{2})$, les éléments $\sigma_{1,0}$ et $\sigma_{1,1}$ ne sont pas des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\sqrt[4]{2})$.

Exercice 19.
La division euclidienne de $X^9 - 1$ par $(X - 1)(X^6 + X^3 + 1)$ permet de montrer que $X^9 - 1 = (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1)$.

Montrons que le polynôme $P = X^6 + X^3 + 1$ est irréductible sur $\mathbb{Q}$. Calculons : $P(X+1) = X^6 + 3X(...) + 3$. Le critère d'Eisenstein (en $p = 3$) montre que $P(X+1)$ est irréductible sur $\mathbb{Q}$, il en est de même pour P. Ainsi l'élément a est de degré 6 sur $\mathbb{Q}$.
Soit $z = \exp(2i\pi/9)$. Alors $X^9 - 1$ a pour racines z^i, $i = 0, \cdots, 8$. Les racines de $X^2 + X + 1$ sont j et j^2 c'est-à-dire les racines de l'unité d'ordre 3 : z^3 et z^6. Ainsi les racines de P sont : $z, z^2, z^4, z^5, z^7, z^8$ et a est un de ces éléments. On peut ensuite noter que $\{z, z^2, z^4, z^5, z^7, z^8\} = \{a, a^2, a^4, a^5, a^7, a^8\}$.
Les $\mathbb{Q}$-plongements de $\mathbb{Q}(a)$ dans $\mathbb{C}$ sont en correspondance avec les $\mathbb{Q}$-conjugués de a, c'est-à-dire avec les racines de $P = \mathrm{Irr}(a, \mathbb{Q})$. On obtient 6 $\mathbb{Q}$-isomorphismes : $\sigma_1 : a \mapsto a$, $\sigma_2 : a \mapsto a^2$, $\sigma_4 : a \mapsto a^4$, $\sigma_5 : a \mapsto a^5$, $\sigma_7 : a \mapsto a^7$, $\sigma_8 : a \mapsto a^8$.
Comme $\sigma_i(a) \in \mathbb{Q}(a)$, ces 6 éléments sont des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(a)$.

Pour finir un petit calcul : $\sigma_2^k : a \mapsto a^{2^k}$. On voit alors que σ_2 est d'ordre 6. Le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(a)$ est un groupe d'ordre 6 engendré par σ_2. Ce groupe est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

CHAPITRE 3

GROUPE DES AUTOMORPHISMES D'UNE EXTENSION FINIE

3.1. Rappels

Définition 3.1.1. — Soit K/k une extension finie. Un automorphisme de l'extension K/k est un k-automorphisme de K, c'est-à-dire un isomorphisme de K sur lui-même dont la restriction à k est l'identité.

Remarque 3.1.2. — Si k est le sous-corps premier de K ($k = \mathbb{Q}$ ou $k = \mathbb{F}_p$), alors tout automorphisme de K est un k-automorphisme de K : cela provient tout simplement du fait que pour un automorphisme σ de K, $\sigma(1) = 1$.

Remarque 3.1.3. — L'ensemble des automorphismes de K/k contient toujours au moins un élément (l'identité). Cet ensemble muni de la composition forme un groupe. Ce groupe est un invariant fondamental de K/k. Son étude permet de déterminer les sous-extensions ainsi que les extensions relatives de K/k : c'est la théorie de Galois (à venir).

Remarque 3.1.4. — Les k-automorphismes de $k(\alpha)$ sont caractérisés par l'image de α.

Comme conséquence immédiate du théorème 2.3.2, nous avons :

Théorème 3.1.5. — *Soit* $k(\alpha)/k$ *une extension algébrique. Le nombre de* k*-automorphismes de* $k(\alpha)$ *est égal au nombre de racines de* $\mathrm{Irr}(\alpha, k)$ *contenues dans* $k(\alpha)$.

Démonstration. — Suivant les notations du théorème 2.3.2, il suffit de prendre une clôture algébrique $\overline{\mathrm{k}}$ de k contenant $\mathrm{k}(\alpha)$, puis $\overline{\mathrm{k}} = \mathrm{L} = \mathrm{L}'$ et $\sigma = \mathrm{id}$. □

Exemple 3.1.6. — (i) L'extension de degré 2, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, a deux automorphismes : $\sigma_0 : \sqrt{2} \mapsto \sqrt{2}$ et $\sigma_0 : \sqrt{2} \mapsto -\sqrt{2}$.
(ii) L'extension de degré 3, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, n'a qu'un seul automorphisme. En effet, les racines de $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q})$ sont $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. Comme $\mathbb{Q}(\sqrt[3]{2})$ est réel, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ ne sont pas $\mathbb{Q}(\sqrt[3]{2})$.
(iii) Soit le corps $\mathrm{K} = \mathbb{Q}(j, \sqrt[3]{2})$. L'extension $\mathrm{K}/\mathbb{Q}$ est de degré 6. Il vient la tour d'extensions

$$\mathbb{Q} \text{ —— } \mathbb{Q}(j) = \mathrm{k} \text{ —— } \mathrm{K} = \mathrm{k}(\sqrt[3]{2}\,) = \mathbb{Q}(j, \sqrt[3]{2})$$

avec $\mathrm{Irr}(\sqrt[3]{2}, \mathrm{k}) = X^3 - 2$. L'extension $\mathrm{k}/\mathbb{Q}$ a deux automorphismes $\sigma_0 : j \mapsto j$ et $\sigma_1 : j \mapsto j^2$. Maintenant $\sigma_0(X^3 - 2) = \sigma_1(X^3 - 2) = X^3 - 2$. Cela signifie que σ_0 et σ_1 se prolongent sur K en trois isomorphismes déterminés par : $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2} \mapsto j\sqrt[3]{2}$ et $\sqrt[3]{2} \mapsto j^2\sqrt[3]{2}$. Au total, les six k-isomorphismes τ de K vérifient $\tau(\mathrm{K}) \subset \mathrm{K}$, ce sont donc des automorphismes de $\mathrm{K}/\mathbb{Q}$. Le groupe des automorphismes de $\mathrm{K}/\mathbb{Q}$ est un groupe à 6 éléments.... isomorphe à S_3 (à venir).

3.2. Extensions algébriques normales

Théorème 3.2.1. — *Soit* K/k *une extension finie contenue dans une clôture algébrique* $\overline{\mathrm{k}}/\mathrm{k}$. *Alors les conditions suivantes sont équivalentes :*

(i) Tout k*-isomorphisme de* K *sur un sous-corps de* $\overline{\mathrm{k}}$ *est un* k*-automorphisme de* K.

(ii) K *est corps des racines sur* k *d'un polynôme* $P \in \mathrm{k}[X]$;

(iii) Tout polynôme irréductible de $\mathrm{k}[X]$, *qui a une racine dans* K, *admet un corps des racines contenu dans* K.

Démonstration. — $(i) \implies (iii)$. Soit $\alpha \in \mathrm{K}/\mathrm{k}$ et soit $\beta \in \overline{\mathrm{k}}$ un k-conjugué de α (ou encore β une racine de $\mathrm{Irr}(\alpha, \mathrm{k})$). Soit σ le k-isomorphisme de $\mathrm{k}(\alpha)$ dans $\overline{\mathrm{k}}$ défini par $\sigma(\alpha) = \beta$. D'après le théorème fondamental du prolongement des isomorphismes 2.3.8, σ se prolonge en un k-isomorphisme $\overline{\sigma}$ de K dans $\overline{\mathrm{k}}$. Comme par hypothèse $\overline{\sigma}$ est un

k-automophisme, $\overline{\sigma}(\mathrm{K}) = \mathrm{K}$ et ainsi $\beta \in \mathrm{K}$. Nous venons de montrer que si $\alpha \in \mathrm{K}$, alors tous les k-conjugués de α sont dans K ce qui prouve (iii).
$(iii) \Longrightarrow (ii)$. Comme K/k est finie, il existe $\alpha_1, \cdots, \alpha_n \in \mathrm{K}$ tels que $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$. En effet, si $\mathrm{K} \neq \mathrm{k}$, il existe $\alpha_1 \in \mathrm{K} - \mathrm{k}$. Alors on a la tour d'extensions

$$\mathrm{k} \text{ —— } \mathrm{k}(\alpha_1) \text{ —— } \mathrm{K}$$

avec $[\mathrm{k}(\alpha_1) : \mathrm{k}] > 1$. Par conséquent $[\mathrm{K} : \mathrm{k}(\alpha_1)] < [\mathrm{K} : \mathrm{k}]$. On continue le processus pour arriver à $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$.
Soit $P_i = \mathrm{Irr}(\alpha_i, \mathrm{k})$. Les éléments α_i sont dans K, donc tous les k-conjugués des α_i sont aussi dans K. Le corps K est alors le corps des racines du polynôme $P_1 \cdots P_n$.
$(ii) \Longrightarrow (i)$. Soit P tel que K soit corps des racines de P dans $\overline{\mathrm{k}}$. Soit σ un k-isomorphisme de K dans $\overline{\mathrm{k}}$. Si α est racine de P dans K, alors $\sigma(\alpha)$ est aussi une racine de P dans $\overline{\mathrm{k}}$ et est dans K. Comme K est engendré sur k par les racines de P, on a bien $\sigma(\mathrm{K}) \subset \mathrm{K}$ d'où $\sigma(\mathrm{K}) = \mathrm{K}$ car $[\sigma(\mathrm{K}) : \mathrm{k}] = [\mathrm{K} : \mathrm{k}]$. □

Définition 3.2.2. — Une extension K/k qui vérifie les points $(i)-(ii)-(iii)$ du théorème 3.2.1 est dite normale.

Remarque 3.2.3. — Les extensions normales K/k sont les corps de racines de polynômes sur k.

Corollaire 3.2.4. — *Fixons une clôture algébrique* $\overline{\mathrm{k}}$ *de* k. *Toute sous-extension finie* K/k *de* $\overline{\mathrm{k}}$/k *est contenue dans une extension finie normale* N/k.

Démonstration. — C'est immédiat. Comme K/k est finie, $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$, $\alpha_i \in \mathrm{K}$. Soit $P_i = \mathrm{Irr}(\alpha_i, \mathrm{k})$, puis $P = P_1 \cdots P_n$. Alors le corps des racines N de P dans $\overline{\mathrm{k}}$ donne une extension normale sur k (point (ii) du théorème 3.2.1) et N contient $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$. □

Corollaire 3.2.5. — *Soit* K/k *une extension (finie) normale et soit* k′/k *une sous-extension de* K/k. *Alors* K/k′ *est normale*

Démonstration. — C'est immédiat. D'après le théorème 3.2.1, K est le corps des racines d'un certain polynôme $P \in \mathrm{k}[X]$. Il suffit de voir le polynôme P dans $\mathrm{k}'[X]$. □

Corollaire 3.2.6. — *Soient* K/k *et* K'/k *deux sous-extensions. Si* K/k *est (finie) normale, l'extension* KK'/K' *est également normale.*

Démonstration. — Par hypothèse, $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$, où les éléments α_i sont les racines d'un polynôme $P \in \mathrm{k}[X]$. Il suffit alors de noter que $\mathrm{K}'\mathrm{K} = \mathrm{K}'\mathrm{k}(\alpha_1, \cdots, \alpha_n) = \mathrm{K}'(\alpha_1, \cdots, \alpha_n)$, puis de voir P dans $\mathrm{K}'[X]$. □

Corollaire 3.2.7. — *Soient* K/k *et* K'/k *deux sous-extensions finies et normales de* $\overline{\mathrm{k}}/\mathrm{k}$. *Alors* $\mathrm{K}'\mathrm{K}/\mathrm{k}$ *est normale.*

Démonstration. — On a $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$, où les éléments α_i sont les racines d'un polynôme $P \in \mathrm{k}[X]$, et $\mathrm{K}' = \mathrm{k}(\beta_1, \cdots, \alpha_m)$, où les éléments β_i sont les racines d'un polynôme $P' \in \mathrm{k}[X]$. Il suffit alors de noter que $\mathrm{K}'\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m)$, puis que les éléments α_i et β_j sont les racines du polynôme $PP' \in \mathrm{k}[X]$. □

3.3. Extensions algébriques séparables

Dans cette section, on aborde l'aspect dénombrement des racines d'un polynôme irréductible.

Définition 3.3.1. — Soit $P \in \mathrm{k}[X]$, P non nul. On dit que le polynôme P est séparable s'il admet des racines distinctes dans une clôture algébrique $\overline{\mathrm{k}}$.

Remarque 3.3.2. — Si $\deg(P) = n$, P est séparable si et seulement si, dans $\overline{\mathrm{k}}$, P admet n racines distinctes (ou encore les racines de P sont simples).

Remarque 3.3.3. — D'après le corollaire 2.3.13, la notion de séparabilité ne dépend pas du choix de $\overline{\mathrm{k}}$.

Définition 3.3.4. — Soit K/k une extension algébrique. Alors $\alpha \in \mathrm{K}$ est dit séparable si $\mathrm{Irr}(\alpha, \mathrm{k})$ est séparable.
L'extension algébrique K/k est dite séparable si tout élément α de K est séparable.

Exemple 3.3.5. — Soit le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et soit $\mathrm{k} = \mathbb{F}_p(X)$. Considérons le polynôme $P = Y^p - X \in \mathrm{k}[Y]$. Le corps k est le corps des fractions de l'anneau principal $\mathbb{F}_p[X]$. Grâce au critère d'Eisenstein

appliqué avec l'idéal premier (X), P est irréductible. Si α désigne une racine de P dans $\overline{\mathrm{k}}$, alors $P = (Y-\alpha)^p$, ce qui montre que P n'admet qu'une seule racine dans $\overline{\mathrm{k}}$. L'extension $\mathrm{k}(\alpha)/\mathrm{k}$, de degré p, n'est pas séparable.

Proposition 3.3.6. — *Soit* K/k *une extension (algébrique) séparable et soit* k'/k *une sous-extension de* K/k. *Alors les extensions* K/k' *et* k'/k *sont séparables.*

Démonstration. — Les extensions K/k' et k'/k sont algébriques et l'extension k'/k est bien séparable (c'est trivial !).
Soit $\alpha \in \mathrm{K}$ et soit $P = \mathrm{Irr}(\alpha, \mathrm{k}')$. Alors le polynôme P divise, dans k', le polynôme $\mathrm{Irr}(\alpha, \mathrm{k})$. Par unicité de la factorisation dans $\overline{\mathrm{k}}[X]$, on en déduit que les racines de P dans $\overline{\mathrm{k}}$ sont simples. □

Proposition 3.3.7. — *Soit* A *une partie de* $\overline{\mathrm{k}}$ *constituée d'éléments séparables sur* k. *Alors l'extension* $\mathrm{k}(A)/\mathrm{k}$ *est séparable.*

Démonstration. — On peut noter que l'extension $\mathrm{k}(A)/\mathrm{k}$ est bien algébrique. Soit $\alpha \in \mathrm{k}(A)/\mathrm{k}$. Comme $\mathrm{k}(A) = \bigcup_{\substack{B \subset A \\ B \text{ fini}}} \mathrm{k}(B)$, il existe $B = \{\beta_1, \cdots, \beta_n\} \subset A$ tels que $\alpha \in \mathrm{k}(B) = \mathrm{k}(\beta_1, \cdots, \beta_n)$.

Lemme 3.3.8. — *Soient* $\beta_1, \cdots, \beta_n \in \overline{\mathrm{k}}$ *des éléments algébriques sur* k. *Alors le nombre de* k*-isomorphismes de* $\mathrm{k}(\beta_1, \cdots, \beta_n)$ *dans* $\overline{\mathrm{k}}$ *est égal à* $[\mathrm{k}(\beta_1, \cdots, \beta_n) : \mathrm{k}]$ *si et seulement si tous les éléments* β_i *sont séparables sur* k.

Démonstration. — On a la tour d'extensions

$$\mathrm{k} \text{ —— } \mathrm{k}(\beta_1) \text{ —— } \cdots \text{ —— } \mathrm{k}(\beta_1, \cdots, \beta_i)(\beta_{i+1}) \text{ —— } \cdots \text{ —— } \mathrm{k}(B) \ ,$$

où $B = \{\beta_1, \cdots, \beta_n\}$.
D'après le théorème du prolongement des isomorphismes (théorème 2.3.8), le prolongement de chaque isomorphisme σ de $\mathrm{k}(\beta_1, \cdots, \beta_i)$ dans $\overline{\mathrm{k}}$ dans l'extension $\mathrm{k}(\beta_1, \cdots, \beta_i)(\beta_{i+1})/\mathrm{k}(\beta_1, \cdots, \beta_i)$ est en correspondance avec le nombre de racines de $\sigma(P_{i+1})$, où $P_{i+1} = \mathrm{Irr}(\beta_{i+1}, \mathrm{k}(\beta_1, \cdots, \beta_i))$.
• Supposons β_1 non séparable sur k. Alors le nombre de k-isomorphismes de $\mathrm{k}(\beta_1)$ dans $\overline{\mathrm{k}}$ est strictement plus petit que $[\mathrm{k}(\beta_1) : \mathrm{k}]$. Ainsi, le nombre

de k-isomorphismes de $\mathrm{k}(B)$ vers $\overline{\mathrm{k}}$ sera strictement plus petit que $[\mathrm{k}(B) : \mathrm{k}]$.
• Réciproquement, supposons les éléments β_i séparables sur k. Il faut maintenant se rappeler que $\sigma_{|\mathrm{k}} = \mathrm{id}$ et ainsi, comme $P_{i+1}|\mathrm{Irr}(\beta_{i+1}, \mathrm{k})$ (dans $\overline{\mathrm{k}}[X]$ par exemple), il vient $\sigma(P_{i+1})|\mathrm{Irr}(\beta_{i+1}, \mathrm{k})$. Les racines de $\mathrm{Irr}(\beta_{i+1}, \mathrm{k})$ dans $\overline{\mathrm{k}}$ étant simples, on a donc $[\mathrm{k}(\beta_1, \cdots, \beta_i, \beta_{i+1}) : \mathrm{k}(\beta_1, \cdots, \beta_i)]$ isomorphismes de $\mathrm{k}(\beta_1, \cdots, \beta_i, \beta_{i+1})$ dans $\overline{\mathrm{k}}$ prolongeant σ. Au total, il vient bien $[\mathrm{k}(B) : \mathrm{k}]$ k-isomorphismes de $\mathrm{k}(B)$ dans $\overline{\mathrm{k}}$. □

Finissons la preuve de la proposition 3.3.7. Soit donc $\alpha \in \mathrm{k}(B)$. Supposons que α n'est pas séparable sur k. Alors le nombre d de k-isomorphismes de $\mathrm{k}(\alpha)$ dans $\overline{\mathrm{k}}$ est strictement plus petit que $[\mathrm{k}(\alpha) : \mathrm{k}]$. Chaque isomorphisme σ de $\mathrm{k}(\alpha)$ dans $\overline{\mathrm{k}}$ a exactement d' prolongements à $\mathrm{k}(B)$, avec $d' \leq [\mathrm{k}(B) : \mathrm{k}(\alpha)]$ (voir la remarque 2.3.3), c'est-à-dire au total $dd' < [\mathrm{k}(B) : \mathrm{k}]$. Mais comme les éléments de B sont séparables, d'après le lemme 3.3.8, ce nombre de prolongements doit être $[\mathrm{k}(B) : \mathrm{k}]$, d'où une contradiction. □

Corollaire 3.3.9. — *Une extension finie* K/k *est séparable si et seulement si il y a* $[\mathrm{K} : \mathrm{k}]$ k*-isomorphismes de* K *dans* $\overline{\mathrm{K}}$.

Démonstration. — C'est immédiat à partir du lemme 3.3.8 et de la proposition 3.3.7. □

Corollaire 3.3.10. — *Soit* K/k *une extension séparable et soit* K'/k *une extension quelconque. Alors* KK'/K' *est séparable.*

Démonstration. — On a $\mathrm{K} = \mathrm{k}(\mathrm{K})$ avec K ne contenant que des éléments séparables sur k. Les éléments de K sont aussi algébriques et séparables sur K' (pour $\alpha \in \mathrm{K}$, $\mathrm{Irr}(\alpha, \mathrm{K}')$ divise $\mathrm{Irr}(\alpha, \mathrm{k})$ dans $\mathrm{K}'[X]$). Comme $\mathrm{K}'\mathrm{K} = \mathrm{K}'(\mathrm{K})$, on conclut avec la proposition 3.3.7. □

Proposition 3.3.11. — *Dans* $\overline{\mathrm{k}}/\mathrm{k}$*, si les extensions* L/K *et* K/k *sont séparables, alors* L/k *est séparable.*

Démonstration. — Soit $\alpha \in \mathrm{L}$ et soit $\mathrm{Irr}(\alpha, \mathrm{K}) = X^n + \cdots + a_1 X + a_0 \in \mathrm{K}[X]$. Soit $\mathrm{k}' = \mathrm{k}(a_1, \cdots, a_n)$. Les éléments a_i étant séparables sur k, d'après la proposition 3.3.7, l'extension k'/k est séparable. Comme $\mathrm{k}' \subset$

K, $\mathrm{Irr}(\alpha, \mathrm{K})|\mathrm{Irr}(\alpha, \mathrm{k}')$ dans $\mathrm{K}[X]$. Les coefficients de ces deux polynômes étant dans k', la division euclidienne se fait dans k' et ainsi $\mathrm{Irr}(\alpha, \mathrm{K}) = \mathrm{Irr}(\alpha, \mathrm{k}')$. Comme α est séparable sur K, alors α l'est aussi sur k'.

Lemme 3.3.12. — *Soit* $\mathrm{K} = \mathrm{k}(\theta)$ *de degré* n *sur* k *et soit* $P = \mathrm{Irr}(\theta, \mathrm{k})$. *Si* K *a* m k*-isomorphismes vers* $\overline{\mathrm{k}}$, *alors tout plongement* σ *de* k *vers* $\overline{\mathrm{k}}$ *se prolonge en exactement* m *isomorphismes.*

Démonstration. — Les k-plongements de K sont en correspondance avec les racines distinctes θ_i de P et les prolongements de σ sont en correspondance avec les racines de $\sigma(P)$. Soit L le corps des racines de $P\sigma(P)$ dans $\overline{\mathrm{k}}$. Alors tout plongement σ se prolonge en τ à L. Les racines de $\sigma(P)$ sont les éléments $\tau(\theta_i)$. On conclut en notant que comme τ est un isomorphisme de L vers L, $\tau(\theta_i) = \tau(\theta_j)$ si et seulement si $\theta_i = \theta_j$. □

Terminons la preuve de la proposition 3.3.11. D'après le lemme 3.3.12, le nombre de prolongements à $\mathrm{k}'(\alpha)$ de tout isomorphisme de k' dans $\overline{\mathrm{k}}$ est égal à $[\mathrm{k}'(\alpha) : \mathrm{k}']$ et ainsi le nombre de k-isomorphismes de $\mathrm{k}'(\alpha)$ dans $\overline{\mathrm{k}}$ est égal à $[\mathrm{k}' : \mathrm{k}][\mathrm{k}'(\alpha) : \mathrm{k}]$. D'après le lemme 3.3.9, $\mathrm{k}'(\alpha)/\mathrm{k}$ est séparable et ainsi α est séparable sur k. □

Corollaire 3.3.13. — *Soient* K/k *et* K′/k *des extensions séparables. Alors* KK′/k *est séparable.*

Démonstration. — Dans ce cas, KK′/K′ (voir le corollaire 3.3.10) et K′/k sont séparables, alors KK′/k est séparable. □

On en arrive à un théorème important.

Théorème 3.3.14 **(Théorème de l'élément primitif)**
Soit K/k *une extension finie. Alors si* K/k *est séparable, il existe* $\alpha \in \mathrm{K}$ *tel que* $\mathrm{K} = \mathrm{k}(\alpha)$.

Démonstration. — • Supposons le corps k fini. Comme K est un k-espace vectoriel de dimension finie, K est également fini. Le groupe des inversible K^* de K est fini, il est cyclique (c'est un résultat classique sur le groupe multiplicatif d'un corps, cf. la section sur les corps finis), engendré par un élément x. Alors $\mathrm{K} = \langle x \rangle \cup \{0\}$ et ainsi $\mathrm{K} = \mathrm{k}(x)$.
• Supposons le corps k infini. Comme $\mathrm{K} = \mathrm{k}(\alpha_1, \cdots, \alpha_n)$, il suffit de montrer le théorème pour $n = 2$.

Pour $\mathrm{K} = \mathrm{k}(\alpha, \beta)$, avec α, β séparables sur k, nous montrons que K/k est une extension simple.
Soit $m = [\mathrm{K} : \mathrm{k}] > 1$ (sinon, il n'y a rien à montrer) et soient $\sigma_1, \cdots, \sigma_m$ les k-isomorphismes distincts de K dans $\overline{\mathrm{k}}$. Considérons le polynôme

$$P = \prod_{i=1}^{m} \prod_{j>i} (\sigma_i(\alpha) - \sigma_j(\alpha) + X(\sigma_i(\beta) - \sigma_j(\beta)) \ \in \overline{\mathrm{k}}[X].$$

L'anneau $\overline{\mathrm{k}}[X]$ étant intègre, le polynôme P est nul si et seulement il existe $i \neq j$, tels que $\sigma_i(\alpha) = \sigma_j(\alpha)$ et $\sigma_i(\beta) = \sigma_j(\beta)$. Comme $\mathrm{K} = \mathrm{k}(\alpha, \beta)$, $P = 0$ si et seulement si $\sigma_i = \sigma_j$. Donc P n'est pas nul.
Comme P n'est pas nul, il n'a qu'un nombre fini de racines. Comme k est infini, il existe $a \in \mathrm{k}$ tel que $P(a) \neq 0$. Alors pour $i \neq j$, $\sigma_i(\alpha) - \sigma_j(\alpha) + a(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0$, ou encore $\sigma_i(\alpha + a\beta) \neq \sigma_j(\alpha + a\beta)$. Posons $x = \alpha + a\beta \in \mathrm{K}$. Alors $\sigma_i(x) \neq \sigma_j(x)$, ce qui signfie que l'éléments x a au moins m k-conjugués distincts ou encore que $[\mathrm{k}(x) : \mathrm{k}] \geq m$. Comme $\mathrm{k}(x) \subset \mathrm{K}$ et que $[\mathrm{K} : \mathrm{k}] = m$, on en déduit $\mathrm{K} = \mathrm{k}(x)$. □

3.4. Dérivée formelle d'un polynôme. Application à la séparabilité

Définition 3.4.1. — Soit k un corps. Dans $\mathrm{k}[X]$, on considère l'opérateur D (dérivée formelle) :

$$\begin{array}{rcl} D : \mathrm{k}[X] & \to & \mathrm{k}[X] \\ D(\sum_{i\geq 0} a_i X^i) & \mapsto & \sum_{i\geq 1} i a_i X^{i-1} \end{array}$$

L'opérateur D a les propriétés attendues :

Proposition 3.4.2. — *Pour tout $P, Q \in \mathrm{k}[X]$, il vient*

(i) $D(P + Q) = D(P) + D(Q)$;

(ii) $D(\lambda P) = \lambda D(P)$, $\lambda \in \mathrm{k}$;

(iii) $D(PQ) = QD(P) + PD(Q)$;

(iv) Si K/k *est une extension, alors la dérivée formelle* D_K *dans* $\mathrm{K}[X]$ *a pour restriction à* $\mathrm{k}[X]$ *la dérivée formelle* D_k.

Démonstration. — À faire en exercice ! □

Pour la suite, nous allons utiliser le *pgcd*. On rappelle que dans $k[X]$ le *pgcd* d de P et Q est caractérisé par : $d|P$, $d|Q$ et il existe $U, V \in \mathrm{k}[X]$ tels que $d = UP + VQ$. Pour toute la suite, nous entendrons par *pgcd* le *pgcd* unitaire.
Cette caractérisation permet de montrer immédiatement la proposition suivante :

Proposition 3.4.3. — *Soit* K/k *une extension et soient* $P, Q \in \mathrm{k}[X]$. *Alors* $pgcd_{\mathrm{k}[X]}(P, Q) = pgcd_{\mathrm{K}[X]}(P, Q)$.

Démonstration. — Soit D_0 le *pgcd* de P et Q dans $\mathrm{k}[X]$: il engendre l'idéal (P, Q) de $\mathrm{k}[X]$, il existe donc U et $V \in \mathrm{k}[X]$ tels que $D_0 = UP + VQ$. Soit D le *pgcd* de P et Q dans $\mathrm{K}[X]$. Alors, comme $D_0|P$ et $D_0|Q$ (dans $\mathrm{K}[X]$), il vient $D\mathrm{K}[X] = (P, Q) \subset D_0\mathrm{K}[X]$. Mais la relation $D_0 = UP + VQ$ implique que $D_0\mathrm{K}[X] \subset (P, Q) = D\mathrm{K}[X]$. Au total, on a donc $D\mathrm{K}[X] = D_0\mathrm{K}[X]$. Comme D et D_0 sont unitaires, il vient $D = D_0$. □

Théorème 3.4.4. — *Soit* $P \in \mathrm{k}[X]$, P *non constant. Alors une condition nécessaire et suffisante pour que* P *soit séparable et que* $pgcd(P, D(P)) = 1$.

Démonstration. — Soit $\overline{\mathrm{k}}$ une clôture algébrique de k et soit

$$P = \prod_{i=1}^{m} (X - \alpha_i)^{s_i},$$

la factorisation de P dans $\overline{\mathrm{k}}[X]$, où les $\alpha_i \in \overline{\mathrm{k}}$ sont distincts deux à deux, et $s_i \geq 1$ (où, sans restriction, on a supposé P unitaire).
•. Supposons P séparable : pour tout i, $s_i = 1$.
Il vient alors $D(P) = \sum_{i \geq 1} \prod_{j \neq i} (X - \alpha_j)$. Les racines de P sont les éléments α_i, mais $D(P)(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0$. Par conséquent, $D(P)$ et P n'ont pas de racines communes et ainsi $pgcd_{\overline{\mathrm{k}}[X]}(P, D(P)) = 1$. On conclut avec la proposition 3.4.3.

• Supposons P non séparable. Alors P a au moins une racine double α_1 : dans la factorisation de P, il vient $s_1 \geq 2$. Alors

$$D(P) = s_1(X-\alpha_1)^{s_1-1}\prod_{j\geq 2}(X-\alpha_j) + \sum_{i\geq 2} s_i(X-\alpha_i)^{s_i-1}\prod_{j\neq i}(X-\alpha_j)^{s_j},$$

et ainsi $D(P)(\alpha_1) = 0$. Les polynômes P et $D(P)$ ont une racine commune par conséquent, $(X-\alpha_1)|pgcd_{\overline{\mathrm{k}}[X]}(P, D(P))$. On conclut avec la proposition 3.4.3. □

Corollaire 3.4.5. — *Soit P un polynôme irréductible de* $\mathrm{k}[X]$*, P non constant. Alors P est séparable sur* k *si et seulement si $D(P) \neq 0$.*

Démonstration. — • Si $D(P) = 0$, alors $(D(P), P) = P$. On conclut avec le théorème 3.4.4.
• Supposons P non séparable. Alors il existe $\alpha \in \overline{\mathrm{k}}$ qui est à la fois racine de P et à la fois racine de $D(P)$. Or $D(P) \in \mathrm{k}[X]$ et $P = \mathrm{Irr}(\alpha, \mathrm{k})$. Par conséquent, P divise $D(P)$ dans $\mathrm{k}[X]$ (voir remarque 1.4.7). Comme $\deg(D(P)) < \deg(P)$, ceci n'est possible que si $D(P) = 0$. □

Exemple 3.4.6. — Revenons au cas où $\mathrm{k} = \mathbb{F}_p(X)$ et $P(Y) = Y^p - X$. Alors $D(P) = \overline{p}Y^{p-1} = 0$. Ainsi, on retrouve bien le fait que P n'est pas séparable sur k.

On en déduit deux corollaires importants en pratique.

Corollaire 3.4.7. — *Tout polynôme irréductible (non constant) sur un corps* k *de caractéristique nulle est séparable.*

Démonstration. — Soit $P = a_nX^n + \cdots + a_1X + a_0 \in \mathrm{k}[X]$, avec $a_n \neq 0$ et $n \geq 1$. Alors $D(P) = na_nX^{n-1} + \cdots + a_1$. Comme $na_n \neq 0$, $D(P) \neq 0$ et on conclut avec le corollaire 3.4.5. □

Corollaire 3.4.8. — *Tout polynôme irréductible (non constant) sur un corps fini* k *est séparable.*

Démonstration. — (Pour plus de détails sur les corps finis, voir le chapitre 5). Soit k un corps fini de caractéristique p. Le corps k est une extension finie de $\mathbb{F}_p$ et en particulier $|\mathrm{k}| = p^r$. Soit $P = a_nX^n + \cdots + a_1X + a_0 \in \mathrm{k}[X]$, avec $a_n \neq 0$ et $n \geq 1$. Alors $D(P) = na_nX^{n-1} + \cdots + a_1$.

Si $D(P) = 0$, cela implique $ia_i = 0$, pour $i = 1, \cdots, n$. Ainsi, pour $i = 1, \cdots, n$, soit $a_i = 0$, soit p divise i. Le polynôme P s'écrit alors

$$P = a_0 + a_p X^p + \cdots + a_{kp} X^{kp} + \cdots + a_{lp} X^{lp} = \sum_{i \geq 0} a_{ip} X^{ip}.$$

Comme k est fini, k^* est cyclique d'ordre $|k| - 1 = p^r - 1$. Ainsi, pour tout x non nul de k, $x^{p^r} - 1 = 1$, ou encore $x^{p^r} = x$ (il en est de même pour $x = 0$). Par conséquent

$$\begin{aligned} P &= a_0^{p^r} + a_p^{p^r} X^p + \cdots + a_{kp}^{p^r} X^{kp} + \cdots + a_{lp}^{p^r} X^{lp} \\ &= \left(a_0^{p^{r-1}} + a_p^{p^{r-1}} X + \cdots + a_{lp}^{p^{r-1}} X^l \right)^p, \end{aligned}$$

ce qui contredit l'irréductibilité de P. □

3.5. Extensions galoisiennes

Nous allons nous intéresser aux extensions finies K/k pour lesquelles le groupe des automorphismes est le plus gros possible, c'est-à-dire d'ordre [K : k].

3.5.1. Définitions. —

Définition 3.5.1. — L'extension finie K/k est dite galoisienne si K/k est normale et séparable. Dans ce cas, le groupe des k-automorphismes de K s'appelle le groupe de Galois de K/k et on le note Gal(K/k).

Remarque 3.5.2. — Nous ne considérons que les extensions galoisiennes finies.

Théorème 3.5.3. — *Si* K/k *est galoisienne (et donc finie), le groupe de Galois* Gal(K/k) *est d'ordre* [K : k].

Démonstration. — D'après le corollaire 3.3.9, comme K/k est séparable, il y a [K : k] k-isomorphismes de K dans $\overline{k}$. L'extension K/k étant normale, tout k-isomorphisme de K est en fait un k-automorphisme, d'où le résultat. □

Corollaire 3.5.4. — *Soient* K/k *et* K′/k *des sous-extensions d'une certaine extension* L/k. *On suppose* K/k *galoisienne. Alors, l'extension* KK′/K′ *est galoisienne.*

Démonstration. — C'est une conséquence immédiate des corollaires 3.2.6 et 3.3.10. □

Corollaire 3.5.5. — *Si* L/k *est galoisienne et si* K/k *est une sous-extension de* L/k, *alors* L/K *est galoisienne.*

Démonstration. — C'est une simple application du corollaire 3.5.4. □

Corollaire 3.5.6. — *Soient* K/k *et* K′/k *deux extensions galoisiennes. Alors* KK′/k *est galoisienne.*

Démonstration. — C'est une conséquence immédiate des corollaires 3.3.13 et 3.2.7. □

Remarque 3.5.7. — Soit K/k une extension séparable finie. Par le théoréme de l'élément primitif, il existe $\theta \in \mathrm{K}$ tel que $\mathrm{K} = \mathrm{k}(\theta)$. Soit N le corps des racines de $P = \mathrm{Irr}(\theta, \mathrm{k})$. Alors N/k est normale. Comme N/k est engendrée par les racines de P (qui est séparable), l'extension N/k est séparable et donc au total galoisienne : l'extension N/k est la plus petite extension galoisienne contenant K/k.

Définition 3.5.8. — Soit K/k une extension séparable finie dans une clôture algébrique $\overline{\mathrm{k}}$ de k. La clôture normale (ou galoisienne) de K/k est la plus petite extension galoisienne (dans $\overline{\mathrm{k}}$) contenant K/k.

Définition 3.5.9. — Une extension K/k est dite abélienne si K/k est galoisienne de groupe de Galois un groupe abélien.
Une extension K/k est dite cyclique si K/k est galoisienne de groupe de Galois un groupe cyclique.

Exemple 3.5.10. — Soit l'élément $\sqrt[3]{2} \in \mathbb{C}$; $P = \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$. Le corps $\mathrm{K} = \mathbb{Q}(j\sqrt[3]{2})$ est le corps des racines de P (voir l'exercice 17). L'extension K/$\mathbb{Q}$ est séparable (car de caractéristique 0) et est normale (K est le corps des racines de P). L'extension K/k est donc galoisienne. Son groupe de Galois est isomorphe à S_3 (à voir en exercice).

Exemple 3.5.11. — Soit la tour d'extensions

$$\mathbb{Q} \text{ —— } \mathrm{K} = \mathbb{Q}(\sqrt{2}) \text{ —— } \mathrm{L} = \mathbb{Q}(\sqrt[4]{2})$$

Les extensions $\mathrm{K}/\mathbb{Q}$ et L/K sont de degré 2 ; $\mathrm{Irr}(\sqrt[4]{2},\mathbb{Q}) = X^4 - 2$ et $\mathrm{Irr}(\sqrt{2},\mathbb{Q}) = X^2 - 2$. Les racines de $X^2 - 2$ étant $\pm\sqrt{2}$, l'extension $\mathrm{K}/\mathbb{Q}$ est normale donc galoisienne. Le groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est d'ordre 2, est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, et est engendré par le $\mathbb{Q}$-automorphisme σ de $\mathbb{Q}(\sqrt{2})$ défini par $\sigma : \sqrt{2} \mapsto -\sqrt{2}$.
Les racines de $X^4 - 2$ sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$. Le corps L étant un sous-corps de $\mathbb{R}$ et comme $i\sqrt[4]{2} \notin \mathrm{L}$, l'extension $\mathrm{L}/\mathbb{Q}$ n'est pas normale. Le corps $\mathrm{F} = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps des racines de $X^4 - 2$. C'est un corps de degré 8 sur $\mathbb{Q}$. L'extension $\mathrm{F}/\mathbb{Q}$ est galoisienne et le groupe de Galois $\mathrm{Gal}(\mathrm{F}/\mathbb{Q})$ est isomorphe au groupe diédral D_8 (voir l'exercice 25).
Á noter que $\mathrm{Irr}(\sqrt[4]{2},\mathrm{K}) = X^2 - \sqrt{2}$. Les racines de $X^2 - \sqrt{2}$ sont $\pm\sqrt[4]{2}$, l'extension L/K est galoisienne.

3.6. Exercices

3.6.1. Énoncés. —

Exercice 20. — *Soit* k *un corps de caractéristique différente de* 2 *et soit* K/k *une extension quadratique (c'est-à-dire de degré* 2*). Montrer que* K/k *est galoisienne.*

Exercice 21. — *Soit* K/k *une extension séparable finie de degré* n*. Soit* N *la clôture galoisienne de* K/k*. Montrer que* $\mathrm{Gal}(N/\mathrm{k})$ *est isomorphe à un sous-groupe transitif de* S_n *(le groupe des permutations à* n *éléments).*

Exercice 22. — *Déterminer, à isomorphisme près, tous les groupes d'ordre* $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14$ *et* 15.

Exercice 23. — *Soit* K *le corps des racines de* $P = X^3 - 2 \in \mathbb{Q}[X]$*. Montrer que* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq S_3$.

Exercice 24. — *Soit le corps* $\mathrm{K} = \mathbb{Q}(\sqrt{2}, i)$*. Montrer que l'extension* K/$\mathbb{Q}$ *est galoisienne, puis déterminer* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

Exercice 25. — *Soit* K *le corps des racines de* $P = X^4 - 2$*. Déterminer le groupe de Galois de* K/$\mathbb{Q}$.

Exercice 26. — *Soit le corps* $\mathrm{k} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$*. Posons* $\theta = (2+\sqrt{2})(3+\sqrt{3})$ *puis* $P = X^2 - \theta \in \mathrm{k}[X]$.

1) Calculer $[\mathrm{k} : \mathbb{Q}]$.
2) Montrer que $\mathrm{k}/\mathbb{Q}$ *est galoisienne et déterminer* $\mathrm{Gal}(\mathrm{k}/\mathbb{Q})$.
3) Pour $\sigma \in \mathrm{Gal}(\mathrm{k}/\mathbb{Q})$, *montrer que* $\theta\sigma(\theta) \in \mathrm{k}^2$.
4) Montrer que P *irréductible sur* k.
5) Soit $\alpha = \sqrt{\theta}$ *une des racines de* P *dans* $\mathbb{C}$ *et soit* $\mathrm{K} = \mathrm{k}(\alpha)$. *Montrer que l'extension* $\mathrm{K}/\mathbb{Q}$ *est galoisienne de degré* 8.
6) Déterminer $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.
7) Montrer que $\mathrm{k} = \mathbb{Q}(\theta)$ *et déterminer* $\mathrm{Irr}(\theta, \mathbb{Q})$.
8) Montrer que $\mathrm{K} = \mathbb{Q}(\alpha)$ *et déterminer* $\mathrm{Irr}(\alpha, \mathbb{Q})$.

Exercice 27. — *Soit* $P = X^5 - 4X^3 - 2 \in \mathbb{Q}[X]$ *et soit* L *le corps des racines de* P *sur* $\mathbb{Q}$. *Posons* $G = \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$.
1) Montrer que G *est un sous-groupe de* S_5 *et que* G *contient un* 5*-cycle.*
2) Montrer que P *a* 3 *racines réelles et* 2 *racines complexes.*
En déduire que G *contient une transposition.*
3) En déduire que $G \simeq S_5$.

3.6.2. Solutions. —
Exercice 20. Soit $\alpha \in \mathrm{K} - \mathrm{k}$. Alors $[\mathrm{k}(\alpha) : \mathrm{k}] > 1$ et la tour d'extensions $\mathrm{k} \text{ —— } \mathrm{k}(\alpha) \text{ —— } \mathrm{K}$, montre que $\mathrm{k}(\alpha) = \mathrm{K}$. Soit $P = \mathrm{Irr}(\alpha, \mathrm{k})$; $P = X^2 + aX + b$, avec $a, b \in \mathrm{k}$. Soit α' l'autre racine de P. Alors comme $\alpha + \alpha' = -a$, $\alpha' \in \mathrm{k}(\alpha)$ et $\mathrm{K} = \mathrm{k}(\alpha) = \mathrm{k}(\alpha, \alpha')$ est le corps des racines de P : K/k est normale. Supposons que $\alpha = \alpha'$. Alors, on obtient $2\alpha = -a$, et comme la caractéristique de K est différente de 2, on en déduit $\alpha = -a/2 \in \mathrm{k}$ ce qui aboutit à une contradiction.
Ainsi α est séparable. L'extension $\mathrm{k}(\alpha)/\mathrm{k}$ est donc normale et séparable : elle est galoisienne de groupe de Galois $G = \langle\sigma\rangle$, où $\sigma : \alpha \mapsto -\alpha - a$.

On aurait pu aussi procéder de la façon suivante. La caractéristique de K étant différente de 2, le calcul suivant a bien un sens :

$$P = X^2 + aX + b = (X + a/2)^2 + (b - a^2/4)$$

Soit alors β une racine de $Q = X^2 + (b - a^2/4)$ (dans une clôture algébrique de k contenant K). Alors $\beta = \pm(\alpha + a/2)$ et ainsi $\mathrm{K} = \mathrm{k}(\alpha) = \mathrm{k}(\beta)$. Les k-conjugués de β sont $\pm\beta \in \mathrm{K}$. Comme la caractéristique de K est

différente de 2, $\beta \neq -\beta$. Ainsi β est séparable sur k et donc k(α)/k est séparable. L'extension K/k est galoisienne de groupe de Galois Gal(K/k) isomorphe à $\mathbb{Z}/2\mathbb{Z}$; Gal(K/k) = $\langle\sigma\rangle$, avec $\sigma : \beta \mapsto -\beta$.

Exercice 21.
L'extension K/k étant séparable, d'après le théorème de l'élément primitif, il existe $\alpha \in$ K tel que K = k(α). En particulier P = Irr(α, k) est un polynôme de degré n. Soient $\alpha = \alpha_1, \cdots, \alpha_n$ les n k-conjugués de α : ces éléments sont deux à deux distincts (car α est séparable). Alors N = k($\alpha_1, \cdots, \alpha_n$). Soit $\sigma \in$ Gal(N/k). Pour tout i, $\sigma(\alpha_i) \in \{\alpha_1, \cdots, \alpha_n\}$ et comme σ est un isomorphisme, pour $k \neq j$, $\sigma(\alpha_j) \neq \sigma(\alpha_k)$. Le groupe Gal($N$/k) opère sur l'ensemble $(\alpha_1, \cdots, \alpha_n)$ par $\sigma \cdot (\alpha_1, \cdots, \alpha_n) = (\sigma(\alpha_1), \cdots, \sigma(\alpha_n))$. On a donc un morphisme ψ de groupes de Gal(N/k) vers S_n. L'action de Gal(N/k) est fidèle (soit $\sigma \in$ Gal(N/k) tel que $\sigma(\alpha_i) = \alpha_i$ pour tout i ; alors σ = id). Ainsi ψ est injectif et Gal(N/k) est bien un sous-groupe de S_n. Ce sous-groupe est même transitif : pour tout i, j, il existe $\sigma \in$ Gal(N/k) tel que $\sigma(\alpha_i) = \alpha_j$.

Exercice 22
Soit un groupe fini G.

• $|G| = p$, où p est un nombre premier. Soit x un élément non trivial de G. Alors l'ordre de $\langle x\rangle$ divise p et est donc égal à p. Ainsi $G = \langle x\rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

• $|G| = p^2$, où p est un nombre premier. On se rappelle que tout p-groupe d'ordre p^2 est abélien et dans ce cas, ou bien $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou bien $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

• $|G| = 6$. Soit G un groupe d'ordre 6. Soit $H = \langle x\rangle$ un 3-Sylow de G et $\langle y\rangle$ un 2-Sylow de G. Comme $[G : \langle x\rangle] = 2$, $\langle x\rangle$ est distingué dans G. Alors $yxy = x^a$, avec $a = \pm 1$.
Le sous-groupe $\langle x, y\rangle$ de G engendré par x et y voit son ordre divisé par 2 et par 3, et ainsi $G = \langle x, y\rangle$.
Si $a = 1$, alors x et y commutent et $G = \langle x\rangle \times \langle y\rangle \simeq \mathbb{Z}/6\mathbb{Z}$.

Si $a = -1$, alors G est le groupe diédral $D_6 = \langle x, y \mid x^3 = 1, y^2 = 1, yxy = x^{-1} \rangle$.

• $|G| = 8$.
Si dans un groupe G, tous les éléments non triviaux de G sont d'ordre 2, alors G est abélien. Si de plus $|G| = 8$, alors $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
Il y a aussi le cas (trivial) ou G contient un élément d'ordre 8 : $G \simeq \mathbb{Z}/8\mathbb{Z}$.
Il reste le cas où G contient un élément x d'ordre 4 (mais pas d'élément d'ordre 8). Alors $\langle x \rangle$ est d'indice 2 dans G et ainsi $\langle x \rangle$ est distingué. Soit y un élément de G qui ne se trouve pas dans $\langle x \rangle$. Alors $\langle y \rangle$ est d'ordre 2 ou 4 et il vient la relation $yxy^{-1} = x^a$, $a \in \mathbb{Z}/4\mathbb{Z}$.

i) Supposons $\langle y \rangle$ d'ordre 2. Pour $z \in G$, notons par φ_z l'homomorphisme de G vers G correspondant à la conjugaison par z. Alors $z \mapsto \varphi_z$ est un morphisme de groupes et $x = \varphi_{y^2}(x) = x^{a^2}$, c'est-à-dire $a \equiv \pm 1 \pmod 4$.
Si $a \equiv 1 (\text{mod } 4)$, le sous-groupe $\langle x, y \rangle$ est commutatif, isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et est donc égal à G.
Si $a \equiv -1 (\text{mod } 4)$, on a les relations $x^4 = 1$, $y^2 = 1$, $yxy = x^{-1}$. Ainsi $G = \langle x, y \rangle$ est le groupe diédral D_8.

ii) Supposons $\langle y \rangle$ d'ordre 4. Alors $yxy^{-1} = x^a$, avec $a \in \mathbb{Z}/4\mathbb{Z}$. Le groupe $\langle x, y \rangle$ contient $\{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$, ces éléments sont bien tous 2 à 2 distincts. Ainsi $G = \langle x, y \rangle = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$. Par conséquent, y^2, d'ordre 2, se trouve dans $\{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$. Comme $y^2 \neq yx^i$, il vient $y^2 = x^2$. On revient à la relation de conjugaison : $x^{a^2} = y^2xy^{-2} = x^2xx^{-2} = x$, et ainsi $a = \pm 1 (\text{mod} 4)$.
Pour $a \equiv 1 (\text{mod } 4)$, on retrouve $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Pour $a \equiv -1 (\text{mod } 4)$, on trouve le groupe $G = \langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$: c'est le groupe $\mathbb{H}_8$ des quaternions d'ordre 8.
On peut vérifier que $D_8 \not\simeq \mathbb{H}_8$: D_8 ne contient qu'un seul sous-groupe cyclique d'ordre 4, alors que $\mathbb{H}_8$ en contient 3.

• $|G| = 10$. Soit x un élément d'ordre 5. Alors $\langle x \rangle$ d'indice 2 dans G, est distingué. Soit ensuite y un élément d'ordre 2. Il apparaît la relation $yxy^{-1} = x^a$, avec $a \equiv \pm 1 (\text{mod } 5)$.
Si $a = 1$, on trouve le groupe commutatif $\mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Si $a = -1$, on trouve le groupe dihédral $D_{10} = \langle x, y \mid x^5 = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$.

• $|G| = 12$. Nous montrons, qu'à isomorphisme près, il y a cinq groupes d'ordre 12.
Commençons par un rappel. *Soit G un groupe d'ordre $p^r N$, $(N, p) = 1$, et soit s le nombre de p-Sylow de G. Alors $s \equiv 1 (\mathrm{mod}\ p)$ et s divise N.*
Soit G un groupe d'ordre 12. Notons par s le nombre de 2-Sylow de G et par t le nombre de 3-Sylow. Alors $s \in \{1, 3\}$ et $t \in \{1, 4\}$.
La discussion va être basée sur les différentes valeurs de s et de t.
$\rightsquigarrow$ $s = 3$ et $t = 4$. Le groupe G contient au moins un élément d'ordre 1 et huit éléments d'ordre 3 provenant des 3-Sylow. Un 2-Sylow apporte 3 nouveaux éléments. Un second 2-Sylow apporte au moins 2 nouveaux éléments, et on au total on obtient déjà $|G| \geq 14$. Ainsi $s = 3$ et $t = 4$ n'est pas possible.
$\rightsquigarrow$ $s = t = 1$. Alors le 3-Sylow H de G et le 2-Sylow H' de G sont distingués. Notons tout d'abord que $H \cap H' = \{1\}$. Soit alors $x \in H$ et $y \in H'$. Alors $xyx^{-1}y^{-1} \in H \cap H' = \{1\}$, c'est-à-dire $xy = yx$. Les sous-groupes H et H' commutent. Le groupe G contient le produit direct $H \times H'$. Ce dernier étant d'ordre 12, on a $G = H \times H'$. En particulier G est commutatif. Ainsi ou bien $G \simeq \mathbb{Z}/12\mathbb{Z}$, ou bien $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
$\rightsquigarrow$ $s = 3$ et $t = 1$. Soit H' le 3-Sylow de G. Celui-ci est distingué. Ensuite soit H un 2-Sylow de G. Alors $H \cap H' = \{1\}$ et H agit sur H'. En particulier G contient le produit $H' \rtimes H$ et, en comparant les cardinaux, $G = H' \rtimes H$. Comme $s \neq 1$, G n'est pas commutatif et l'action de H sur H' n'est pas triviale. Soit x un générateur de H'.
(i) Supposons que $H = \langle y \rangle$, avec y d'ordre 4. Alors $G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, produit non-direct. En particulier G contient un élément d'ordre 4. On peut pousser un peu plus loin la description. On note que $yxy^{-1} = x^{-1}$ puis que $y^2xy^{-2} = x$, c'est-à-dire que y^2 commute avec x. Posons $s = xy^2$ et $t = y$. Alors $G = \langle s, t, s^6 = 1, t^4 = 1, tst^{-1} = s^{-1}, s^3 = t^2 \rangle$.
(ii) Supposons que $H = \langle y, z \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Parmi les trois éléments $\{y, z, yz\}$ d'ordre 2 de H, deux agissent par -1 et le troisième agit trivialement (car l'action de H sur H' n'est pas triviale). Par exemple y et yz agissent par -1 sur x. Alors z agit trivialement sur x. Les éléments x et z

commutent, ainsi xz est d'ordre 6. On a de plus $y(xz)y = x^{-1}z = (xz)^{-1}$ puis $\langle xz\rangle \cap \langle y\rangle = \{1\}$. Par conséquent, le groupe $\langle xz, y\rangle$ est isomorphe au groupe diédral $D_{12} = \langle u, v \mid u^6 = 1, v^2 = 1, vuv = u^{-1}\rangle$ et donc $G \simeq D_{12}$. Comme D_{12} ne contient pas d'élément d'ordre 4, celui-ci n'est pas isomorphe au groupe du point (i).
$\rightsquigarrow$ $s = 1$ et $t = 4$. Le groupe G agit transitivement sur l'ensemble $E = \{H_1, H_2, H_3, H_4\}$ constitué des 3-Sylow de G. Ceci permet de déterminer un morphisme de groupes $\psi : G \to S_4$, où $\psi(\tau)(i)$ est défini par $H_{\psi(\tau)(i)} = \tau H_i \tau^{-1}$. Le noyau de ψ est l'intersection des sous-groupes d'isotropie G_{H_i} des H_i. Comme $t = |G|/|G_{H_i}|$, on a $|G_{H_i}| = 3$. Or $H_i \subset G_{H_i}$, par conséquent $G_{H_i} = H_i$. Ainsi, pour $i \neq j$, $H_i \cap H_j = \{1\}$, $\ker(\psi) = \{1\}$, puis $G \hookrightarrow S_4$. Comme le seul sous-groupe de S_4 d'ordre 12 est A_4, on obtient finalement $G \simeq A_4$.

• $|G| = 14$. Comme pour $|G| = 10$, on trouve ou bien $G \simeq \mathbb{Z}/14\mathbb{Z}$ ou bien $G \simeq D_{14} = \langle x, y \mid x^7 = 1, y^2 = 1, yxy^{-1} = x^{-1}\rangle$.

• $|G| = 15$. Soit $H' = \langle x\rangle$ un 3-Sylow de G et soit $H = \langle y\rangle$ un 5-Sylow de G. Comme le nombre N_5 de 5-Sylow de G est congru à 1 modulo 5 et que N_5 divise 3, on obtient $N_5 = 1$. Le groupe H est distingué. Alors $xyx^{-1} = y^a$, avec $a^3 \equiv 1 (\text{mod } 5)$. On en déduit que $a \equiv 1 (\text{mod } 5)$. Ainsi $G = \langle x\rangle \times \langle y\rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$.

Exercice 23.
On sait déja que $\mathrm{K} = \mathbb{Q}(j, \sqrt[3]{2})$.
Le groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est d'ordre 6 et est un sous-groupe de S_3 (voir exercice 21). Ainsi $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq S_3$.

Retrouvons $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ via la tour d'extensions

$$\mathbb{Q} \text{ —— } \mathbb{Q}(j) \text{ —— } \mathbb{Q}(j)(\sqrt[3]{2}) = \mathrm{K}$$

L'extension $\mathbb{Q}(j)/\mathbb{Q}$ a deux isomorphismes : $\sigma_0 : j \mapsto j$ et $\sigma_1 : j \mapsto j^2$. L'extension $\mathrm{K}/\mathbb{Q}(j)$ étant normale, σ_0 (idem pour σ_1) se prolonge en 3 isomorphismes de K. Ensuite $P = \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}(j)) = X^3 - 2$, et donc

$P = \sigma_0(P) = \sigma_1(P)$. Ainsi, on obtient pour les prolongements de σ_0 :

$$\sigma_{0,0}\left|\begin{array}{ccc} j & \mapsto & j \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array}\right. ; \sigma_{0,1}\left|\begin{array}{ccc} j & \mapsto & j \\ \sqrt[3]{2} & \mapsto & j\sqrt[3]{2} \end{array}\right. ; \sigma_{0,2}\left|\begin{array}{ccc} j & \mapsto & j \\ \sqrt[3]{2} & \mapsto & j^2\sqrt[3]{2} \end{array}\right.$$

et pour les prolongements de σ_1 :

$$\sigma_{1,0}\left|\begin{array}{ccc} j & \mapsto & j^2 \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array}\right. ; \sigma_{1,1}\left|\begin{array}{ccc} j & \mapsto & j^2 \\ \sqrt[3]{2} & \mapsto & j\sqrt[3]{2} \end{array}\right. ; \sigma_{1,2}\left|\begin{array}{ccc} j & \mapsto & j^2 \\ \sqrt[3]{2} & \mapsto & j^2\sqrt[3]{2} \end{array}\right.$$

Posons $\sigma = \sigma_{0,1}$ et $\tau = \sigma_{1,0}$. Alors $\tau(\sigma(j)) = \tau(j) = j^2$ et $\tau(\sigma(\sqrt[3]{2})) = \tau(j\sqrt[3]{2}) = \tau(j)\tau(\sqrt[3]{2}) = j^2\sqrt[3]{2}$:

$$\tau\circ\sigma\left|\begin{array}{ccc} j & \mapsto & j^2 \\ \sqrt[3]{2} & \mapsto & j^2\sqrt[3]{2} \end{array}\right. ; \sigma\circ\tau\left|\begin{array}{ccc} j & \mapsto & j^2 \\ \sqrt[3]{2} & \mapsto & j\sqrt[3]{2} \end{array}\right.$$

On observe ainsi : $\sigma \circ \tau \neq \tau \circ \sigma$ et on retrouve le fait que le groupe $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ n'est pas commutatif.
On peut noter que $\tau^2(j) = \tau(\tau(j)) = \tau(j^2) = \tau(j)^2 = j^4 = j$ et que $\tau^2(\sqrt[3]{2}) = \sqrt[3]{2}$: l'élément τ est d'ordre 2. On peut vérifier que l'élément σ est d'ordre 3 et que l'on a aussi la relation

$$\tau\sigma\tau = \sigma^2 = \sigma^{-1} = \sigma_{0,2}.$$

Exercice 24.
L'extension $\mathrm{K}/\mathbb{Q}$ est le compositum de $\mathbb{Q}(i)/\mathbb{Q}$ et de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Ces deux dernières extensions sont galoisiennes (voir l'exercice 21), ainsi $\mathrm{K}/\mathbb{Q}$ est galoisienne. Comme $i \notin \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$: les extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(i)/\mathbb{Q}$ sont linéairement disjointes et $[\mathrm{K} : \mathbb{Q}] = 4$. Le groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est d'ordre 4 : il est isomorphe ou bien à $\mathbb{Z}/4\mathbb{Z}$ ou bien à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Partons de la tour d'extensions

$$\mathbb{Q} \text{ —— } \mathbb{Q}(i) \text{ —— } \mathbb{Q}(i)(\sqrt{2}) = \mathrm{K}$$

L'extension $\mathbb{Q}(i)/\mathbb{Q}$ a deux isomorphismes : $\sigma_0 : i \mapsto i$ et $\sigma_1 : i \mapsto -i$. Ensuite $P = \mathrm{Irr}(\sqrt{2}, \mathbb{Q}(i)) = X^2 - 2$, puis $\sigma_0(P) = \sigma_1(P) = P$. Ainsi, on obtient pour les prolongements de σ_0 :

$$\sigma_{0,0}\left|\begin{array}{ccc} i & \mapsto & i \\ \sqrt{2} & \mapsto & \sqrt{2} \end{array}\right. ; \sigma_{0,1}\left|\begin{array}{ccc} i & \mapsto & i \\ \sqrt{2} & \mapsto & -\sqrt{2} \end{array}\right.$$

et pour les prolongements de σ_1 :

$$\sigma_{1,0}\left|\begin{array}{ccc} i & \mapsto & -i \\ \sqrt{2} & \mapsto & \sqrt{2} \end{array}\right. ; \sigma_{1,1}\left|\begin{array}{ccc} i & \mapsto & -i \\ \sqrt{2} & \mapsto & -\sqrt{2} \end{array}\right.$$

On peut noter $\sigma_{0,0} = \mathrm{id}$, puis que $\sigma_{0,1}, \sigma_{1,0}$ et $\sigma_{1,1}$ sont d'ordre 2. Ainsi $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Soyons plus précis. Si l'on pose $\sigma = \sigma_{0,1}$ et $\tau = \sigma_{1,0}$, alors $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \langle\sigma\rangle \times \langle\tau\rangle$.

Exercice 25.
Dans $\mathbb{C}$, posons $\alpha = \sqrt[4]{2}$. Les racines de $X^4 - 2$ sont $\pm\alpha$, $\pm i\alpha$.
Soit K le corps des racines de P. Les racines de P s'expriment en fonction de α et de i, ainsi $\mathrm{K} \subset \mathbb{Q}(i, \alpha)$. D'un autre côté, $i, \alpha \in \mathrm{K}$, et au final $\mathrm{K} = \mathbb{Q}(i, \alpha)$.
Comme $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\mathbb{Q}(i) \cap \mathbb{Q}(\alpha) = \mathbb{Q}$, les extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ et $\mathbb{Q}(i)/\mathbb{Q}$ sont linéairement disjointes (voir l'exercice 5 et se rappeler que $[\mathbb{Q}(i) : \mathbb{Q}] = 2$) et ainsi $[\mathrm{K} : \mathbb{Q}] = 8$. En particulier $[\mathbb{Q}(i, \alpha) : \mathbb{Q}(i)] = 4$ et $\mathrm{Irr}(\alpha, \mathbb{Q}(i)) = X^4 - 2$.

$$\begin{array}{ccc} \mathbb{Q}(\alpha) & \overset{2}{\text{———}} & \mathbb{Q}(i, \alpha) \\ {\scriptstyle 4}\,\big| & & \big|\,{\scriptstyle 4} \\ \mathbb{Q} & \underset{2}{\text{———}} & \mathbb{Q}(i) \end{array}$$

Nous allons déterminer les $\mathbb{Q}$-isomorphismes de $\mathbb{Q}(i)$ puis les prolonger à $\mathrm{K} = \mathbb{Q}(i, \alpha)$.
L'extension $\mathbb{Q}(i)/\mathbb{Q}$ a deux isomorphismes : $\sigma_0 : i \mapsto i$ et $\sigma_1 : i \mapsto -i$. Ensuite, comme $P = \mathrm{Irr}(\alpha, \mathbb{Q}(i)) = X^4 - 2$, $\sigma_0(P) = \sigma_1(P) = P$. Ainsi, on obtient pour les prolongements de σ_0 au corps K :

$$\sigma_{0,0}\left|\begin{array}{ccc} i & \mapsto & i \\ \alpha & \mapsto & \alpha \end{array}\right. ; \sigma_{0,1}\left|\begin{array}{ccc} i & \mapsto & i \\ \alpha & \mapsto & -\alpha \end{array}\right. ; \sigma_{0,2}\left|\begin{array}{ccc} i & \mapsto & i \\ \alpha & \mapsto & i\alpha \end{array}\right. ; \sigma_{0,3}\left|\begin{array}{ccc} i & \mapsto & i \\ \alpha & \mapsto & -i\alpha \end{array}\right.$$

et pour les prolongements de σ_1 :

$$\sigma_{1,0}\left|\begin{array}{ccc} i & \mapsto & -i \\ \alpha & \mapsto & \alpha \end{array}\right. ; \sigma_{1,1}\left|\begin{array}{ccc} i & \mapsto & -i \\ \alpha & \mapsto & -\alpha \end{array}\right. ; \sigma_{1,2}\left|\begin{array}{ccc} i & \mapsto & -i \\ \alpha & \mapsto & i\alpha \end{array}\right. ; \sigma_{1,3}\left|\begin{array}{ccc} i & \mapsto & -i \\ \alpha & \mapsto & -i\alpha \end{array}\right.$$

Posons $\sigma = \sigma_{1,0}$ et $\tau = \sigma_{0,2}$. L'élément σ est d'ordre 2, τ est d'ordre 4 et

$$\sigma\tau\sigma \left| \begin{array}{ccc} i & \mapsto & i \\ \alpha & \mapsto & -i\alpha \end{array} \right.$$

c'est-à-dire $\sigma\tau\sigma = \sigma_{0,3} = \tau^{-1}$. On vérifie que les éléments $\sigma_{1,*}$ sont tous d'ordre 2. Le groupe de Galois $\mathrm{Gal(K/\mathbb{Q})}$ ne contient qu'un seul sous-groupe cyclique d'ordre 4 (le sous-groupe $\langle\tau\rangle$).
Ainsi, d'après l'exercice 22, $\mathrm{Gal(K/\mathbb{Q})} \simeq D_8$.

Exercice 26.
1) et 2). Notons que $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. En effet, sinon $\sqrt{2} = a+b\sqrt{3}$, $a, b \in \mathbb{Q}$. On élève au carré pour obtenir, par identification, $ab = 0$ et $2 = a^2 + 3b^2$, d'où une contradiction.
De ceci, on en déduit que $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt{2})$ est une sous-extension strcite de $\mathbb{Q}(\sqrt{3})$, c'est donc $\mathbb{Q}$. Les extensions $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont linéairement disjointes et ainsi $[\mathrm{k} : \mathbb{Q}] = 4$.
On procède comme pour l'exercice 24. L'extension $\mathrm{K}/\mathbb{Q}$ est galoisienne (comme compositum d'extensions galoisiennes) et les 4 $\mathbb{Q}$-isomorphismes de k sont :

$$\sigma_1 \left| \begin{array}{ccc} \sqrt{3} & \mapsto & \sqrt{3} \\ \sqrt{2} & \mapsto & \sqrt{2} \end{array} \right. ; \sigma_2 \left| \begin{array}{ccc} \sqrt{3} & \mapsto & \sqrt{3} \\ \sqrt{2} & \mapsto & -\sqrt{2} \end{array} \right. ; \sigma_3 \left| \begin{array}{ccc} \sqrt{3} & \mapsto & -\sqrt{3} \\ \sqrt{2} & \mapsto & \sqrt{2} \end{array} \right. ; \sigma_4 \left| \begin{array}{ccc} \sqrt{3} & \mapsto & -\sqrt{3} \\ \sqrt{2} & \mapsto & -\sqrt{2} \end{array} \right.$$

3) $\theta\sigma_1(\theta) = \theta^2 \in \mathrm{k}^2$; $\theta\sigma_2(\theta) = (3+\sqrt{3})^2(\sqrt{2})^2 \in \mathrm{k}^2$; $\theta\sigma_3(\theta) = (\sqrt{3}\sqrt{2})^2(2+\sqrt{2})^2$; $\theta\sigma_4(\theta) = (2\sqrt{3})^2 \in \mathrm{k}^2$.

4) Tout élément de k s'écrit sous la forme $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, $a, b, c, d \in \mathbb{Q}$ (voir, par exemple, le lemme 1.3.7). Regardons si $\theta \in \mathrm{k}^2$. Peut-on avoir

$$(a + b\sqrt{2} + \sqrt{3}(c + d\sqrt{2}))^2 = \theta \ ? \tag{2}$$

On fait agir σ_3 sur l'égalité précédente, pour obtenir :

$$(a + b\sqrt{2} - \sqrt{3}(c + d\sqrt{2}))^2 = \sigma_3(\theta) \tag{3}$$

On multiplie (2) et (3) pour obtenir

$$\Big((a + b\sqrt{2})^2 - 3(c + d\sqrt{2})^2\Big)^2 = 6(2 + \sqrt{2})^2. \tag{4}$$

De (4), on en déduit

$$\sqrt{3} = \pm\frac{(a+b\sqrt{2})^2 - 3(c+d\sqrt{2})^2}{\sqrt{2}(2+\sqrt{2})} \in \mathbb{Q}(\sqrt{2}),$$

d'où une contradiction.
L'élément θ n'est pas un carré de k, le polynôme $P = X^2 - \theta$ est donc irréductible sur k et ainsi $[\mathrm{k}(\alpha) : \mathbb{Q}] = [\mathrm{k}(\alpha) : \mathrm{k}][\mathrm{k} : \mathbb{Q}] = 2 \cdot 4 = 8$.

5) et 6) Chaque $\mathbb{Q}$-automorphisme σ_i de k se prolonge en deux k-isomorphismes $\sigma_{i,j}$ de K et ces prolongements sont en correspondance avec les racines des polynômes $\sigma_i(P)$.
Ainsi σ_1 se prolonge en

$$\sigma_{1,1}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & \sqrt{3}\\ \sqrt{2} & \mapsto & \sqrt{2}\\ \alpha & \mapsto & \sqrt{\theta}\end{array}\right. ; \sigma_{1,2}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & \sqrt{3}\\ \sqrt{2} & \mapsto & \sqrt{2}\\ \alpha & \mapsto & -\sqrt{\theta}\end{array}\right.$$

σ_2 se prolonge en

$$\sigma_{2,1}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & \sqrt{3}\\ \sqrt{2} & \mapsto & -\sqrt{2}\\ \alpha & \mapsto & \sqrt{\sigma_2(\theta)}\end{array}\right. ; \sigma_{2,2}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & \sqrt{3}\\ \sqrt{2} & \mapsto & -\sqrt{2}\\ \alpha & \mapsto & -\sqrt{\sigma_2(\theta)}\end{array}\right.$$

σ_3 se prolonge en

$$\sigma_{3,1}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & -\sqrt{3}\\ \sqrt{2} & \mapsto & \sqrt{2}\\ \alpha & \mapsto & \sqrt{\sigma_3(\theta)}\end{array}\right. ; \sigma_{3,2}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & -\sqrt{3}\\ \sqrt{2} & \mapsto & \sqrt{2}\\ \alpha & \mapsto & -\sqrt{\sigma_3(\theta)}\end{array}\right.$$

et σ_4 se prolonge en

$$\sigma_{4,1}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & -\sqrt{3}\\ \sqrt{2} & \mapsto & -\sqrt{2}\\ \alpha & \mapsto & \sqrt{\sigma_4(\theta)}\end{array}\right. ; \sigma_{4,2}\left|\begin{array}{rcl}\sqrt{3} & \mapsto & -\sqrt{3}\\ \sqrt{2} & \mapsto & -\sqrt{2}\\ \alpha & \mapsto & -\sqrt{\sigma_4(\theta)}\end{array}\right.$$

Maintenant, grâce à la question 3), on obtient que $\sigma_{i,j}(\alpha) \in \mathrm{k}(\alpha)$ et ainsi les huit k-isomorphismes $\sigma_{i,j}$ sont des k-automorphismes de K. L'extension K/k est donc bien galoisienne.

Soit $\sigma = \sigma_{2,1}$. Alors

$$\begin{aligned}\sigma^2(\alpha) &= \sigma\left(\frac{(3+\sqrt{3})\sqrt{2}}{\alpha}\right)\\ &= \frac{\sigma\left(3+\sqrt{3}\right)\sigma\left(\sqrt{2}\right)}{\sigma(\alpha)}\\ &= -\alpha\end{aligned}$$

L'élément σ est d'ordre 4 et

$$\sigma^3 \left| \begin{array}{rcl} \sqrt{3} & \mapsto & \sqrt{3} \\ \sqrt{2} & \mapsto & -\sqrt{2} \\ \alpha & \mapsto & -\sqrt{\sigma_3(\theta)} \end{array} \right.$$

Posons ensuite $\tau = \sigma_{3,1}$. Alors

$$\begin{aligned}\tau^2(\alpha) &= \tau\left(\frac{(2+\sqrt{2})\sqrt{2}\sqrt{3}}{\alpha}\right)\\ &= \frac{\tau\left(\sqrt{2}(2+\sqrt{2})\right)\tau\left(\sqrt{3}\right)}{\tau(\alpha)}\\ &= -\alpha\end{aligned}$$

L'élément τ est d'ordre 4 et $\tau \notin \langle\sigma\rangle$. Le groupe $\mathrm{Gal(K/\mathbb{Q})}$ contient deux sous-groupes (distincts) d'ordre 4 : ce n'est donc pas D_8. Mais $\sigma(\tau(\alpha)) = \dfrac{-(2-\sqrt{2})\sqrt{3}}{3+\sqrt{3}}\alpha$ et $\tau(\sigma(\alpha)) = \dfrac{3-\sqrt{3}}{\sqrt{3}(2+\sqrt{2})}\alpha$. Ces quantités sont différentes (de signes opposés !) ainsi $\sigma\tau \neq \tau\sigma$, le groupe $\mathrm{Gal(K/\mathbb{Q})}$ n'est pas commutatif et ainsi, il est isomorphe à $\mathbb{H}_8$.

7) On note que pour $i \neq j$, $\sigma_i(\theta) \neq \sigma_j(\theta)$. Or les $\mathbb{Q}$-conjugués de θ, c'est-à-dire les racines de $\mathrm{Irr}(\theta, \mathbb{Q})$, sont exactement les éléments $\sigma_i(\theta)$. Ces éléments étant tous distincts, cela signifie que $\mathrm{Irr}(\theta, \mathbb{Q})$ est de degré 4 et

$$\begin{aligned}\mathrm{Irr}(\theta, \mathbb{Q}) &= \prod_{i=1}^{4}(X - \sigma_i(\theta))\\ &= X^4 - 24X^3 + 144X^2 - 288X + 144.\end{aligned}$$

8) Là aussi, on compare les 8 $\mathbb{Q}$-conjugués de α.

Supposons $\sigma_{i,j}(\alpha) = \sigma_{r,s}(\alpha)$. Alors $\sigma_{i,j}(\theta) = \sigma_{k,l}(\theta)$, et ainsi, en notant que $\sigma_{i,j}(\theta) = \sigma_i(\theta)$, on obtient tout d'abord $i = r$. Ensuite, comme

$\sigma_{i,1}(\alpha) = -\sigma_{i,2}(\alpha)$ on en déduit que les 8 éléments $\sigma_{i,j}(\alpha)$ sont 2 à 2 distincts. L'éléments α est donc bien de degré 8 sur $\mathbb{Q}$ et

$$\begin{aligned} \mathrm{Irr}(\alpha, \mathbb{Q}) &= \prod_{i,j}(X - \sigma_{i,j}(\alpha)) \\ &= \mathrm{Irr}(\theta, \mathbb{Q})(X^2) \\ &= X^8 - 24X^6 + 144X^4 - 288X^2 + 144. \end{aligned}$$

Exercice 27.
1) Le polynôme P est irréductible sur $\mathbb{Q}$ (critère d'Eisenstein avec $p = 2$). Ainsi G est un sous-groupe de S_5. D'autre part, si θ est une racine de P, L contient $\mathbb{Q}(\theta)$. Ainsi $[\mathbb{Q}(\theta) : \mathbb{Q}]$ divise $|G|$, ou encore G contient un élément τ d'ordre 5 : cet élément τ est un 5-cycle.
2) Une étude rapide de la fonction $x \mapsto P(x)$ montre que P a trois racines réelles $\theta_1, \theta_2, \theta_3$ et deux complexes θ_4 et θ_5.
Soit c la conjugaison complexe. L'élément c est un élément de $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ et c laisse fixe θ_1, θ_2 et θ_3, mais permute θ_4 et θ_5. En d'autres termes, G contient une transposition (la transposition $(4, 5)$).
3) On conclut avec un résultat de théorie des groupes : soit p un nombre premier, si un sous-groupe H de S_p contient un p-cycle et une transposition, alors $H = S_p$ (voir la proposition 5.4.2).

CHAPITRE 4

THÉORIE DE GALOIS

Étant donnée une extension galoisienne K/k, la théorie de Galois consiste à décrire le treillis des sous-extensions de K/k à partir de celui des sous-groupes de Gal(K/k).

4.1. Corps fixes

Commençons par un lemme.

Lemme 4.1.1. — *Soit H un groupe d'automorphismes d'un corps* K. *Alors*

$$\{x \in \mathrm{K},\ \forall \sigma \in H,\ \sigma(x) = x\}$$

est un sous-corps de K *et*

$$\{\sigma \in H,\ \sigma_{|\mathrm{K}} = \mathrm{id}\}$$

est un sous-groupe de H.

Démonstration. — Immédiat ! □

Définition 4.1.2. — Soit H un groupe d'automorphismes d'un corps K. Alors $\{x \in \mathrm{K},\ \forall \sigma \in H,\ \sigma(x) = x\}$ est appelé le sous-corps de K fixe par H et est noté K^H.
On dit qu'un élément x de K est fixe par H si $x \in \mathrm{K}^H$.

Proposition 4.1.3. — *Soit* L/k *une extension galoisienne (donc finie) de groupe de Galois G.*
(i) Alors $\mathrm{L}^G = \mathrm{k}$.

(ii) Si K/k *est une sous-extension de* L/k*, alors* L/K *est galoisienne et le groupe de Galois* $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ *est égal à* $\{\sigma \in G,\ \sigma_{|\mathrm{K}} = id\}$*.*

Démonstration. — Tout d'abord, d'après le lemme 4.1.1, L^G est bien un sous-corps de L et $\{\sigma \in G,\ \sigma_{|\mathrm{K}} = \mathrm{id}\}$ bien un sous-groupe de G.
(i) Comme $G = \mathrm{Gal}(\mathrm{L}/\mathrm{k})$ est le groupe des k-automorphismes de L, il vient que pour tout élément $\sigma \in G$, $\sigma_{|\mathrm{k}} = \mathrm{id}$. Ainsi $\mathrm{k} \subset \mathrm{L}^G$ et on a la tour d'extensions

$$\mathrm{k} \text{ —— } \mathrm{L}^G \text{ —— } \mathrm{L}$$

Comme G agit trivialement sur L^G, tout élément de G peut être vu comme un L^G-automorphisme de L/L^G. D'autre part, d'après le corollaire 3.5.5, comme L/k est galoisienne, l'extension L/L^G est galoisienne et donc $G \hookrightarrow \mathrm{Gal}(\mathrm{L}/\mathrm{L}^G)$. Ainsi $|G|$ divise $[\mathrm{L} : \mathrm{L}^G]$. Comme $|G| = [\mathrm{L} : \mathrm{k}]$, on a au final $[\mathrm{L}^G : \mathrm{k}] = 1$.
(ii) L'extension L/K est galoisienne (voir le corollaire 3.5.5). Soit $\sigma \in \{\sigma \in G,\ \sigma_{|\mathrm{K}} = \mathrm{id}\}$. Alors σ est un K-automorphisme de L, c'est-à-dire $\sigma \in \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Ainsi $\{\sigma \in G,\ \sigma_{|\mathrm{K}} = \mathrm{id}\}$ est un sous-groupe de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Réciproquement. Soit $\sigma' \in \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Alors σ' est un K-automorphisme de L. En particulier, comme $\mathrm{k} \subset \mathrm{K}$, c'est un k-automorphisme de L dont la restriction à K est l'identité. Ainsi $\sigma' \in \{\sigma \in G,\ \sigma_{|\mathrm{K}} = \mathrm{id}\}$.
Au final, on a bien la double inclusion souhaitée. □

Donnons une première application utile en pratique de la proposition 4.1.3.

Proposition 4.1.4. — *Soient* K *et* K′ *des sous-extensions de* L/k*. On suppose que* K/k *est finie galoisienne. Alors* K/k *et* K'/k *sont linéairement disjointes si et seulement si* $\mathrm{K} \cap \mathrm{K}' = \mathrm{k}$*.*

Démonstration. — On sait déja qu'il est nécessaire d'avoir $\mathrm{K} \cap \mathrm{K}' = \mathrm{k}$. Supposons donc que $\mathrm{K} \cap \mathrm{K}' = \mathrm{k}$. Soit $(\alpha_1, \cdots, \alpha_n)$ une famille k-libre d'éléments de K′ que l'on suppose K-liée, où l'entier n est minimal ; $n > 1$. Il existe $\lambda_i \in \mathrm{K}$ tels que

$$\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n = 0. \tag{5}$$

L'extension KK'/K' étant galoisienne (voir corollaire 3.5.4), soit $\sigma \in \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$. Alors

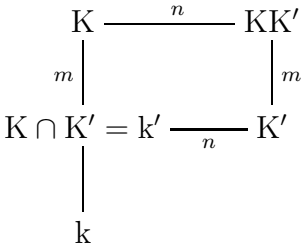
$$\alpha_1 + \sigma(\lambda_2)\alpha_2 + \cdots + \sigma(\lambda_n)\alpha_n = 0 \tag{6}$$

On soustrait (5) et (6) pour obtenir

$$(\sigma(\lambda_2) - \lambda_2)\alpha_2 + \cdots + (\sigma(\lambda_n) - \lambda_n)\alpha_n = 0. \tag{7}$$

Or $\sigma \in \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$, en particulier σ est un k-isomorphisme de KK'. La restriction de σ à K est un k-isomorphisme de K. Mais comme K/k est galoisienne, tout k-isomorphisme de K est un k-automorphisme. Ainsi $\sigma(\lambda_i) \in \mathrm{K}$ et la relation (7) donne une relation de dépendance sur K entre les éléments $\alpha_2, \cdots, \alpha_n$. Par minimalité de n, la relation (7) doit être triviale : pour $i = 2, \cdots, n$, $\sigma(\lambda_i) = \lambda_i$. Ainsi, si l'on pose $H = \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$, on a pour $i = 2, \cdots, n$, $\lambda_i \in (\mathrm{KK}')^H \cap \mathrm{K} = \mathrm{K}' \cap \mathrm{K} = \mathrm{k}$, ce qui contredit la liberté de $(\alpha_1, \cdots, \alpha_n)$ sur k. □

Corollaire 4.1.5. — *Soient* K/k *et* K′/k *deux extensions finies. Posons* $\mathrm{k}' = \mathrm{K} \cap \mathrm{K}'$ *et supposons* K/k *galoisienne. Alors les extensions* K/k′ *et* K′/k′ *sont linéairement disjoints et* $[\mathrm{KK}' : \mathrm{k}] = [\mathrm{K} : \mathrm{k}][\mathrm{K}' : \mathrm{k}']$. *Au final, on a*



Démonstration. — On applique la proposition 4.1.4 aux extensions K/k′ et K′/k′ (en notant que K/k′ est bien galoisienne). □

On en arrive à un lemme clé.

Proposition 4.1.6 **(Lemme d'Artin)**. — *Soit* K *un corps et soit* H *un groupe fini d'automorphismes de* K. *Alors* K/K^H *est galoisienne de groupe de Galois* H.

Démonstration. — Nous allons tout d'abord montrer que l'extension K/K^H est séparable puis que si α est un élément de K, alors les K^H-conjugués de α sont dans K (c'est la normalité pour une extension quelconque).
Soit $\alpha \in \mathrm{K}$. Considérons le plus gros sous-ensemble $S = \{\sigma_1(\alpha), \cdots, \sigma_r(\alpha)\}$ de $\{\sigma(\alpha),\ \sigma \in H\}$ tel que les éléments de S sont 2 à 2 distincts. Comme H est fini, l'ensemble S est fini. Ensuite, par maximalité de S, H opère sur $S : \forall \tau \in H,\ \tau(\sigma_i(\alpha)) \in S$. Soit alors

$$P = \prod_{x \in S} (X - x).$$

Comme H est un groupe d'automorphismes de K, $P \in \mathrm{K}[X]$. En fait, on a mieux. Comme H opère sur S, pour tout élément $\tau \in H$, $\tau(P) = P$. Les coefficients de P sont stables sous l'action de H, c'est-à-dire, $P \in \mathrm{K}^H[X]$. Comme $\mathrm{id} \in H$, α est une racine de P, par conséquent $\mathrm{Irr}(\alpha, \mathrm{K}^H) | P$. Le polynôme P étant séparable, on en déduit la séparabilité de $\mathrm{Irr}(\alpha, \mathrm{K}^H)$. On a également obtenu le fait que les K^H-conjugués de α sont dans l'ensemble S, c'est-à-dire sont dans K, puis que $[\mathrm{K}^H(\alpha) : \mathrm{K}^H] \leq |H| = n$. Nous venons donc de montrer que K/K^H est séparable et normale. L'extension K/K^H est galoisienne de groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathrm{K}^H)$.

Montrons maintenant que K/K^H est de degré au plus n. Supposons $[\mathrm{K} : \mathrm{K}^H] > n$, où $n = |H|$. Alors, on peut trouver une suite d'éléments $y_1, \cdots, y_k \in \mathrm{K}$, tels que $[\mathrm{K}^H(y_1, \cdots, y_i, y_{i+1}) : \mathrm{K}^H(y_1, \cdots, y_i)] > 1$ et $[\mathrm{K}^H(y_1, \cdots, y_k) : \mathrm{K}^H] > n$. Nous avons vu que les éléments y_i sont séparables sur K^H, ainsi l'extension $\mathrm{K}^H(y_1, \cdots, y_k)/\mathrm{K}^H$ est séparable et par le théorème de l'élément primitif, il existe $z \in \mathrm{K}$ tel que $\mathrm{K}^H(z) = \mathrm{K}^H(y_1, \cdots, y_k)$. Or d'après le début de la preuve, $[\mathrm{K}^H(z) : \mathrm{K}] \leq |H| = n$, d'où une contradiction.
On a donc : $[\mathrm{K} : \mathrm{K}^H] \leq n$.

Pour terminer, il suffit alors de noter que le groupe H agit via l'identité sur K^H, ainsi H est un sous groupe de $\mathrm{Gal}(\mathrm{K}/\mathrm{K}^H)$ ce qui implique $[\mathrm{K} : \mathrm{K}^H] \geq n$. Au final, $[\mathrm{K} : \mathrm{K}^H] = n$ et $H = \mathrm{Gal}(\mathrm{K}/\mathrm{K}^H)$. □

4.2. Correspondance de Galois

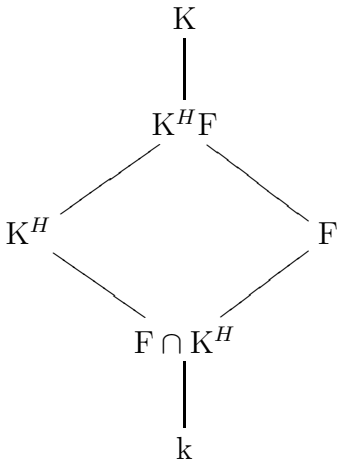
Théorème 4.2.1 **(Premier théorème fondamental)**
Soit K/k *une extension galoisienne (finie) de groupe de Galois* G*. Alors il existe une correspondance bijective entre l'ensemble des sous-extensions de* K/k *et l'ensemble des sous-groupes de* G*. Cette correspondance est la suivante :*

$$H \text{ sous-groupe de } G \longrightarrow \mathrm{K}^H \text{ le corps fixe par les éléments de } H.$$

La correspondance inverse étant :

$$\mathrm{F},\ \mathrm{k} \subset \mathrm{F} \subset \mathrm{K} \longrightarrow H = \mathrm{Gal}(\mathrm{K}/\mathrm{F}) \subset G.$$

Démonstration. — Montrons l'injectivité de la correspondance : groupes $\to$ corps. Soient H_1 et H_2 deux sous-groupes de G tels que $\mathrm{K}^{H_1} = \mathrm{K}^{H_2}$. Par le lemme d'Artin 4.1.6, $\mathrm{K}/\mathrm{K}^{H_1}$ et $\mathrm{K}/\mathrm{K}^{H_2}$ sont galoisiennes et, $\mathrm{Gal}(\mathrm{K}/\mathrm{K}^{H_1}) = H_1$, $\mathrm{Gal}(\mathrm{K}/\mathrm{K}^{H_2}) = H_2$. Ainsi, il vient $H_1 = H_2$.
Montrons la surjectivité. Soit F/k une sous-extension de K/k. Soit $H = \{\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{k}),\ \sigma_{|\mathrm{F}} = \mathrm{id}\}$. D'après le lemme 4.1.1, H est un sous-groupe de Gal(K/k) et d'après la proposition 4.1.3, $\mathrm{Gal}(\mathrm{K}/\mathrm{F}) = H$.
Soit alors le corps K^H. Considérons le compositum $\mathrm{K}^H\mathrm{F}$ dans l'extension K/k.



Comme H agit trivialement sur K^H et sur F, H agit trivialement sur $\mathrm{K}^H\mathrm{F}$. En particulier, $H \subset \mathrm{Gal}(\mathrm{K}/\mathrm{K}^H\mathrm{F})$. Or l'extension K/K^H est galoisienne de groupe de Galois H, ce qui signifie que $[\mathrm{K} : \mathrm{K}^H] = |H|$. On en déduit alors que $H = \mathrm{Gal}(\mathrm{K}/\mathrm{K}^H\mathrm{F})$ et $\mathrm{K}^H\mathrm{F} = \mathrm{K}^H$ c'est-à-dire $\mathrm{F} \subset \mathrm{K}^H$. On utilise ensuite le fait que K/F est également galoisienne de groupe de Galois H (donc $[\mathrm{K} : \mathrm{F}] = |H|$) pour obtenir au final $\mathrm{K}^H = \mathrm{F}$.

Pour terminer, montrons que les correspondances annoncées sont bien inverses l'une de l'autre :

$$H \to \mathrm{K}^H \to \mathrm{Gal}(\mathrm{K}/\mathrm{K}^H) = H,$$

grâce au lemme d'Artin. Puis

$$\mathrm{F} \to H = \{\sigma \in G,\ \sigma_{|\mathrm{F}} = \mathrm{id}\} \to \mathrm{K}^H = \mathrm{F},$$

d'après le preuve de la surjectivité de la première correspondance. □

Corollaire 4.2.2. — *Soit* K/k *une extension galoisienne de groupe de Galois G. Alors la correspondance de Galois a les propriétés suivantes :*

(i) $\mathrm{F}_1 \subset \mathrm{F}_2$ *si et seulement si* $\mathrm{Gal}(\mathrm{K}/\mathrm{F}_2) \subset \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1)$ *;*

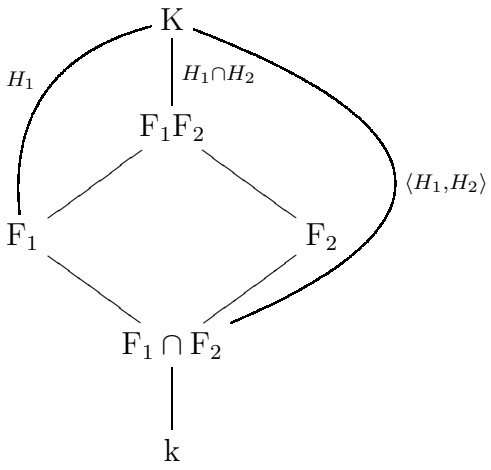
(ii) $\mathrm{Gal}(\mathrm{K}/\mathrm{F}_1\mathrm{F}_2) = \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1) \cap \mathrm{Gal}(\mathrm{K}/\mathrm{F}_2)$ *;*

(iii) $\mathrm{Gal}(\mathrm{K}/\mathrm{F}_1 \cap \mathrm{F}_2) = \langle \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1), \mathrm{Gal}(\mathrm{K}/\mathrm{F}_2) \rangle$.

Démonstration. — Soit $H_i = \mathrm{Gal}(\mathrm{K}/\mathrm{F}_i) = \{\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{k}),\ \sigma_{|\mathrm{F}_i} = \mathrm{id}\}$.
(i) Suppsons $\mathrm{F}_1 \subset \mathrm{F}_2$. Si $\sigma_{|\mathrm{F}_2} = \mathrm{id}$, alors on a aussi $\sigma_{|\mathrm{F}_1} = \mathrm{id}$ et ainsi $H_2 \subset H_1$.
Réciproquement. Si $H_2 \subset H_1$, alors $\mathrm{K}^{H_1} \subset \mathrm{K}^{H_2}$, c'est-à-dire $\mathrm{F}_1 \subset \mathrm{F}_1$.
(ii) Soit $\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1) \cap \mathrm{Gal}(\mathrm{K}/\mathrm{F}_2)$. Alors σ agit trivialement sur F_1 et sur F_2 ; l'élément σ agit trivialement sur le compositum $\mathrm{F}_1\mathrm{F}_2$ et ainsi $\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1\mathrm{F}_2)$, d'où une inclusion.
Réciproquement. Soit $\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1\mathrm{F}_2)$. Alors $\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{F}_i)$, en effet σ agit comme l'identité sur $\mathrm{F}_1\mathrm{F}_2$ donc sur F_1 et sur F_2. Ainsi $\sigma \in \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1) \cap \mathrm{Gal}(\mathrm{K}/\mathrm{F}_2)$.
(iii) On note que tout élément de H_1 laisse fixe $\mathrm{F}_1 \cap \mathrm{F}_2$. Ainsi pour tout élément $\sigma \in \langle H_1, H_2 \rangle$, σ laisse fixe $\mathrm{F}_1 \cap \mathrm{F}_2$, d'où $\langle H_1, H_2 \rangle \subset \mathrm{Gal}(\mathrm{K}/\mathrm{F}_1 \cap \mathrm{F}_2)$.

Réciproquement. Notons par $H = \langle H_1, H_2 \rangle$. Alors K^H est un sous-corps de $\mathrm{F}_1 = \mathrm{K}^{H_1}$ et de $\mathrm{F}_2 = \mathrm{K}^{H_2}$. Ainsi $\mathrm{K}^H \subset \mathrm{F}_1 \cap \mathrm{F}_2$ ou encore $\mathrm{Gal}(\mathrm{K}/\mathrm{K}_1 \cap \mathrm{K}_2) \subset H$. □

Remarque 4.2.3. — Il vient le schéma (ou treillis) suivant ($H_i = \mathrm{Gal}(\mathrm{K}/\mathrm{F}_i)$) :



On en arrive à un problème important en théorie de Galois. Étant donnée une extension galoisienne K/k et une sous-extension F/k de K/k, à quelle condition l'extension F/k est-elle galoisienne ?

Théorème 4.2.4 **(Second théorème fondamental)**
Soit K/k *une extension galoisienne (finie) de groupe de Galois* G*. Soit* F/k *une sous-extension de* K/k *et soit* $H = \mathrm{Gal}(\mathrm{K}/\mathrm{F})$.
Alors l'extension F/k *est galoisienne si et seulement si le sous-groupe* H *est distingué (ou normal) dans le groupe* G.
Si c'est le cas, on a $\mathrm{Gal}(\mathrm{F}/\mathrm{k}) \xrightarrow[can.]{\simeq} G/H$ *. L'isomorphisme résulte de la factorisation de l'homomorphisme de restriction*

$$\begin{array}{rcl} h : G & \to & \mathrm{Gal}(\mathrm{F}/\mathrm{k}) \\ \sigma & \mapsto & \sigma_{|\mathrm{F}} \end{array}$$

Remarque 4.2.5. — On peut noter que $\ker(h) = \{\sigma \in G,\ \sigma_{|\mathrm{F}} = \mathrm{id}\} = \mathrm{Gal}(\mathrm{F}/\mathrm{K})$ (d'après le théorème 4.2.1).

Démonstration. — Commençons par le lemme suivant :

Lemme 4.2.6. — *Conservons les notations du théorème 4.2.4. Soit $\sigma \in G$. Alors* $\mathrm{K}/\sigma(\mathrm{F})$ *est galoisienne et* $\mathrm{Gal}(\mathrm{K}/\sigma(\mathrm{F})) = H_\sigma$, *où* $H_\sigma = \sigma H \sigma^{-1}$ *est le conjugué de* H *par* σ.

Démonstration. — Il est clair que $\mathrm{K}/\sigma(\mathrm{F})$ est galoisienne. Comme $[\mathrm{K} : \mathrm{F}] = [\sigma(\mathrm{K}) : \sigma(\mathrm{F})] = [\mathrm{K} : \sigma(\mathrm{F})]$, il suffit de montrer que $H_\sigma \subset \mathrm{Gal}(\mathrm{K}/\sigma(\mathrm{F}))$ ou encore que H_σ laisse fixe $\sigma(\mathrm{F})$. C'est alors élémentaire. Soit $\tau \in H$ et soit $x \in \mathrm{F}$. Alors

$$\sigma\tau\sigma^{-1}(\sigma(x)) = \sigma(\tau(x)) = \sigma(x),$$

car $\tau(x) = x$ (en effet, $\tau \in \mathrm{Gal}(\mathrm{K}/\mathrm{F})$). □

(Suite de la preuve du théorème 4.2.4.)
• Supposons F/k galoisienne.
Soit $\sigma \in G$. Alors $\sigma_{|\mathrm{F}}$ est un k-isomorphisme de F dans $\overline{\mathrm{k}}$. Par hypothèse c'est un automorphisme de F et $\sigma(\mathrm{F}) = \mathrm{F}$. Par conséquent, à l'aide du lemme 4.2.6, $H = \mathrm{Gal}(\mathrm{K}/\mathrm{F}) = \mathrm{Gal}(\mathrm{K}/\sigma(F)) = H_\sigma$, ce qui signifie exactement que H est normal dans G.
• Réciproquement. Supposons H distingué dans G.
Soit $\sigma \in G$. Alors $H_\sigma = H$. Ainsi par unicité de la correspondance de Galois et le lemme 4.2.6, il vient $\sigma(\mathrm{F}) = \mathrm{F}$. Partons alors d'un k-isomorphisme τ de F. Par le théorème de prolongement des isomorphismes, τ se prolonge en un k-isomorphisme $\overline{\tau}$ de K. Comme K/k est normale, $\overline{\tau}$ est un automorphisme de K/k : $\overline{\tau} \in G$. Ainsi, $\tau(\mathrm{F}) = \overline{\tau}(\mathrm{F}) = \mathrm{F}$ et ainsi F/k est normale ; elle est également séparable (voir proposition 3.3.6) : l'extension F/k est galoisienne.
• Pour terminer, vérifions que l'homomorphisme de groupes h est bien un isomorphisme. Comme F/k est normale, pour tout élément $\sigma \in G$, $\sigma_{|\mathrm{F}}$ est un k-automorphisme de F, c'est-à-dire est un élément de $\mathrm{Gal}(\mathrm{F}/\mathrm{k})$. On a aussi $\ker(h) = \mathrm{Gal}(\mathrm{K}/\mathrm{F})$. Reste à montrer que $\mathrm{Im}(h) = \mathrm{Gal}(\mathrm{F}/\mathrm{k})$. Or $|\mathrm{Im}(h)| = |\mathrm{Gal}(\mathrm{K}/\mathrm{k})|/|\ker(h)| = [\mathrm{K} : \mathrm{k}]/[\mathrm{K} : \mathrm{F}] = [\mathrm{F} : \mathrm{k}]$ d'où la surjectivité. La factorisation de h donne alors bien $\mathrm{Gal}(\mathrm{F}/\mathrm{k}) \simeq G/H$. □

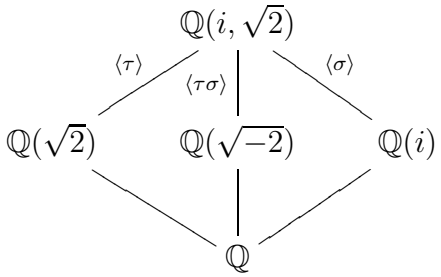
Exemple 4.2.7. — Soit l'extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. C'est une extension galoisienne de groupe de Galois $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (voir l'exercice 24). Soit

$$\sigma \left| \begin{array}{ccc} i & \mapsto & i \\ \sqrt{2} & \mapsto & -\sqrt{2} \end{array} \right. ; \tau \left| \begin{array}{ccc} i & \mapsto & -i \\ \sqrt{2} & \mapsto & \sqrt{2} \end{array} \right.$$

Alors $G = \langle\sigma\rangle \times \langle\tau\rangle$ et

$$\sigma\tau \left| \begin{array}{ccc} i & \mapsto & -i \\ \sqrt{2} & \mapsto & -\sqrt{2} \end{array} \right.$$

Déterminons les sous-groupes de G.
Un seul sous-groupe d'ordre 1 : $\langle \mathrm{id} \rangle$.
Trois sous-groupes d'ordre 2 : $\langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle$.
Un seul sous-groupe d'ordre 4.
La correspondance de Galois indique alors que l'extension $\mathrm{K}/\mathbb{Q}$ contient trois sous-corps stricts : $\mathrm{K}^{\langle\sigma\rangle}$, $\mathrm{K}^{\langle\tau\rangle}$ et $\mathrm{K}^{\langle\sigma\tau\rangle}$.
On note ensuite que σ laisse fixe i et ainsi $\mathbb{Q}(i) \subset \mathrm{K}^{\langle\sigma\rangle}$. Comme $[\mathrm{K}^{\langle\sigma\rangle} : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$, on conclut à $\mathbb{Q}(i) = \mathrm{K}^{\langle\sigma\rangle}$.
Ensuite, on note que τ laisse fixe $\sqrt{2}$ et ainsi, comme pour $\mathbb{Q}(i)$, on a $\mathrm{K}^{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2})$. Enfin $\sigma\tau$ laisse fixe $i\sqrt{2} = \sqrt{-2}$ et on conclut à $\mathrm{K}^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{-2})$.
Au total, on a le treillis complet des sous-corps de $\mathbb{Q}(i, \sqrt{2})$:



Un tel treillis permet par exemple de trouver un élément primitif pour l'extension $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$. Typiquement, comme σ, τ et $\sigma\tau$ ne fixent pas $i + \sqrt{2}$, on en déduit que $\mathbb{Q}(i + \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$. (Voir aussi l'exercice 32.)
Enfin, notons que comme G est abélien, tous les sous-groupes sont distingués et donc toutes les extensions en jeu sont galoisiennes.

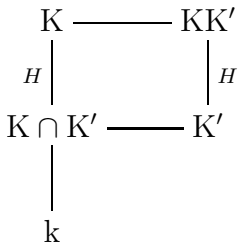
4.3. Propriétés élémentaires

Théorème 4.3.1. — *Soient* K/k *une extension galoisienne et* K'/k *une extension quelconque. Alors* KK'/K' *est galoisienne de groupe de Galois canoniquement isomorphe à* $\mathrm{Gal}(\mathrm{K}/\mathrm{K} \cap \mathrm{K}')$. *L'isomorphisme est donné*

par restriction

$$\begin{array}{rcl} h : \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}') & \to & \mathrm{Gal}(\mathrm{K}/\mathrm{K}\cap\mathrm{K}') \\ \sigma & \mapsto & \sigma_{|\mathrm{K}} \end{array}$$

Remarque 4.3.2. — On a le schéma suivant



Démonstration. — On sait déja que KK'/K' est galoisienne de degré $|\mathrm{Gal}(\mathrm{K}/\mathrm{K}\cap\mathrm{K}')|$ (voir le corollaire 4.1.5).
Ensuite, remarquons que h est bien défini. Soit $\sigma \in \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$. Alors pour tout $x \in \mathrm{K}\cap\mathrm{K}' \subset \mathrm{K}'$, $\sigma(x) = x$, ainsi $\sigma_{|\mathrm{K}}$ est en particulier un $\mathrm{K}\cap\mathrm{K}'$-isomorphisme de K. Comme $\mathrm{K}/\mathrm{K}\cap\mathrm{K}'$ est galoisienne, $\sigma_{|\mathrm{K}}$ est un automorphisme de K, ou encore $\sigma_{|\mathrm{K}} \in \mathrm{Gal}(\mathrm{K}/\mathrm{K}\cap\mathrm{K}')$.
Il suffit alors de montrer l'injectivité de h. C'est immédiat. Soit $\sigma \in \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$ tel que $\sigma_{|\mathrm{K}} = \mathrm{id}$. Comme on a aussi $\sigma_{|\mathrm{K}'} = \mathrm{id}$, au final, on obtient $\sigma = \mathrm{id}$. □

Théorème 4.3.3. — *Soient* K/k *et* K'/k *deux extensions galoisiennes. Notons* $H = \mathrm{Gal}(\mathrm{K}/\mathrm{K}\cap\mathrm{K}')$ *puis* $H' = \mathrm{Gal}(\mathrm{K}'/\mathrm{K}\cap\mathrm{K}')$.
Alors $\mathrm{KK}'/\mathrm{K}\cap\mathrm{K}'$ *est galoisienne de groupe de Galois* $\mathrm{Gal}(\mathrm{KK}'/\mathrm{K}) \times \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$ *et ce groupe est canoniquement isomorphe à* $H \times H'$.

Démonstration. — Il suffit de montrer que $\mathrm{Gal}(\mathrm{KK}'/\mathrm{K}\cap\mathrm{K}') = \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}) \times \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$. La suite se déduit du théorème 4.3.1.
On sait déja que $|\mathrm{Gal}(\mathrm{KK}'/\mathrm{K}\cap\mathrm{K}'| = |\mathrm{Gal}(\mathrm{KK}'/\mathrm{K})| \times |\mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')|$. Ensuite clairement $\langle \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}), \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')\rangle \subset \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}\cap\mathrm{K}')$ puis, tout automorphisme de $\mathrm{Gal}(\mathrm{KK}'/\mathrm{K}) \cap \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$ restreint à $\mathrm{K}\cap\mathrm{K}'$ est trivial.
Vérifions pour finir qu'étant donné $\sigma \in \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}')$ et $\tau \in \mathrm{Gal}(\mathrm{KK}'/\mathrm{K})$, alors $\sigma\tau = \tau\sigma$.

Soit $x \in \mathrm{K}$. Notons que $\sigma(x) = \sigma_{|\mathrm{K}}(x) \in \mathrm{K}$, car $\sigma_{|\mathrm{K}} \in \mathrm{Gal}(\mathrm{K}/\mathrm{K} \cap \mathrm{K}')$. Alors $\tau(\sigma(x)) = \sigma(x) = \sigma(\tau(x))$, car $\tau_{|\mathrm{K}} = \mathrm{id}$. Ainsi σ et τ commutent sur K. Il en est de même sur K′ et donc $\sigma\tau = \tau\sigma$.
Au final, $\langle \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}), \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}') \rangle = \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}) \times \mathrm{Gal}(\mathrm{KK}'/\mathrm{K}') = \mathrm{Gal}(\mathrm{KK}'/\mathrm{K} \cap \mathrm{K}')$. □

4.4. Norme et trace

4.4.1. — Soit K/k une extension galoisienne de groupe de Galois G. La norme et la trace permettent, à partir de la connaissance d'un élément de K, de construire un élément de k.

Lemme 4.4.1. — *Soit* K/k *une extension galoisienne de groupe de Galois* G. *Pour tout* $\alpha \in \mathrm{K}$, *les éléments* $\sum_{\sigma \in G} \sigma(\alpha)$ *et* $\prod_{\sigma \in G} \sigma(\alpha)$ *sont dans* k.

Démonstration. — Soit $\tau \in G$. Alors

$$\begin{array}{rcl} \tau\left(\sum_{\sigma \in G} \sigma(\alpha)\right) & = & \sum_{\sigma \in G} \tau(\sigma(\alpha)) \\ & = & \sum_{\sigma' \in G} \sigma'(\alpha) \end{array}$$

où l'on a posé $\sigma' = \tau\sigma$ (σ parcourt G si et seulement si σ' parcourt G). Ainsi $\displaystyle\sum_{\sigma \in G} \sigma(\alpha) \in \mathrm{K}^G = \mathrm{k}$.
De même pour $\displaystyle\prod_{\sigma \in G} \sigma(\alpha)$. □

Définition 4.4.2. — Soit K/k une extension galoisienne de groupe de Galois G. Soit $\alpha \in \mathrm{K}$.
La quantité $\displaystyle\sum_{\sigma \in G} \sigma(\alpha)$ est appelée trace de α dans K/k et est notée $\mathrm{Tr}_{\mathrm{K/k}}(\alpha)$.
La quantité $\displaystyle\prod_{\sigma \in G} \sigma(\alpha)$ est appelée norme de α dans K/k et est notée $\mathrm{N}_{\mathrm{K/k}}(\alpha)$.

Remarque 4.4.3. — Si $\alpha \in \mathrm{k}$, alors $\mathrm{Tr}_{\mathrm{K/k}}(\alpha) = [\mathrm{K} : \mathrm{k}]\alpha$ et $\mathrm{N}_{\mathrm{K/k}}(\alpha) = \alpha^{[\mathrm{K:k}]}$.

Proposition 4.4.4. — *Soit* K/k *une extension galoisienne. Alors pour tout* $\alpha, \beta \in \mathrm{K}$,

$$\mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(\alpha+\beta) = \mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(\alpha) + \mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(\beta)$$

et

$$\mathrm{N}_{\mathrm{K}/\mathrm{k}}(\alpha\beta) = \mathrm{N}_{\mathrm{K}/\mathrm{k}}(\alpha) \cdot \mathrm{N}_{\mathrm{K}/\mathrm{k}}(\beta).$$

Démonstration. — C'est immédiat. □

Proposition 4.4.5. — *Soit* K/k *une extension galoisienne de degré* $n = md$ *et soit* $\alpha \in \mathrm{K}/\mathrm{k}$ *de degré* d *sur* k.
Soit $\mathrm{Irr}(\alpha, \mathrm{k}) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ *le polynôme irréductible de* α *sur* k. *Alors* $\mathrm{N}_{\mathrm{K}/\mathrm{k}}(\alpha) = (-1)^n a_0^m$ *et* $\mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(\alpha) = -ma_{d-1}$.

Démonstration. — Le résultat repose sur le théorème du prolongement des isomorphismes. L'extension $\mathrm{k}(\alpha)/\mathrm{k}$ étant séparable, elle admet $\sigma_1, \cdots, \sigma_d$ isomorphismes dans $\overline{\mathrm{k}}$ (en fait dans K). En particulier,

$$\mathrm{Irr}(\alpha, \mathrm{k}) = \prod_{i=1}^{d} (X - \sigma_i(\alpha))$$

et après identification, on trouve

$$a_{d-1} = -\sum_{i=1}^{d} \sigma_i(\alpha) \text{ et } \ a_0 = (-1)^d \prod_{i=1}^{d} \sigma_i(\alpha).$$

Chaque isomorphisme σ_i se prolonge en m k-automorphismes $\sigma_{i,j}$ de K. En particulier, $\sigma_{i,j}(\alpha) = \sigma_i(\alpha)$. Ainsi

$$\begin{aligned} \mathrm{Tr}_{\mathrm{K}/\mathrm{k}}\alpha &= \textstyle\sum_{i=1}^{d}\sum_{j=1}^{m} \sigma_{i,j}(\alpha) \\ &= \textstyle\sum_{i=1}^{d}\sum_{j=1}^{m} \sigma_i(\alpha) \\ &= m\textstyle\sum_{i=1}^{d} \sigma_i(\alpha) \\ &= -ma_{d-1}. \end{aligned}$$

De même

$$\begin{aligned} \mathrm{N}_{\mathrm{K}/\mathrm{k}}\alpha &= \textstyle\prod_{i=1}^{d}\prod_{j=1}^{m} \sigma_{i,j}(\alpha) \\ &= \textstyle\prod_{i=1}^{d}\prod_{j=1}^{m} \sigma_i(\alpha) \\ &= (\textstyle\prod_{i=1}^{d} \sigma_i(\alpha))^m \\ &= (-1)^n a_0^m. \end{aligned}$$

□

On a ainsi le corollaire suivant :

Corollaire 4.4.6. — *Soit* $\mathrm{k}(\alpha)/\mathrm{k}$ *une extension galoisienne de degré* n. *Alors*

$$\mathrm{Irr}(\alpha, \mathrm{k}) = X^n - \mathrm{Tr}_{\mathrm{K/k}}(\alpha)X^{n-1} + \cdots + (-1)^n \mathrm{N}_{\mathrm{K/k}}(\alpha).$$

4.4.2. — Soit $P \in \mathbb{Q}[X]$ unitaire de degré n, et soit $\theta_1, \cdots, \theta_n$ les racines de P.

Théorème 4.4.7. — *Supposons que* $P \in \mathbb{Z}[X]$ *(et unitaire). Alors*

$$\mathbb{Z}[\theta_1, \cdots, \theta_n] \cap \mathbb{Q} = \mathbb{Z}.$$

Démonstration. — Pour ce faire, nous allons passer par la notion d'*entiers algébriques*. Commençons par un lemme.

Lemme 4.4.8. — *Soit* B *un anneau commutatif et soit* $x \in B$. *Supposons qu'il existe un polynôme* $S \in \mathbb{Z}[X]$ *unitaire (donc non nul) tel que* $S(x) = 0$. *Alors* $\mathbb{Z}[x]$ *est un* $\mathbb{Z}$*-module de type fini.*

Remarque 4.4.9. — Un tel élément x est dit entier algébrique.

Démonstration. — Soit $n = \deg(S)$ et soit $Q \in \mathbb{Z}[X]$ un polynôme quelconque. Alors la division euclidienne de Q par S s'effectue dans $\mathbb{Z}[X]$ de reste R de degré plus petit que $n-1$, et on a donc $Q(x) = R(x)$, prouvant que $\mathbb{Z}[x] = \mathbb{Z} + \mathbb{Z}x_+\mathbb{Z}x^2 + \cdots + \mathbb{Z}x^{n-1}$, et donc que $\mathbb{Z}[x]$ est un $\mathbb{Z}$-module de type fini. □

Soit alors l'anneau $A = \mathbb{Z}[\theta_1, \cdots, \theta_n] \subset \mathrm{K}_P$.
Le lemme 4.4.8 nous permet alors de montrer que l'anneau A est un $\mathbb{Z}$-module de type fini. En effet le lemme 4.4.8 (appliqué à l'anneau $\mathbb{Z}[\theta_1]$ et à l'élément θ_2) montre que $\mathbb{Z}[\theta_1][\theta_2]$ est un $\mathbb{Z}[\theta_1]$-module de type fini. Comme $\mathbb{Z}[\theta_1]$ est lui-même de type fini (toujours par le lemme 4.4.8), on en déduit que $\mathbb{Z}[\theta_1, \theta_2] = \mathbb{Z}[\theta_1][\theta_2]$ est un $\mathbb{Z}$-module de type fini. Etc.

Nous allons maintenant montrer que pour tout élément de $a \in A$, l'anneau $\mathbb{Z}[a]$ est un $\mathbb{Z}$-module de type fini. Pour cela nous allons vérifier qu'il existe un polynôme S unitaire et à coefficients entiers tels que $S(a) = 0$. Il suffira ensuite d'utiliser le lemme 4.4.8 pour conclure. Soit

alors $\{b_1, \cdots, b_m\}$ une famille génératrice de A en tant que $\mathbb{Z}$-module. Pour $i = 1, \cdots, m$, l'élément ab_i s'écrit en fonction des b_j :

$$ab_i = \sum_j \lambda_{i,j} b_j,$$

avec $\lambda_{i,j} \in \mathbb{Z}$. Si l'on note par $M = (\lambda_{i,j})_{i,j}$ la matrice carrée d'ordre $m \times m$, il vient que a est une valeur propre de M et donc que a est un zéro du polynôme caractéristique de M, qui est bien dans $\mathbb{Z}[X]$ et unitaire.
Nous pouvons établir la preuve du théorème 4.4.7. Soit $a \in A \cap \mathbb{Q}$. Alors d'après le point précédent $\mathbb{Z}[a]$ doit être de type fini. Ecrivons $a = p/q$ avec $(p, q) = 1$. Soit ensuite $a_1, \cdots, a_m$ une famille d'éléments de $\mathbb{Z}[p/q]$ engendrant $\mathbb{Z}[p/q]$ comme $\mathbb{Z}$-module. Il est alors immédiat de voir qu'il existe k tel que $\mathbb{Z}[p/q] \subset \mathbb{Z}\dfrac{1}{q^k}$. Ceci ne peut être possible que si $q = \pm 1$. □

Corollaire 4.4.10. — *Soit $P \in \mathbb{Z}[X]$ unitaire et soit $\theta_1, \cdots, \theta_n$ les racines de P. Alors pour tout $\alpha \in A := \mathbb{Z}[\theta_1, \cdots, \theta_n]$, on a $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$. En particulier $\mathrm{N}_{\mathbb{Q}_P/\mathbb{Q}}(\alpha)$ et $\mathrm{Tr}_{\mathbb{Q}_P/\mathbb{Q}}(\theta)$ sont dans $\mathbb{Z}$, où $\mathbb{Q}_P$ est le corps des racines de P.*

Démonstration. — Soit ensuite $\alpha \in A$. Observons que les conjugués α_i de α sont aussi dans A car A est stable par $G = \mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$. Par conséquent tous les coefficients de $\mathrm{Irr}(\alpha, \mathbb{Q})$ sont aussi dans A (car A est un anneau), mais également dans $\mathbb{Q}$. D'après le théorème 4.4.7, on a donc $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$, et en particulier $\mathrm{N}_{\mathbb{Q}_P/\mathbb{Q}}(\alpha)\mathbb{Z}$ et $\mathrm{Tr}_{\mathbb{Q}_P/\mathbb{Q}}(\alpha)$ sont bien dans $\mathbb{Z}$ (d'après la proposition 4.4.5). □

4.5. Exercices

4.5.1. Énoncés. —

Exercice 28. — *Soit $\mathrm{K} = \mathbb{C}(X_1, \cdots, X_n)$ le corps des fractions rationnelles sur $\mathbb{C}$ en n variables. Sur K opère le groupe S_n par $\sigma(X_i) = X_{\sigma(i)}$. Soit le corps $\mathrm{k} = \mathrm{K}^{S_n}$.*
1) Déterminer le corps k, puis montrer que K/k est galoisienne. Que vaut $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$?

2) On prend $n = 2$. Trouver un élément primtif θ de K/k puis décrire $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$ à partir de θ.
3) On suppose $n = 3$. Déterminer tous les sous-corps de K/k puis donner un polynôme irréductible sur k, de degré 3, ayant K comme corps des racines.

***Exercice 29* (Suite de l'exercice 23).** — *Déterminer tous les sous-corps de l'extension $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$.*

***Exercice 30* (Suite de l'exercice 25).** — *Déterminer tous les sous-corps du corps des racines $\mathrm{K}/\mathbb{Q}$ de $P = X^4 - 2 \in \mathbb{Q}[X]$, puis toutes les sous-extensions galoisiennes $\mathrm{F}/\mathbb{Q}$ de $\mathrm{K}/\mathbb{Q}$.*

***Exercice 31* (Suite de l'exercice 26).** — *Reprendre l'exercice 26 en déterminant tous les sous-extensions de $\mathrm{K}/\mathbb{Q}$, puis celles qui sont galoisiennes sur $\mathbb{Q}$.*

Exercice 32. — *Soit k un corps de caractéristique p (éventuellement $p = 0$). Soient $\mathrm{k}(\alpha_1)/\mathrm{k}$ et $\mathrm{k}(\alpha_2)/\mathrm{k}$ deux extensions galoisiennes de degré m et n avec $(mn, p) = 1$. Posons $\mathrm{k}_0 = \mathrm{k}(\alpha_1) \cap \mathrm{k}(\alpha_2)$.*
On veut montrer que $\alpha_1 + \alpha_2$ est un élément primitif de K/k, où $\mathrm{K} = \mathrm{k}(\alpha_1, \alpha_2)$.
Supposons : $\mathrm{k}(\alpha_1 + \alpha_2) \neq \mathrm{k}(\alpha_1, \alpha_2)$.
Soit $H_i = \mathrm{Gal}(\mathrm{K}/\mathrm{k}(\alpha_i))$.
1) Montrer que pour $i = 1$ ou $i = 2$, il existe $s \in H_i$, $s \neq \mathrm{id}$, tel que pour $j \neq i$, $s(\alpha_j) - \alpha_j \in \mathrm{k}_0 = \mathrm{k}(\alpha_1) \cap \mathrm{k}(\alpha_2)$.
Pour la suite, nous supposons que $s \in H_1$.
2) Soit $\Gamma = \langle s \rangle \times H_2$ et $\mathrm{F} = \mathrm{K}^{\Gamma}$.
a) Montrer que $\mathrm{F} \subset \mathrm{k}_0(\alpha_2)$ puis que $[\mathrm{k}_0(\alpha_2) : \mathrm{F}] > 1$.
b) Soit $\beta = \sum_{i=0}^{m'-1} s^i(\alpha_2)$, où m' est l'ordre de $\langle s \rangle$.
Montrer que $\mathrm{k}_0(\beta) = \mathrm{k}_0(\alpha_2)$ puis que $\mathrm{k}_0(\beta) \subset F$.
Conclure à une absurdité.

Exercice 33. — *Soit un nombre premier p et soit K/k une extension galoisienne de groupe de Galois G. On suppose le groupe G abélien. Soit $G^p = \{\sigma^p, \sigma \in G\}$.*

Montrer que toute sous-extension F/k *de degré* p *de* K/k *est fixe par* G^p.

Exercice 34. — *On propose de montrer que* $\mathbb{C}$ *est algébriquement clos.*
1) Soit θ *algébrique sur* $\mathbb{C}$. *Quel est le degré de* θ *sur* $\mathbb{R}$ *?*
2) Supposons $\mathbb{C}$ *non algébriquement clos. Soit* θ *algébrique sur* $\mathbb{C}$, *avec* $\theta \notin \mathbb{C}$. *Montrer l'existence d'une extension galoisienne* $\mathrm{K}/\mathbb{R}$ *de degré une puissance de* 2, *avec* $\mathbb{R}(\theta) \subset \mathrm{K}$.
3) Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{C}$. *Conclure.*

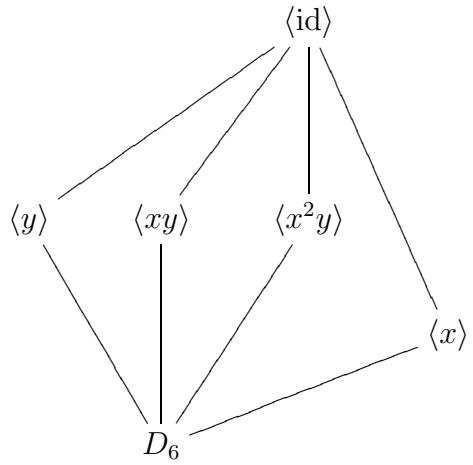
4.5.2. Solutions. —

Exercice 44.
1) Le corps k est le corps des fractions rationnelles stables sous l'action de S_n. Par factorialité de $\mathbb{C}[X_1, \cdots, X_n]$, une fraction rationnelle stable sous S_n s'écrit sous la forme P/Q, avec P et Q deux polynômes symétriques (c'est-à-dire stables sous S_n). Pour aller plus loin, on peut se rappeler que tout polynôme symétrique se trouve dans l'algèbre engendrée par les polynômes symétriques élémentaires. L'extension K/k est galoisienne et $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = S_n$ (par application du lemme d'Artin).

2) Ici $S_2 = \langle (1,2) \rangle = \langle \sigma \rangle$ et $\mathrm{K} = \mathbb{C}(X, Y)$. Il nous faut trouver un élément $\theta \notin \mathrm{k}$. Par exemple $\theta = X - Y$. En effet : $\sigma(X - Y) = Y - X \neq X - Y$ et donc $\mathrm{k}(\theta) = \mathrm{K}$. Les conjugués de θ sont donc $\pm\theta$ et $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = \langle \tau \rangle$ avec $\tau : \theta \mapsto -\theta$.
À noter que $(X - Y)^2 = X^2 + Y^2 - 2XY \in \mathrm{k}$, ce qui signifie que $X - Y$ est racine du polynôme $P(T) = T^2 - (X^2 + Y^2 - 2XY) \in \mathrm{k}[T]$.

3) Ici $\mathrm{K} = \mathbb{C}(X_1, X_2, X_3)$ et $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = S_3$. Posons $X = X_1$, $Y = X_2$ et $Z = X_3$.
Le groupe S_3 est égal au groupe diédral $D_6 = \langle x, y,\ x^3 = 1,\ y^2 = 1,\ yxy = x^{-1} \rangle$. Prenons pour x le 3-cycle $(1, 2, 3)$ et pour y la transposition $(1, 2)$.
On a ainsi, $x(X) = Y$, $x(Y) = Z$, $x(Z) = X$, $y(X) = Y$, $y(Y) = X$ et $y(Z) = Z$.
Listons les sous-groupes de D_6. Le point de départ est que l'ordre d'un sous-groupe de D_6 divise 6. Comme les diviseurs stricts de 6 sont premiers, les sous-groupes stricts sont cycliques.

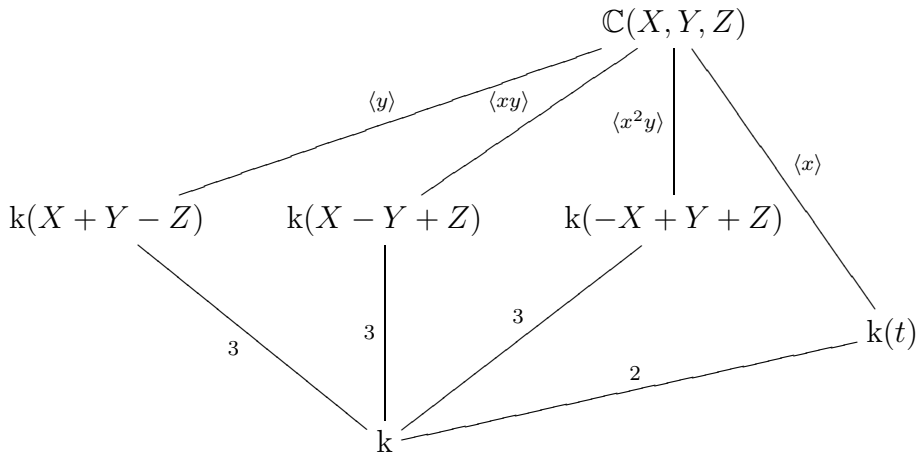
1 seul sous-groupe d'ordre 1 : $\langle \mathrm{id} \rangle$.
3 sous-groupes d'ordre 2 : $\langle y \rangle$, $\langle xy \rangle$, $\langle x^2 y \rangle$
1 seul sous-groupe d'ordre 3 : $\langle x \rangle$
1 seul sous-groupe d'ordre 6 : D_6.
On obtient le treillis des sous-groupes de D_6 :



Le polynôme $X + Y - Z$ est fixe par l'action de y, mais n'est pas symétrique. Ainsi, $[\mathrm{k}(X + Y - Z) : \mathrm{k}] > 1$ et $\mathrm{k}(X + Y - Z)$ est contenu dans $\mathrm{K}^{\langle y \rangle}/\mathrm{k}$. Or $[\mathrm{K} : \mathrm{K}^{\langle y \rangle}] = |\langle y \rangle| = 2$, ainsi on a la tour d'extensions

$$\mathrm{k} \overset{3}{\frown} \mathrm{k}(X + Y - X) \frac{\quad}{} \mathrm{K}^{\langle y \rangle} \overset{2}{\frac{\quad}{}} \mathrm{K} \, ,$$

d'où $\mathrm{k}(X + Y - Z) = \mathrm{K}^{\langle y \rangle}$.
Suivant la même démarche : $xy = (1, 3)$ et $\mathrm{K}^{\langle xy \rangle} = \mathrm{k}(X + Z - Y)$; $x^2 y = (2, 3)$ et $\mathrm{K}^{\langle x^2 y \rangle} = \mathrm{k}(-X + Y + Z)$.
Enfin, $(X - Y)(X - Z)(Y - Z)$ est fixe par le 3-cycle $(1, 2, 3)$ mais pas par $(1, 2)$. Ainsi $\mathrm{K}^{\langle x \rangle} = \mathrm{k}((X - Y)(X - Z)(Y - Z)$. Au total, on obtient le treillis complet des sous-extensions de K/k :



où l'on a posé $t = (X-Y)(X-Z)(Y-Z)$. À noter que $\langle x\rangle$ est le seul sous-groupe distingué non trivial de D_6 et ainsi $\mathrm{k}(t)/\mathrm{k}$ est la seule sous-extension galoisienne stricte de K/k.

Soit $P = \mathrm{Irr}(X+Y-Z, \mathrm{k})$. Comme $\mathrm{k}(X+Y-Z)/\mathrm{k}$ n'est pas galoisienne, le corps des racines de P est strictement plus grand que $\mathrm{k}(X+Y-Z)$ mais est contenu dans K : il est égal à K.
Recherchons donc P. Le polynôme P est un polynôme de degré 3 et

$$P(T) = \prod_{i=1}^{3}(T-\alpha_i),$$

où les α_i sont les k-conjugués de $X+Y-Z$. Lorsque l'on fait varier $\sigma \in G$, on est sûr que $\sigma(X+Y-Z)$ donne les 3 conjugués recherchés (en double). Or $xy(X+Y-Z) = Z+Y-X$ et $x^2y(X+Y-Z) = X+Z-Y$. Ainsi les k-conjugués de $X+Y-Z$ sont : $X+Y-Z$, $Z+Y-X$ et $X+Z-Y$. D'où

$$\begin{aligned} P(T) &= (T-(X+Y-Z))(T-(Z+Y-X))(T-(X+Z-Y)) \\ &= T^3 - a_2T^2 - a_1T + a_0 \end{aligned}$$

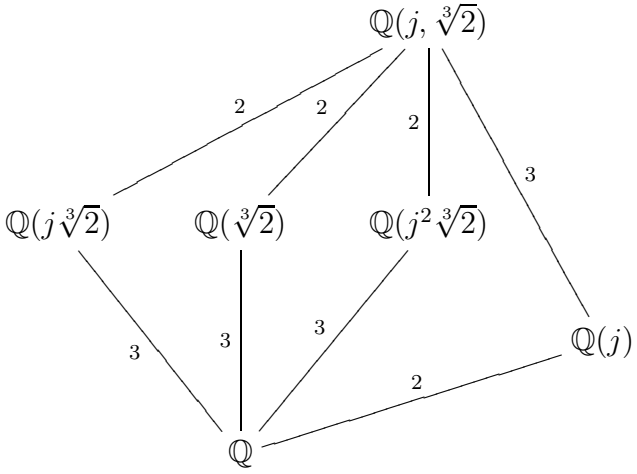
avec

$$\begin{cases} a_2 = X+Y+Z \\ a_1 = X^2+Y^2+Z^2-2(XY+XZ+YZ) \\ a_0 = X^3+Y^3+Z^3+5XYZ+(X+Y+Z)(XY+XZ+YZ) \end{cases}$$

Exercice 29. On reprend les notations de l'exercice 23. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q})$ est engendré par σ et τ :

$$\sigma \left| \begin{array}{ccc} j & \mapsto & j \\ \sqrt[3]{2} & \mapsto & j\sqrt[3]{2} \end{array} \right. \quad \tau \left| \begin{array}{ccc} j & \mapsto & j^2 \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array} \right.$$

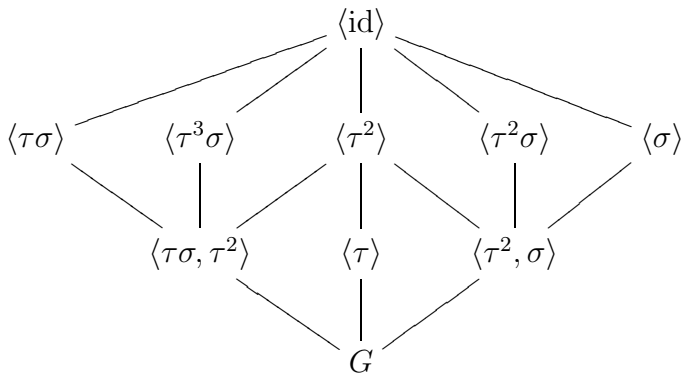
L'élément σ est d'ordre 3, τ est d'ordre 2, et on a la relation $\tau\sigma\tau = \sigma^{-1}$.
Le groupe $S_3 = D_6$ contient :
1 seul sous-groupe d'ordre 1 : $\langle \mathrm{id} \rangle$.
3 sous-groupes d'ordre 2 : $\langle \tau \rangle$, $\langle \sigma\tau \rangle$, $\langle \sigma^2\tau \rangle$
1 seul sous-groupe d'ordre 3 : $\langle \sigma \rangle$
1 seul sous-groupe d'ordre 6 : D_6.
On retrouve donc la situation de l'exercice précédent. On note que σ laisse fixe j et ainsi $\mathrm{K}^{\langle\sigma\rangle} = \mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$; τ laisse fixe $\sqrt[3]{2}$ et ainsi $\mathrm{K}^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$; $\sigma\tau$ laisse fixe $j\sqrt[3]{2}$ et ainsi $\mathrm{K}^{\langle\sigma\tau\rangle} = \mathbb{Q}(j\sqrt[3]{2})$; enfin $\mathrm{K}^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(j^2\sqrt[3]{2})$.
On obtient ainsi le treillis suivant :



Exercice 30.
On conserve les notations de l'exercice 25. Le corps $\mathrm{K} = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps des racines de P. Le groupe de Galois de $\mathrm{K}/\mathbb{Q}$ est le groupe diédral D_8. Soient

$$\sigma \left| \begin{array}{ccc} i & \mapsto & -i \\ \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \end{array} \right. ; \tau \left| \begin{array}{ccc} i & \mapsto & i \\ \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} \end{array} \right.$$

Alors $D_8 = \langle \sigma, \tau \rangle = \{\mathrm{id}, \tau^i, \sigma\tau^i, i = 1, \cdots, 4\}$, σ est d'ordre 2, τ est d'ordre 4 et $\sigma\tau\sigma = \tau^{-1}$.
L'ordre d'un sous-groupe H de D_8 divise 8. Si cet ordre vaut 4, on a deux possibilités pour H : ou bien un groupe cyclique, ou bien le groupe de Klein. Les sous-groupes cycliques de D_8 sont :
1 seul sous-groupe d'ordre 1 : $\langle \mathrm{id} \rangle$;
5 sous-groupes d'ordre 2 : σ, $\langle \tau^2 \rangle$, $\langle \tau\sigma \rangle$, $\langle \tau^2\sigma \rangle$, $\langle \tau^3\sigma \rangle$;
1 seul sous-groupe cyclique d'ordre 4 : $\langle \tau \rangle$.
Il nous reste à trouver les groupes de Klein $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Listons les éléments d'ordre 2 : $\sigma, \tau^2, \tau\sigma, \tau^2\sigma, \tau^3\sigma$. On peut noter que σ commute avec τ^2. Ainsi $\langle \tau^2, \sigma \rangle = \{\mathrm{id}, \tau^2, \tau^2\sigma, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. De même τ^2 commute avec $\tau\sigma$ et $\langle \tau^2, \tau\sigma \rangle = \{\mathrm{id}, \tau^2, \tau\sigma, \tau^3\sigma\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ce sont les seuls sous-groupes de Klein de D_8.
On obtient ainsi le treillis des sous-groupes de $G = D_8$:



La correspondance de Galois va nous permettre de déterminer les sous-corps de $\mathbb{Q}(i, \sqrt[4]{2})$.

Tout d'abord $\mathrm{K}^G = \mathbb{Q}$ et $\mathrm{K}^{\langle \mathrm{id} \rangle} = \mathbb{Q}(i, \sqrt[4]{2})$.
On peut chercher un élément primitif pour $\mathrm{K}/\mathbb{Q}$. Testons $z = i + \sqrt[4]{2}$. Il est facile de voir que z n'est fixe par aucun des sous-groupes stricts de G (il suffit de tester avec les sous-groupes d'ordre 2). Ainsi $\mathrm{K} = \mathbb{Q}(i + \sqrt[4]{2})$.

Ensuite τ laisse fixe i et $[\mathrm{K}^{\langle \tau \rangle} : \mathbb{Q}] = 8/4 = 2$. En comparant les degrés, on obtient $\mathbb{Q}(i) = \mathrm{K}^{\langle \tau \rangle}$.

L'élément σ laisse fixe $\sqrt[4]{2}$ et $[\mathrm{K}^{\langle \sigma \rangle} : \mathbb{Q}] = 8/2 = 4$. Comme précédemment, $\mathrm{K}^{\langle \sigma \rangle} = \mathbb{Q}(\sqrt[4]{2})$.

Ensuite $\tau^2(\sqrt[4]{2}) = -\sqrt[4]{2}$. Ainsi $\sqrt{2} = \sqrt[4]{2}$ est fixe par τ^2. On note aussi que σ laisse fixe $\sqrt{2}$ et ainsi $\mathbb{Q}(\sqrt{2}) \subset \mathrm{K}^{\langle\sigma,\tau^2\rangle}$. En comparant les degrés, on a l'égalité $\mathrm{K}^{\langle\tau^2\rangle} = \mathbb{Q}(\sqrt{2})$.

L'élément τ^2 laisse fixe i et $\sqrt{2}$, il laisse donc fixe $i + \sqrt{2}$. En comparant les degrés, $\mathrm{K}^{\langle\tau^2\rangle} = \mathbb{Q}(i + \sqrt{2})$ (voir l'exemple 4.2.7).

L'élément $\tau^2\sigma$ laisse fixe $i\sqrt[4]{2}$. En comparant les degrés, on obtient $\mathrm{K}^{\langle\tau^2\sigma\rangle} = \mathbb{Q}(i\theta)$.

Ensuite $i\sqrt{2} = \sqrt{-2}$, de degré 2 sur $\mathbb{Q}$, est dans le corps $\mathbb{Q}(i, \sqrt{2})$ mais n'est ni dans $\mathbb{Q}(i)$ ni dans $\mathbb{Q}(\sqrt{2})$, c'est donc le corps $\mathrm{K}^{\langle\tau\sigma,\tau^2\rangle}$. On aurait pu aussi noter que $i\sqrt{2}$ est fixe par $\langle\tau\sigma, \tau^2\rangle$.

Les deux corps restant sont un peu plus difficiles.
Regardons $\mathrm{K}^{\langle\tau\sigma\rangle}$. Partons de l'élément primitif $z = i + i\theta$ de $\mathrm{K}/\mathbb{Q}$. Soit la trace de z dans $\mathrm{K}/\mathrm{K}^{\langle\tau\rangle}$:

$$\mathrm{Tr}_{\mathrm{K}/\mathrm{K}^{\langle\tau\rangle}}(z) = z + \sigma\tau(z) = (1 + i)\sqrt[4]{2} \in \mathrm{K}^{\langle\tau\rangle}.$$

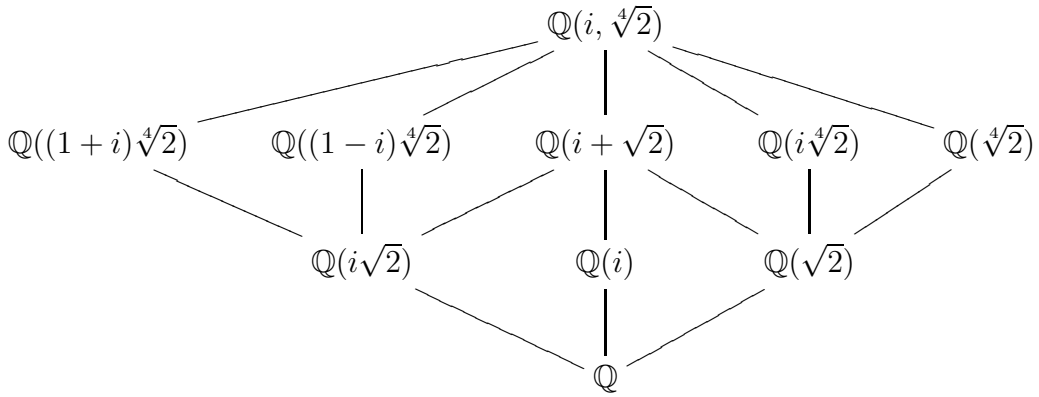
C'est un candidat. Comme $(1 + i)\sqrt[4]{2}$ n'est pas fixe par τ^2 (en effet : $\tau^2((1 + i)\sqrt[4]{2}) = -(1 + i)\sqrt[4]{2}$), on a $(1 + i)\sqrt[4]{2} \notin \mathbb{Q}(i\sqrt{2}) = \mathrm{K}^{\langle\tau\sigma,\tau^2\rangle}$. Donc nécessairement $\mathrm{K}^{\langle\tau\sigma\rangle} = \mathbb{Q}((1 + i)\sqrt[4]{2})$.

Pour finir, il reste $\mathrm{K}^{\langle\tau^{-1}\sigma\rangle}$. Comme précédemment, on regarde

$$\mathrm{Tr}_{\mathrm{K}/\mathrm{K}^{\langle\tau^{-1}\sigma\rangle}}(z) = z + \tau^{-1}\sigma(z) = (1 - i)\sqrt[4]{2} \in \mathrm{K}^{\langle\tau^{-1}\sigma\rangle}.$$

Cet élément n'est pas fixe par τ^2, ainsi $(1-i)\sqrt[4]{2}$ n'est pas dans sous-corps strict de $\mathrm{K}^{\langle\tau^{-1}\sigma\rangle}$: $\mathbb{Q}((1 - i)\sqrt[4]{2}) = \mathrm{K}^{\langle\tau^{-1}\sigma\rangle}$.

On obtient au final le treillis suivant :



À noter que toutes les branches correspondent à des extensions de degré 2.

Pour terminer, on note que $\langle \tau^2 \rangle$ est le seul sous-groupe d'ordre 2 distingué de G. Les sous-groupes d'ordre 4 sont d'indice 2 et sont donc distingués. Ainsi les sous-extensions galoisiennes de K/$\mathbb{Q}$ sont :

(i) les extensions relatives K/F (il y a entre autres 2 groupes de Klein et un groupe cyclique d'ordre 4) ;

(ii) l'extension $\mathbb{Q}(i+\sqrt{2})/\mathbb{Q}$ de groupe de Galois le groupe de Klein ;

(iii) les extensions quadratiques $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$;

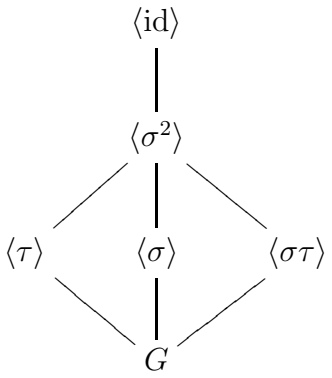
(iv) toutes les sous-extensions relatives strictes F/F′, car elles sont de degré 2.

Exercice 31.
On reprend les notations de l'exercice 26. On a vu que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{H}_8$. Soient les deux $\mathbb{Q}$-automorphismes de K

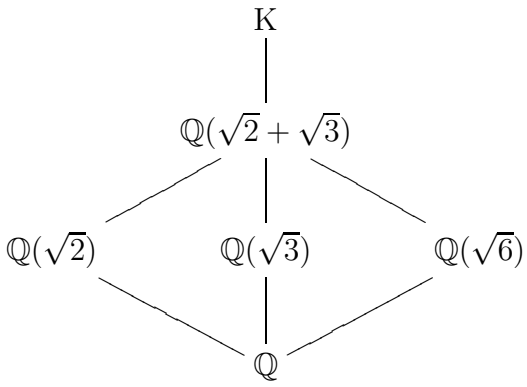
$$\sigma \left| \begin{array}{rcl} \sqrt{3} & \mapsto & \sqrt{3} \\ \sqrt{2} & \mapsto & -\sqrt{2} \\ \alpha & \mapsto & \dfrac{\sqrt{2}(3+\sqrt{3})}{\alpha} \end{array} \right. ; \tau \left| \begin{array}{rcl} \sqrt{3} & \mapsto & -\sqrt{3} \\ \sqrt{2} & \mapsto & \sqrt{2} \\ \alpha & \mapsto & \dfrac{\sqrt{3}\sqrt{2}(2+\sqrt{2})}{\alpha} \end{array} \right.$$

Alors σ et τ sont d'ordre 4, $\sigma^2 = \tau^2$ et un petit calcul montre que $\sigma\tau\sigma^{-1} = \tau^{-1}$. Ainsi $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle = \{\mathrm{id}, \sigma, \sigma^2 = \tau^2, \sigma^{-1}, \tau, \tau^{-1}, \sigma\tau, \sigma\tau^{-1}\}$.

Les sous-groupes de $\mathbb{H}_8$ sont d'ordre divisant 8.
Il y a un seul sous-groupe d'ordre 1 : $\langle \mathrm{id} \rangle$.
Il n'y a qu'un seul sous-groupe d'ordre 2 : $\langle \tau^2 \rangle$.
Il y a 3 sous groupes cycliques d'ordre 4 : $\langle \tau \rangle, \langle \sigma \rangle, \langle \sigma\tau \rangle$.
Pas de sous-groupe de Klein.
On obtient le treillis des sous-groupes de $\mathbb{H}_8$:



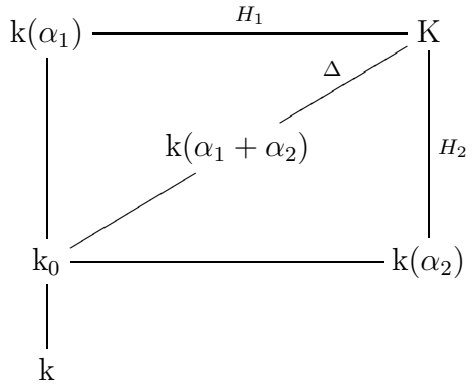
On sait déja que K contient les sous-corps quadratiques de $\mathbb{Q}(\sqrt{2},\sqrt{3})$. La correspondance de Galois nous indique qu'il n'y en a pas plus !
L'élément $\sqrt{2}$ est fixe par τ, ainsi $\mathbb{Q}^{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2})$. L'élement $\sqrt{3}$ est fixe par σ, ainsi $\mathrm{K}^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{3})$ puis, $\sqrt{6}$ est fixe par $\sigma\tau$ et ainsi $\mathrm{K}^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{6})$.
On peut noter aussi que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathrm{K}^{\langle\sigma^2\rangle}$.
Au final, on a le treillis suivant



Toutes les sous-extensions de $\mathrm{K}/\mathbb{Q}$ sont galoisiennes.

Exercice 32.

1) Nous avons le schéma suivant :



où $\mathrm{k}_0 = \mathrm{k}(\alpha_1) \cap \mathrm{k}(\alpha_2)$.
On sait que $\mathrm{Gal}(\mathrm{K}/\mathrm{k}_0) = H_1 \times H_2$ (cf. théorème 4.3.3). Le groupe $\Delta = \mathrm{Gal}(\mathrm{K}/\mathrm{k}(\alpha_1 + \alpha_2))$ est donc un sous-groupe de $H_1 \times H_2$. Soit $\sigma \in \Delta$, $\sigma \neq \mathrm{id}$. Il existe $s_i \in H_i$, tels que $\sigma = s_1 s_2$ (et s_1 et s_2 commutent).
Alors

$$\alpha_1 + \alpha_2 = s_1 s_2(\alpha_1 + \alpha_2) = s_2(\alpha_1) + s_1(\alpha_2), \tag{8}$$

car H_i agit trivialement sur α_i et $s_1 s_2 = s_2 s_1$. Or $s_i \in \mathrm{Gal}(\mathrm{K}/\mathrm{k}(\alpha_i)) \subset \mathrm{Gal}(\mathrm{K}/\mathrm{k})$. Comme $\mathrm{k}(\alpha_i)/\mathrm{k}$ est galoisienne, on a $s_1(\alpha_2) \in \mathrm{k}(\alpha_2)$ et $s_2(\alpha_1) \in \mathrm{k}(\alpha_1)$. Ainsi l'égalité (8) donne

$$s_1(\alpha_2) - \alpha_2 = s_2(\alpha_1) - \alpha_1 \in \mathrm{k}(\alpha_1) \cap \mathrm{k}(\alpha_2) = \mathrm{k}_0.$$

Comme $\sigma \neq \mathrm{id}$, nécessairement s_1 ou s_2 n'est pas réduit à l'identité. Supposons par exemple que c'est s_1.
2) On pose $s = s_1$ et $\Gamma = \langle s \rangle \times H_2$. Soit $\mathrm{F} = \mathrm{K}^{\Gamma}$.
a) Comme $\mathrm{k}_0(\alpha_2) = \mathrm{k}(\alpha_2) = \mathrm{K}^{H_2}$ et que $H_2 \subset \Gamma$, la correspondance de Galois indique que $\mathrm{F} \subset \mathrm{k}_0(\alpha_2)$ et $[\mathrm{k}_0(\alpha_2) : \mathrm{F}] = |\Gamma|/|H_2| = |\langle s \rangle| > 1$, car $s \neq \mathrm{id}$.
b) Soit m' l'ordre de $\langle s \rangle$. Alors m' divise m et donc $(m', p) = 1$. Soit $\beta = \sum_{i=0}^{m'-1} s^i(\alpha_2) \in \mathrm{K}$. Alors comme $s(\alpha_2) = \alpha_2 + a_s$, $a_s \in \mathrm{k}_0$, on en déduit

$$s^i(\alpha_2) = \alpha_2 + i a_s$$

Ainsi,

$$\begin{aligned}\beta &= \alpha_2 + s(\alpha_2) + \cdots + s^{m'-1}(\alpha_2)\\ &= \alpha_2 + \alpha_2 + a_s + \cdots + \alpha_2(m'-1)a_s\\ &= m'\alpha_2 + a_s m'(m'-1)/2\end{aligned}$$

et comme $(m', p) = 1$, on a : $\mathrm{k}_0(\beta) = \mathrm{k}_0(\alpha_2)$.
Or $s(\beta) = \beta$, et ainsi $\beta \in \mathrm{K}^\Gamma = \mathrm{F}$, d'où $\mathrm{k}_0(\beta) \subset \mathrm{F}$, ce qui contredit $[\mathrm{k}_0(\beta) : \mathrm{F}] > 1$.

Exercice 33.
On note tout d'abord que G^p est bien un sous-groupe de G.
Par le théorème de structure des groupes abéliens finis (avec le théorème des restes chinois), il vient

$$G \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z} \times G',$$

avec $n_i \leq n_{i+1}$ et G' d'ordre premier à p. Ainsi

$$G/G^p \simeq (\mathbb{Z}/p\mathbb{Z})^r.$$

Soit $\mathrm{K}_p = \mathrm{K}^{G^p}$. Alors, G étant abélien, $\mathrm{Gal}(\mathrm{K}_p/\mathrm{k}) \simeq G/G^p \simeq (\mathbb{Z}/p\mathbb{Z})^r$.
Soit donc F/k une sous-extension de degré p (cyclique donc) de K/k.
Alors $\mathrm{F} \cap \mathrm{K}_p$ est un sous-corps de F : c'est soit F soit k. Si c'est F, cela signifie que $\mathrm{F} \subset \mathrm{K}_p$ et donc F est fixe par G_p.
Montrons que $\mathrm{K}_p \cap \mathrm{F}$ ne peut pas être égal à k. En effet, sinon cela signifie qu'il y a disjonction linéaire entre F/k et K_p/k. Alors FK_p/k est galoisienne de groupe de Galois isomorphe à $\mathrm{Gal}(\mathrm{F}/\mathrm{k}) \times \mathrm{Gal}(G/G^p) \simeq (\mathbb{Z}/p\mathbb{Z})^{r+1}$. En particulier, cela signifie que G admet un quotient isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{r+1}$, ce qui n'est pas possible.

Exercice 34.
1) Soit θ algébrique sur $\mathbb{C}$. Alors θ est algébrique sur $\mathbb{R}$ et soit $P = \mathrm{Irr}(\theta, \mathbb{R})$. Comme un polynôme réel de degré impair a toujours un zéro dans $\mathbb{R}$, $\deg(P)$ est pair. Ainsi $[\mathbb{R}(\theta) : \mathbb{R}]$ est pair.
2) Soit θ algébrique sur $\mathbb{C}$, mais $\theta \notin \mathbb{C}$. Alors d'après 1), $P = \mathrm{Irr}(\theta, \mathbb{R})$ est de degré pair.
L'extension $\mathbb{R}(\theta)/\mathbb{R}$ n'est peut-être pas galoisienne. Soit alors K le corps des racines de P sur $\mathbb{R}$ (ou encore la clôture normale de $\mathbb{R}(\theta)/\mathbb{R}$). Soit $G = \mathrm{Gal}(\mathrm{K}/\mathbb{R})$. Comme $[\mathbb{R}(\theta) : \mathbb{R}]$ divise $|G|$, le groupe G a un 2-Sylow

H non trivial. Soit $\mathrm{F} = \mathrm{K}^H$. Alors K/K^H est galoisienne de groupe de Galois égal au 2-groupe H et $[\mathrm{F} : \mathbb{R}]$ est impair.
Par le théorème de l'élément primitif, il existe $\alpha \in \mathrm{F}$, tel que $\mathrm{F} = \mathbb{R}(\alpha)$. Or d'après la question 1), $\mathrm{Irr}(\alpha, \mathbb{R})$ est de degré pair, ce qui implique $\alpha \in \mathbb{R}$ et donc $G = H$ est un 2-groupe.
On arrive ensuite aux deux alternatives suivantes.
(i) $\mathrm{K} \cap \mathbb{C} = \mathbb{R}$. Dans ce cas, les extensions $\mathbb{C}/\mathbb{R}$ et $\mathrm{K}/\mathbb{R}$ sont linéairement disjointes et $\mathrm{K}\mathbb{C}/\mathbb{C}$ est galoisienne de groupe de Galois isomorphe à G.
(ii) $\mathrm{K} \cap \mathbb{C} = \mathbb{C}$. Dans ce cas, $\mathbb{C}/\mathbb{R}$ est une sous-extension de $\mathrm{K}/\mathbb{R}$; l'extension $\mathrm{K}/\mathbb{C}$ est galoisienne de groupe de Galois un sous-groupe de G : c'est aussi un 2-groupe.
Dans les deux cas, on obtient une extension $\mathrm{K}'/\mathbb{C}$ galoisienne de groupe de Galois un 2-groupe Δ.
3) Soit $P = X^2 + aX + b \in \mathbb{C}[X]$. Alors P admet toujours au moins une racine dans $\mathbb{C}$ (en extrayant une racine carrée de $a^2 - 4b$). Ainsi tout polynôme $P \in \mathbb{C}[X]$ de degré 2 est réductible : il n'existe pas d'extension de degré 2 de $\mathbb{C}$.
On peut conclure. Comme Δ est un 2-groupe, Δ est résoluble : si Δ est non trivial, il existe un sous-groupe distingué Δ_0 de Δ d'indice 2 : $\Delta/\Delta_0 \simeq \mathbb{Z}/2\mathbb{Z}$. Du point de vue de la théorie de Galois, cela signifie qu'il existe une extension quadratique de $\mathbb{C}$ contenue dans $\mathrm{K}'/\mathbb{C}$. Ainsi Δ est trivial.
On compare ce fait avec les points (i) et (ii) de la question précédente.
Le cas (i) est à exclure car $\Delta = G$ n'est pas trivial. On se trouve donc dans la situation (ii) avec $\mathrm{K} = \mathbb{C}$. Comme $\theta \in \mathrm{K}$, cela implique $\theta \in \mathbb{C}$, d'où une contradiction.

CHAPITRE 5

CORPS FINIS

5.1. La classification

Si k est un corps fini, sa caractéristique est finie, disons p. Alors le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est le sous-corps premier de k, et k est une extension de $\mathbb{F}_p$. Le corps k est un $\mathbb{F}_p$-espace vectoriel, nécessairement de dimension finie $d \geq 1$. Ainsi, $|k| = p^d$. Réciproquement, si $|\mathrm{k}| = p^d$, alors k est une extension de degré d de $\mathbb{F}_p$.

Théorème 5.1.1. — *Soient* k *et* k′ *deux corps finis chacun de cardinal* p^d. *Alors* k *et* k′ *sont* $\mathbb{F}_p$*-isomorphes.*

Démonstration. — Nous commençons par le lemme suivant :

Lemme 5.1.2. — *Soit* k *un corps ayant* p^d *éléments. Alors pour tout* $x \in \mathrm{k}$, $x^{p^d} = x$.

Démonstration. — Le résultat est valable si $x = 0$.
Soit $G = \mathrm{k}^*$ le groupe multiplicatif de k. Le groupe G est fini d'ordre $p^d - 1$ et ainsi pour tout x non nul, $x^{p^d-1} = 1$.

□

Les corps k et k′ sont donc des corps des racines du polynôme $P = X^{p^d} - X \in \mathbb{F}_p[X]$. On conclut avec le corollaire 2.3.13. □

Reste à présent la question de l'existence d'un corps fini à p^d éléments.

Théorème 5.1.3. — *Soit un nombre premier p et soit un entier $d \geq 1$. Alors il existe un corps* k *ayant exactement p^d éléments. Le corps* k *est le corps des racines du polynôme $P = X^{p^d} - X$ dans $\overline{\mathbb{F}_p}$. On le note $\mathbb{F}_{p^d}$.*

Démonstration. — Soit le polynôme $P = X^{p^d} - X \in \mathbb{F}_p[X]$ et soit K le corps des racines (sur $\mathbb{F}_p$) de P dans une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$.
Comme $pgcd(P, D(P)) = pgcd(P, -1) = 1$, le polynôme P est séparable et ainsi le corps K contient au moins p^d éléments, correspondant aux racines de P.
Montrons ensuite que l'ensemble des racines de P forme un corps. Cela va reposer sur l'observation suivante. Puisque le corps K est de caractéristique p, alors pour tout $x, y \in \mathrm{K}$, $(x+y)^p = x^p + y^p$.
Soient α, β deux racines non nulles de P. Alors il est facile de voir que α^{-1} et $-\alpha$ sont aussi des racines de P puis que

$$P(\alpha+\beta) = (\alpha+\beta)^{p^d} - (\alpha+\beta) = \alpha^{p^d} + \beta^{p^d} - (\alpha+\beta) = P(\alpha) + P(\beta) = 0,$$

et

$$P(\alpha\beta) = (\alpha\beta)^{p^d} - \alpha\beta = \alpha^{p^d}\beta^{p^d} - \alpha\beta = \alpha\beta - \alpha\beta = 0.$$

Ainsi l'ensemble des racines de P est un corps (contenant $\mathbb{F}_p$), c'est donc le corps K, et $|\mathrm{K}| = p^d$. □

Définition 5.1.4. — On appelle $\mathbb{F}_{p^n}$ (ou encore $\mathbb{F}_q$, $q = p^n$) le corps fini à p^n éléments.

Remarque 5.1.5. — Le corps $\mathbb{F}_{p^n}$ est l'ensemble des racines du polynôme $X^{p^n} - X$.

***Corollaire 5.1.6* (Sur l'existence d'une clôture algébrique de $\mathbb{F}_p$)** *Le corps $\bigcup_{n\geq 1} \mathbb{F}_{p^{n!}}$ est une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$.*

Exemple 5.1.7. — Soit $\mathrm{k} = \mathbb{F}_2$ et soit $P = X^2 + X + 1 \in \mathrm{k}[X]$. Comme P n'a pas de racine dans k, le polynôme P est irréductible sur k. Soit θ une racine de P dans $\overline{\mathrm{k}}$. Alors $[\mathrm{k}(\theta) : \mathrm{k}] = 2$, $|\mathrm{k}(\theta)| = 2^2$ et donc $\mathrm{k}(\theta) = \mathbb{F}_4$. On obtient aussi que tout élément x de $\mathbb{F}_4$ s'écrit de manière unique : $x = a + b\theta$, avec $a, b \in \{0, 1\}$.

5.2. L'automorphisme de Frobenius

Fixons une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$. Soit $q = p^d$ une puissance du nombre premier p.
Soit φ_q l'application

$$\begin{array}{rccc} \varphi_q : & \overline{\mathrm{k}} & \to & \overline{k} \\ & x & \mapsto & x^q. \end{array}$$

Proposition 5.2.1. — *1) L'application φ_q est un $\mathbb{F}_q$-automorphisme de $\overline{\mathrm{k}}$.*
2) On a : $\varphi_{p^d} = \varphi_p^d$.
3) Soit $\mathrm{k}/\mathbb{F}_p$ une extension finie ; $|\mathrm{k}| = p^d = q$ ($\mathrm{k} = \mathbb{F}_q$). La restriction de φ_p à k est un $\mathbb{F}_p$-automorphisme de k d'ordre d.

Démonstration. — 1) Le fait que $(x+y)^q = x^q + y^q$ montre que φ_q est un morphisme de corps et la restriction de φ_q à $\mathbb{F}_q$ est bien l'identité (d'après la remarque 5.1.5).

2) C'est immédiat : $\varphi_p^d(x) = x^{p^d} = x^q = \varphi_q(x)$.

3) On s'appuye sur le lemme suivant

Lemme 5.2.2. — *Soit un corps fini k. Alors le groupe k^* est cyclique.*

Démonstration. — Soit le groupe $G = (\mathrm{k}^*, \cdot)$. C'est un groupe abélien fini. Par le théorème de structure des groupes abéliens finis, il existe des entiers $a_1 | \cdots | a_n$ tels que $G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$. En particulier, tout élément x de G vérifie $x^{a_n} = 1$ et est donc racine de $X^{a_n} - 1$. Or dans un corps k, un polynôme Q non nul a au plus $\deg(Q)$ racines (utiliser la division euclidienne dans $\mathrm{k}[X]$) et donc nécessairement $G \simeq \mathbb{Z}/a_n\mathbb{Z}$. □

Soit ε un générateur de k^*. Alors $\varphi_p^i(\varepsilon) = \varepsilon^{p^i}$. Comme ε est d'ordre $q-1$, on voit que le plus petit entier i tel que $\varphi_{p^i}(\varepsilon) = \varepsilon$ vérifie $p^i = q$, ou encore $i = d$. Comme $\mathrm{k} = \{0\} \cup \langle\varepsilon\rangle$, on conclut que φ_p est bien d'ordre d. □

Corollaire 5.2.3. — *Le corps $\mathbb{F}_q$ est exactement l'ensemble des points fixes de $\overline{\mathrm{k}}$ sous l'action de φ_q.*

Démonstration. — Un élément $x \in \overline{\mathrm{k}}$ est fixe sous l'action de φ_q si et seulement si $\varphi_q(x) = x$, ce qui équivaut à $x^q = x$, ou encore, x est

racine de $X^q - X$, ce qui est exactement la caractérisation de $\mathbb{F}_q$ (voir la remarque 5.1.5) □

Définition 5.2.4. — L'élément φ_p est appelé automorphisme de Frobenius.

Proposition 5.2.5. — *Soient deux extensions finies* $\mathrm{k}/\mathbb{F}_p$ *et* $\mathrm{k}'/\mathbb{F}_p$. *Si* $|\mathrm{k}| = p^d$ *et* $|\mathrm{k}'| = p^{d'}$, *alors* $\mathrm{k} \subset \mathrm{k}'$ *si et seulement si* $d|d'$.

Démonstration. — Supposons $d' = nd$ et posons $q = p^d$ et $q' = p^{d'}$. Alors $\varphi_{q'} = \varphi_q^{nd}$. Ainsi si x est stable sous l'action de φ_q, alors x est également stable sous l'action de $\varphi_{q'}$ et on conclut avec le corollaire 5.2.3.
Supposons $\mathrm{k} \subset \mathrm{k}'$. L'automorphisme de Frobenius φ_p restreint à k' est d'ordre d' et φ_p restreint à k est d'ordre d. Ainsi $\left((\varphi_p)_{|\mathrm{k}}\right)^{d'} = \mathrm{id}$ ce qui implique $d|d'$. □

Exemple 5.2.6. — Le corps $\mathbb{F}_{2^{12}}$ a pour sous-corps le treillis suivant :

$$\begin{array}{ccccc} \mathbb{F}_8 & \overset{2}{\text{———}} & \mathbb{F}_{64} & \overset{2}{\text{———}} & \mathbb{F}_{4096} \\ {\scriptstyle 3}\big| & & {\scriptstyle 3}\big| & & {\scriptstyle 3}\big| \\ \mathbb{F}_2 & \underset{2}{\text{———}} & \mathbb{F}_4 & \underset{2}{\text{———}} & \mathbb{F}_{16} \end{array}$$

Théorème 5.2.7. — *Soient* $\mathrm{k} = \mathbb{F}_q$ *un corps fini et* K/k *une extension de degré* n. *Alors* K/k *est galoisienne et le groupe de Galois* $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$ *est engendré par le Frobenius* φ_q. *En particulier* $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$ *est cyclique d'ordre* n.

Démonstration. — Soit $\mathrm{k} = \mathbb{F}_q$ et soit K/k une extension finie de degré n (à noter que $\mathrm{K} = \mathbb{F}_{q^n}$). On sait déja que l'extension K/k est séparable (voir le corollaire 3.4.8).
Le corps K est le corps des racines du polynôme $X^{q^n} - X$, et ainsi K/k est normale.
Au total l'extension K/k est donc bien galoisienne. Le groupe de Galois de K/k est un groupe d'ordre n.
Maintenant on a un élément privilégié de $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$: l'automorphisme de Frobenius φ_q. Si $q = p^d$, alors $|\mathrm{K}| = p^{nd}$. D'après la proposition 5.2.1,

la restriction de φ_p à K est d'ordre nd c'est-à-dire

$$\varphi_q = \varphi_{p^d} = \varphi_p^d$$

est d'ordre n. Comme $|\mathrm{Gal(K/k)}| = n$, on conclut : $\mathrm{Gal(K/k)} = \langle \varphi_q \rangle$. □

5.3. Polynômes primitifs

Soit k un corps fini ayant p^d éléments. Le groupe k^* est engendré par un élément ε. En particulier, $\mathrm{k} = \mathbb{F}_p(\varepsilon)$. L'élément ε est donc de degré d sur $\mathbb{F}_p$ et $\mathrm{Irr}(\varepsilon, \mathbb{F}_p)$ est de degré d.

Définition 5.3.1. — Un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré d dont une racine est d'ordre $p^d - 1$ dans $\overline{\mathrm{k}}^*$, est appelé polynôme primitif de degré d.

Remarque 5.3.2. — Si P est primitif de degré d, alors toutes les racines de P sont d'ordre $p^d - 1$ dans $\overline{\mathrm{k}}^*$ (on passe d'une racine à l'autre via un automorphisme).

Exemple 5.3.3. — Sur $\mathbb{F}_3[X]$, le polynôme $P = X^2 + 1$ est irréductible (il n'a pas de racine dans $\mathbb{F}_3$), mais n'est pas primitif. En effet si θ est une racine de P dans $\overline{\mathrm{k}}$, alors $\theta^2 = -1$, $\theta^4 = 1$ et donc θ est d'ordre 4. Or ici $\mathbb{F}_3(\theta) = \mathbb{F}_9$ et $\mathbb{F}_9^*$ est cyclique d'ordre 8.
Par contre le polynôme $P = X^2 - X - 1$ est primitif (sur $\mathbb{F}_3$). Si α est une racine de P, alors $\alpha^2 = \alpha + 1$ et $\alpha^4 = -1$. L'ordre de α divise 8, il est donc égal à 8. Ainsi $\mathbb{F}_9^* = \langle \alpha \rangle$.

Proposition 5.3.4. — *Le nombre de polynômes primitifs de degré d sur $\mathbb{F}_p$ est exactement $\varphi(p^d - 1)/d$, où φ est la fonction d'Euler.*

Démonstration. — Soit ε un générateur de k. Dans k^*, ε est d'ordre $p^d - 1$ et ε^i est également d'ordre $p^d - 1$ si et seulement si $pgcd(i, p^d - 1) = 1$. Il y a donc $\varphi(p^d - 1)$ éléments de k^* qui engendrent k^* soit au total $\varphi(p^d - 1)/d$ polynômes primitifs. □

5.4. Groupe de Galois sur $\mathbb{Q}$ et réduction modulo p

Dans cette section nous allons montrer comment la factorisation modulo p d'un polynôme $P \in \mathbb{Z}[X]$ peut permettre de déterminer le groupe de Galois de P.

5.4.1. Rappels. —

5.4.1.1. Sur le groupe symétrique. — Soit $n \geq 2$ et soit S_n le groupe symétrique sur n éléments. On rappelle l'homomorphisme *signature* ε défini sur S_n et à valeurs dans ± 1 :

$$\begin{array}{rccc} \varepsilon : S_n & \longrightarrow & \langle \pm 1 \rangle & \\ \sigma & \mapsto & \epsilon(\sigma) = \displaystyle\prod_{1 \leq i < j \leq n} \frac{X_{\sigma(i)} - X_{\sigma(j)}}{X_i - X_j}. \end{array}$$

Le groupe alterné A_n est défini comme le noyau de ε : il est d'ordre $n!/2$. On rappelle que pour $n \geq 5$, le groupe A_n est simple.
Tout élément $\sigma \in S_n$ s'écrit comme produit de transpositions τ_i : $\sigma = \prod_{i=1}^{k} \tau_i$. On rappelle alors que $\epsilon(\sigma) = (-1)^k$.

Proposition 5.4.1. — *Soit G un sous-groupe transitif de S_n contenant une transposition et un $(n-1)$-cycle. Alors $G = S_n$.*

Démonstration. — Quitte à reprendre la numérotation, supposons que le $(n-1)$-cycle soit le cycle $(1\ 2 \cdots n-1)$. Soit alors la transposition $(i\ j) \in G$. Il existe $\sigma \in G$ tel que $\sigma(i) = n$. Alors un petit calcul montre que $\sigma(i\ j)\sigma^{-1} = (k\ n)$ pour $k = \sigma(j)$. Pour $k \leq n-2$, on obtient ensuite $(1\ 2 \cdots n-1)(k\ n)(1\ 2 \cdots n-1)^{-1} = (k+1\ n)$ et pour $k = n-1$, cette conjugaison de $(n-1\ n)$ donne la transposition $(1\ n)$. Ainsi G contient l'ensemble des transpositions $(k\ n)$, $k = 1, \cdots, n$, et on conclut en se rappelant que celles-ci engendrent S_n. □

Proposition 5.4.2. — *Soit p un nombre premier et soit G un sous-groupe de S_p. Si G contient un p-cycle et une transposition alors $G = S_p$.*

Démonstration. — Quitte à reprendre la numérotation on peut supposer que G contient la transposition $(1\ 2)$ et que le p-cycle est de la forme $(1\ 2 \cdots p)$ (pour ce dernier, on commence par prendre une bonne puissance pour avoir $(1\ 2\ \cdots)$ et on reprend ensuite la numérotation des $p-2$

lettres restantes). Mais alors $(1\ 2\cdots p)^k(1\ 2)(1\ 2\cdots p)^{-k} = (k\ k+1)$, et l'on sait que ces transpositions engendrent S_p. □

Remarque 5.4.3. — Rappelons que si G est un sous-groupe de S_p et que p divise l'ordre de G alors G contient un p-cycle (ici p est un nombre premier).

***Proposition 5.4.4* (Jordan)**. — *Soit G un sous-groupe transitif de S_n. Supposons que G contienne un 3-cycle. Si n n'est pas premier, supposons de plus que G contienne un $(n-1)$-cycle. Alors G est soit A_n soit S_n.*

Démonstration. — Admise. □

5.4.1.2. Sur le discriminant d'un polynôme. — Commencçons par une définition.

Définition 5.4.5. — Soit $P \in \mathbb{Q}[X]$. On appelle discriminant de P, et on note $\mathrm{disc}(P)$, la quantité :

$$\mathrm{disc}(P) = \prod_{i<j}(\theta_i - \theta_j)^2,$$

où les θ_i sont les racines de P dans $\mathbb{C}$.

On observe alors que $\mathrm{disc}(P) = 0$ si et seulement si P a au moins une racine multiple.

Proposition 5.4.6. — *Soit $P \in \mathbb{Q}[X]$ unitaire de degré n. Alors $\mathrm{disc}(P) = (-1)^{n(n-1)/2}P'(\theta_1)\cdots P'(\theta_n)$, où $P' = D(P)$ est le polynôme dérivé. De plus $\mathrm{disc}(P) \in \mathbb{Q}$. En particuler, si $P \in \mathbb{Z}[X]$ alors $\mathrm{disc}(P) \in \mathbb{Z}$.*
Si de plus P est irréductible, il vient $\mathrm{disc}(P) = (-1)^{n(n-1)/2}N_{\mathrm{K}/\mathbb{Q}}P'(\theta)$, où $\mathrm{K} = \mathbb{Q}(\theta)$.

Démonstration. — Montrons tout d'abord l'identité :

$$\begin{aligned}
\mathrm{disc}(P) &= \textstyle\prod_{i<j}(\theta_i - \theta_j)^2 \\
&= (-1)^{n(n-1)/2}\textstyle\prod_{i\neq j}(\theta_i - \theta_j) \\
&= (-1)^{n(n-1)/2}\textstyle\prod_{i=1}^{n}\prod_{j=1,j\neq i}^{n}(\theta_i - \theta_j) \\
&= (-1)^{n(n-1)/2}P'(\theta_1)\cdots P'(\theta_n).
\end{aligned}$$

Soit $\mathbb{Q}_P = \mathbb{Q}(\theta_1, \cdots, \theta_n)$. Alors l'extension $\mathbb{Q}_P/\mathbb{Q}$ est galoisienne (c'est le corps des racines de P). Comme $\mathrm{disc}(P) = \pm P'(\theta_1)\cdots P'(\theta_n)$, il vient que $\mathrm{disc}(P)$ est fixe par l'action de tout automorphisme σ de $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$; ainsi, $\mathrm{disc}(P) \in \mathbb{Q}$. Mais en fait on a mieux lorsque $P \in \mathbb{Z}[X]$ unitaire : comme pour $i = 1, \cdots, n$, on a $P'(\theta_i) \in \mathbb{Z}[\theta_1, \cdots, \theta_n]$, il vient alors $\mathrm{disc}(P) \in \mathbb{Q} \cap \mathbb{Z}[\theta_1, \cdots, \theta_n]$, et donc $\mathrm{disc}(P) \in \mathbb{Z}$ par le théorème 4.4.7. La dernière assertion est évidente. □

Exemple 5.4.7. — On a $\mathrm{disc}(X^2 + aX + b) = a^2 - 4b$. En effet, si l'on note par θ_1 et θ_2 les racines de P, il vient :

$$\begin{aligned} \mathrm{disc}(X^2 + aX + b) &= (\theta_1 - \theta_2)^2 \\ &= \theta_1^2 + \theta_2 - 2\theta_1\theta_2 \\ &= -a(\theta_1 + \theta_2) - 2b - 2\theta_1\theta_2 \\ &= a^2 - 4b. \end{aligned}$$

Exemple 5.4.8. — Soit $P = X^3 + aX + b$. Alors $\mathrm{disc}(P) = -4a^3 - 27b^2$. Voir l'exercice 43.

Soit $P \in \mathbb{Z}[X]$ irréductible de degré n et soit $\mathbb{Q}_P$ le corps des racines de P sur $\mathbb{Q}$. L'extension $\mathbb{Q}_P/\mathbb{Q}$ est galoisienne de groupe de Galois G, et G s'identifie alors à un sous-groupe transitif de S_n (voir l'exercice 21 du chapitre 3).

Proposition 5.4.9. — *Sous les notations précédentes, le groupe G est un sous-groupe de A_n si et seulement si* $\mathrm{disc}(P) \in \mathbb{Z}^2$.

Démonstration. — Soit $A = \prod_{1 \leq i < j \leq n}(\theta_i - \theta_j)$. Observons que $A^2 = \mathrm{disc}(P)$. Soit $\tau \in S_n$ une transposition. On vérifie que $\tau(A) = -A$. Et ainsi, si $\sigma = \prod_k \tau_k$, il vient $\sigma(A) = (-1)^k A = \epsilon(\sigma)A$.
Supposons $G \subset A_n$. Alors pour tout $\sigma \in G$ on a $\sigma(A) = A$, et ainsi par la correspondance de Galois, $A \in \mathbb{Q}$ (en fait $\mathbb{Z}$), d'où $\mathrm{disc}(P) \in \mathbb{Z}^2$.
Réciproquement. Soit $\sigma \in G$ mais non dans A_n. Alors $\sigma(A) = -A$ et par conséquent $A \notin \mathbb{Q}$ (en fait dans $\mathbb{Z}$), ce qui implique $\mathrm{disc}(P) \notin \mathbb{Z}^2$. □

Avant d'aller plus loin donnons une première conséquence.

Proposition 5.4.10. — *Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré 3. Soit $\mathbb{Q}_P$ le corps des racines de P. Alors*

- *si* $\mathrm{disc}(P)$ *est un carré de $\mathbb{Q}$, il vient* $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ *;*

– *si* $\mathrm{disc}(P)$ *n'est pas un carré de* $\mathbb{Q}$*, il vient* $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q}) \simeq S_3$.

Démonstration. — On sait que 3 divise $|\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})|$ et que $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q}) \hookrightarrow S_3$. Le résultat découle alors de la proposition 5.4.9. □

5.4.2. Réduction modulo p. — Soit $P \in \mathbb{Z}[X]$ unitaire. Les réductions modulo p de P quand le nombre premier p varie peuvent permettre de montrer que P est irréductible. Mais en fait, ces réductions peuvent donner plus de renseignements comme le montre le résultat principal de cette section.

Théorème 5.4.11. — *Soit $P \in \mathbb{Z}[X]$ irréductible unitaire et soit un nombre premier p. Soit $\bar{P}_1 \cdots \bar{P}_g$ la factorisation de P dans $\mathbb{F}_p[X]$, où les polynômes $\bar{P}_i \in \mathbb{F}_p[X]$ sont irréductibles de degré n_i. Supposons que les $\bar{P}_i$ sont deux à deux premiers entre eux (ce qui est équivalent au fait que $p \nmid \mathrm{disc}(P)$). Alors le groupe de Galois $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$ contient un élément $g \in S_n$ s'écrivant $g = [n_1][n_2]\cdots[n_g]$ comme produit de cycles $[n_i]$ de longueurs n_i, deux à deux à supports disjoints.*

Notons par $\theta_1, \cdots, \theta_n \in \mathbb{C}$ les racines de P, et soit l'anneau $A := \mathbb{Z}[\theta_1, \cdots, \theta_n]$. Soit p un nombre premier et soit l'idéal pA. Nous allons commencer par montrer la proposition suivante.

Proposition 5.4.12. — *On a $pA \neq A$.*

Démonstration. — Supposons que $pA = A$. Il existe alors $\alpha \in A$ tel que $p\alpha = 1$. En passant à la norme on obtient $\mathrm{N}_{\mathbb{Q}_P/\mathbb{Q}}(p)\mathrm{N}_{\mathbb{Q}_P/\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}_P/\mathbb{Q}}(1) = 1$. Comme $p^n | \mathrm{N}_{\mathbb{Q}_P/\mathbb{Q}}(p)$, et que $\mathrm{N}_{Q_P/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ (d'après le théorème 4.4.7), on arrive à une absurdité. □

Continuons la preuve du théorème 5.4.11.
Soit $\mathfrak{M}$ un idéal maximal de A contenant l'idéal pA et soit $\varphi : A \to A/\mathfrak{M}$ l'homomorphisme de réduction. Pour $i = 1, \cdots, n$, posons $x_i = \varphi(\theta_i)$. L'idéal $\mathbb{Z} \cap \mathfrak{M}$ est un idéal premier de $\mathbb{Z}$ contenant p, il est donc égal à $p\mathbb{Z}$. Comme P est unitaire, chaque x_i vérifie une relation non triviale sur $\mathbb{F}_p$, ce sont des éléments algébriques qui annulent en fait $\bar{P} := P(\mathrm{mod}\ p) \in \mathbb{F}_p[X]$. Ainsi $A/\mathfrak{M}$ est un corps fini, donc de la forme $\mathbb{F}_{p^f}$ pour un certain entier f. Remarquons que les x_i engendrent A/$\mathfrak{M}$

ou encore que $\mathbb{F}_{p^f} = \mathbb{F}_p(x_1, \cdots, x_n)$, mais aussi que chaque $\mathrm{Irr}(x_i, \mathbb{F}_p)$ divise $\bar{P}$.
Nous pouvons déjà montrer la proposition suivante :

Proposition 5.4.13. — *Ecrivons $\bar{P} = \bar{P}_1 \cdots \bar{P}_g$, avec $\bar{P}_i \in \mathbb{F}_p[X]$ irréductibles. Alors les $\bar{P}_i$ sont deux à deux premiers entre eux si et seulement si, $p \nmid \mathrm{disc}(P)$.*

Démonstration. — Observons tout d'abord que dans $\mathbb{F}_{p^f}$ il vient $\bar{P} = \prod_{i=1}^{n}(X - x_i)$. En particulier, les x_i sont exactement les racines des polynômes $\bar{P}_j$ dans $\overline{\mathbb{F}_p}$. La proposition se déduit alors tout simplement de l'identité suivante :

$$\mathrm{disc}(P) \pmod p = \varphi(\mathrm{disc}(P)) = \pm \prod_{i \neq j}(x_i - x_j),$$

et en se rappelant que les polynômes $\bar{P}_j$ sont séparables (voir le corollaire 3.4.8). □

Obervons maintenant que G agit sur A et notons par $D = \{\sigma \in G,\ \sigma(\mathfrak{M}) \subset \mathfrak{M}\}$. L'ensemble D est un sous-groupe de G, il est appelé le groupe de décomposition de $\mathfrak{M}$. Par restriction, il vient que tout élément σ de D peut être vu comme un élément de $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$. Plus précisément notons par $\psi : D \to \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ ce morphisme de restriction. Nous avons alors le point clef suivant.

Proposition 5.4.14. — *Le morphisme ψ est surjectif.*

Démonstration. — Soit $0 \neq x \in \mathbb{F}_{p^f}$ tel que $\mathbb{F}_{p^f} = \mathbb{F}_p(x)$.
Pour $\sigma \in G$, remarquons que $\sigma^{-1}(\mathfrak{M})$ est un idéal maximal de A contenant $p\mathbb{Z}$. Notons alors $\mathfrak{M}_1, \cdots, \mathfrak{M}_g$, l'ensemble de tels idéaux maximaux avec la convention que $\mathfrak{M}_1 = \mathfrak{M}$ et qu'ils sont deux à deux distincts (en particulier $g \leq |G - D|$). Comme pour $i \neq j$, $\mathfrak{M}_i + \mathfrak{M}_j = A$, le théorème des restes chinois garantit l'existence d'un élément $y \in A$ tel que

$$\begin{cases} y \equiv x & (\bmod\ \mathfrak{M}_1) \\ y \equiv 0 & (\bmod\ \mathfrak{M}_i), i = 2, \cdots, g \end{cases}$$

Soit ensuite le polynôme $R = \prod_{\sigma \in G} (X - \sigma(y))$. On a $R(y) = 0$, ce qui implique $\varphi(R(y)) = 0$ ou encore que $\overline{R}(x) = 0$, où $\overline{R} := R(\text{mod } \mathfrak{M})$. Or comme pour tout $\sigma \in G - D$, il vient $\sigma(y) \in \mathfrak{M}$, on a donc

$$\bar{R} = \prod_{\sigma \in D} \big(X - \psi(\sigma)(x)\big) \prod_{\sigma \in G-D} X.$$

Comme $x \neq 0$, il vient que $\text{Irr}(x, \mathbb{F}_p)$ divise $\bar{R}$. La conclusion est alors immédiate. Soit $\bar{\sigma} \in \text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$: l'élément $\bar{\sigma}$ est déterminé par $\bar{\sigma}(x)$. Or $\overline{\sigma}(x)$ est une racine de $\text{Irr}(x, \mathbb{F}_p)$: il existe $\sigma \in D$ tel que $\psi(\sigma)(x) = \bar{\sigma}(x)$, ce qui signifie exactement que ψ est surjectif. □

Jusqu'à présent nous n'avons pas utiliser la condition $p \nmid \text{disc}(P)$. Supposons donc maintenant que $p \nmid \text{disc}(P)$. Alors le polynôme $\bar{P}$ s'écrit $\bar{P}_1 \cdots \bar{P}_g$, avec $\bar{P}_i \in \mathbb{F}_p[X]$ irréductibles et premiers deux à deux entre eux. Soit φ_p l'élément de Frobenius engendrant le groupe de Galois $\text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$. Notons par $x_{i,1}, \cdots, x_{i,n_i}$ les racines de $\bar{P}_i$, où $n_i = \deg \bar{P}_i$. Pour chaque entier i, l'action du morphisme de Frobenius φ_p restreint à l'extension $\mathbb{F}_p(x_{i,1}, \cdots, x_{i,n_i})/\mathbb{F}_p$ est cyclique de degré n_i, et correspond à un cycle de longueur $[n_i]$ mettant en jeu les racines $x_{i,j}$, $j = 1, \cdots, n_i$. D'après la propostion 5.4.14, φ_p se relève en un $\sigma \in G$. Comme les racines de $\bar{P}$ sont simples, il y a une correspondance bijective entre les θ_i et les x_i. Ainsi, à un ensemble $\{x_{i,1}, \cdots, x_{i,n_i}\}$ de racines de $\bar{P}_i$ correspond un ensemble $\{\theta_{i,1}, \cdots, \theta_{i,n_i}\}$ de racines de P, et par conséquent le Frobenius φ_p se relève en $\sigma \in D$ tel que $\sigma_{|\{\theta_{i,1}, \cdots, \theta_{i,n_i}\}}$ correspond à un cycle de longueur $[n_i]$, et les cycles obtenus sont bien à support disjoints. Ceci achève la preuve du théorème 5.4.11.

Exemple 5.4.15. — Soit le polynôme $P = X^5 + 20X + 16$, et soit $G = \text{Gal}(\text{K}_P/\mathbb{Q})$. Tout d'abord, on note les réductions suivantes

(i) le polynôme P est irréducible modulo 3 ;

(ii) on a $P \equiv (X-4)(X-5)(X^3 + 2X^2 + 5X + 5) \text{ (mod } 7)$, où $X^3 + 2X^2 + 5X + 5$ est irréductible sur $\mathbb{F}_7$.

Ainsi, par (i) le polynôme P est irréductible. Un calcul montre (voir exercice 43) que $\text{disc}(P) = 2^{16}5^6$. Par conséquent $G \subset A_5$ par la proposition 5.4.9. D'autre part le point (ii) associé au théorème 5.4.11 montre que G

contient un 3-cycle. Avec la proposition 5.4.4 on obtient finalement que $G = A_5$.

5.5. Exercices

Pour chaque nombre premier p, on se fixe une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$.

5.5.1. Énoncés. —

Exercice 35. — *Montrer que tout anneau intègre fini est un corps.*

Exercice 36. — *Établir la table d'addition et de multiplication de* $\mathbb{F}_4$.

Exercice 37. — *Soit le corps fini* $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, *avec* α *vérifiant* $\alpha^2 + \alpha + 1 = 0$. *Exprimer les éléments* $1/\alpha$ *et* $1/(\alpha^4 + 1)$ *dans la* $\mathbb{F}_2$*-base* $(1, \alpha)$.

Exercice 38. —
1) Définir $\mathbb{F}_9$.
2) Trouver les polynomes irréductibles de degré 2 sur $\mathbb{F}_3$.
3) Trouver les polynomes primitifs de degré 2 sur $\mathbb{F}_3$.
4) Soient $P = X^2 + X - 1$ *et* α *une racine de* P.
On définit $Z_\alpha : \{1, \cdots, 7\} \to \{1, \cdots, 7\}$ *par* $\mathbb{Z}_\alpha(i) = j$ *où* $1 - \alpha^i = \alpha^j$.
Déterminer $Z_\alpha(i)$, $i = 1, \cdots, 7$. *En déduire :*

- *La simplification de* $(1 + \alpha + \alpha^6) + \alpha(1 - \alpha^6)^4$
- *La factorisation sur* $\mathbb{F}_9$ *de* $X^3 + 1 + \alpha^7$.

Exercice 39. — *Soit* $\mathbb{F}_{3^n}$ *le corps des racines (sur* $\mathbb{F}_3$*) de* $X^5 + X^2 + 2X + 1$. *Déterminer* n.

Exercice 40. — *1) Montrer que pour* p *premier,* $n \geq 1$,

$$X^{p^n} - X = \prod_{Q \in S} Q,$$

où S *est l'ensemble constitué des polynômes irréductibles de* $\mathbb{F}_p[X]$ *unitaires dont le degré divise* n.
2) Soit $P_p(d)$ *le nombre de polynômes irréductibles de degré* d *sur* $\mathbb{F}_p$.
Montrer alors la formule suivante :

$$p^n = \sum_{d|n} d.P_p(d).$$

Calculer $P_2(1)$, $P_2(2)$, $P_2(4)$ *et* $P_2(8)$.

Exercice 41. — *Soit* $\mathbb{F}_q$ *le corps à* q *éléments. On suppose* q *impair.*
1) Montrer que tout élément de $\mathbb{F}_q$ *est somme de deux carrés.*
2) Montrer que -1 *est un carré dans* $\mathbb{F}_q$ *si et seulement si* $q \equiv 1 \ (mod\ 4)$.

Exercice 42. — *Soit* p *un nombre premier. On veut montrer que* $P = X^p - X - 1$ *est irréductible sur* $\mathbb{Q}$.
1) On considère $\Psi : \mathbb{Z}[X] \mapsto \mathbb{F}_p[X]$, *l'homomorphisme de réduction modulo* p *et soit* $f = X^p - X - 1$ *l'image* $\Psi(P)$ *de* P *dans* $\mathbb{F}_p[X]$. *Soit* α *une racine de* f *dans* $\overline{\mathbb{F}_p}$.
a) Calculer $f(a + \alpha)$ *pour tout* $a \in \mathbb{F}_p$.
b) En déduire le corps K *des racines de* f.
2) a) Quelle est la factorisation de f *dans* $\overline{\mathbb{F}_p}[X]$ *?*
b) Montrer qu'il est impossible d'avoir $f = gh$ *avec* $deg(g), deg(h) \geq 1$, $f, g \in \mathbb{F}_p[X]$.
3) En déduire que P *est irréductible sur* $\mathbb{Q}$.

Exercice 43. — *Dans cet exercice, les polynômes sont supposés irréductibles.*
1) Montrer que $\mathrm{disc}(X^4 + aX^2 + b) = 16b(a^2 - 4b)^2$.
2) Plus généralement, montrer que (pour $n \geq 1$*)*

$$\mathrm{disc}(X^{2n} + aX^n + b) = (-1)^n n^{2n} b^{n-1}(-a^2 + 4b)^n.$$

3) Soit $n \geq 2$. *Montrer que*

$$\mathrm{disc}(X^n + aX + b) = (-1)^{n(n-1)/2} \left((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\right).$$

Exercice 44. — *Suite de l'exercice 42. Soit* $p > 2$ *un nombre premier et soit* $P = X^p - X - 1 \in \mathbb{Z}[X]$.
1) Que vaut $\mathrm{disc}(P)$ *? En déduire que* $2 \nmid \mathrm{disc}(P)$.
2) Soit $\theta \in \overline{\mathbb{F}_2}$ *une racine de* $X^2 + X + 1 = 0$.
a) Calculer les puissances de θ.
b) On suppose $p \equiv 2 (\mathrm{mod}\ 3)$. *Que peut-on en déduire de la factorisation de* P *dans* $\mathbb{F}_2[X]$ *?*
3) Soit $\mathbb{Q}_P$ *le corps des racines de* P *sur* $\mathbb{Q}$. *Déterminer* $\mathrm{Gal}(\mathrm{K}_P/\mathbb{Q})$ *quand* $p = 5$ *et* $p = 11$.

5.5.2. Solutions. —

Exercice 35.

Soit A un anneau intègre et fini. Il nous faut montrer que tout élément non-nul x de A admet un inverse.

Pour $x \in$ A non-nul, considérons l'application

$$\begin{array}{rccc} \varphi_x : & \mathrm{A} & \to & \mathrm{A} \\ & y & \mapsto & xy. \end{array}$$

Comme A est fini, on a l'équivalence entre les trois assertions suivantes : (i) φ_x est bijective ; (ii) φ_x est injective ; (iii) φ_x est surjective.

Montrons que φ_x est injective : soient y et z dans A tels que $\varphi_x(y) = \varphi_x(z)$, alors $x(y-z) = 0$, et comme x est non-nul et que A est intègre on en déduit que $y = z$. Par conséquent φ_x est surjective et l'élément 1 admet donc un antécédent : il existe $x' \in$ A tel que $\varphi_x(x') = 1$, ou encore que $xx' = 1$, ce qui montre que x admet un inverse.

Exercice 36.

Le corps $\mathbb{F}_4$ est l'extension quadratique de $\mathbb{F}_2$. Elle est engendrée par un élément α de degré 2 sur $\mathbb{F}_2$. Or sur $\mathbb{F}_2$, il n y a qu'un seul polynôme irréductible unitaire de degré 2 : $P = X^2 + X + 1$. Ainsi α vérifie la relation $\alpha^2 + \alpha + 1 = 0$ et tout élément de $\mathbb{F}_4$ sécrit de manière unique $a + b\alpha$, avec $a, b \in \{0, 1\}$. On obtient les tables suivantes :

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Exercice 37.

On a la relation $\alpha^2+\alpha=-1=1$. On la divise par α, pour obtenir $1/\alpha=\alpha+1$.
Ensuite $\alpha\in\mathbb{F}_4$ et $\mathbb{F}_4$ est l'ensemble des racines de X^4-X. Ainsi $\alpha^4=\alpha$ (en effet : $\alpha^4=(\alpha+1)^2=\alpha^2+1=\alpha$) et $1+\alpha^4=1+\alpha$. Comme $1=\alpha(1+\alpha)$, on obtient au final $1/(1+\alpha^4)=1/(\alpha+1)=\alpha$.

Exercice 38. 1) Le corps $\mathbb{F}_9$ est l'unique corps à 9 éléments (à isomorphisme prés) : c'est l'extension de degré 2 de $\mathbb{F}_3$.
2) $P=X^2+aX+b\in\mathbb{F}_3[X]$ est irréductible si et seulement si P n'a pas de racine dans $\mathbb{F}_3$. Au total, il y a 9 polynômes $P\in\mathbb{F}_3[X]$ de la forme X^2+aX+b et parmi ceux-ci seuls les polynômes suivants sont irréductibles : X^2+1 ; X^2+X-1 ; X^2-X-1
3) On sait qu'il y a $\varphi(8)/2=2$ polynômes primitifs de degré 2.
• Soit θ une racine de X^2+1. Alors $\theta^2=-1$ et $\theta^4=1$. L'élément θ, d'ordre 4, n'engendre pas $\mathbb{F}_9^*$.
• Soit θ une racine de X^2+X-1. Alors $\theta^4=(1-\theta)^2=\theta^2+\theta+1=-1$ et ainsi θ est d'ordre 8 et X^2+X-1 est primitif.
• X^2-X-1 est primitif.
4) L'élément α vérifie $\alpha^2=-\alpha+1$. Comme X^2-X+1 est primitif, α engendre $\mathbb{F}_9^*$ et Z_α a bien un sens. A noter aussi que $\alpha^4=-1$. Ainsi $1-\alpha^4=2=-1=\alpha^4$ et donc $Z_\alpha(4)=4$. Immédiatement $1-\alpha=\alpha^2$ et $1-\alpha^2=\alpha$ et donc $Z_\alpha(1)=2$ et $Z_\alpha(2)=1$.
Ensuite on note que

$$1-\alpha^i=\alpha^8-\alpha^i=\alpha^4\alpha^i(1-\alpha^{8-i}) \tag{9}$$

Ainsi en servant de la relation (9) $1-\alpha^7=\alpha^{4+7+2}=\alpha^5$ et donc $Z_\alpha(7)=5$, puis $Z_\alpha(6)=3$ (toujours en se servant de (9)). Ensuite, $\alpha^3=\alpha(1-\alpha)=\alpha-\alpha^2=\alpha-(1-\alpha)=\alpha^5-1$ et donc, en servant de (9), $1-\alpha^5=-\alpha^3=\alpha^7$ et ainsi $Z_\alpha(5)=7$ puis $Z_\alpha(3)=6$.

• La simplification.

$$\begin{aligned} 1+\alpha+\alpha^6+\alpha(1-\alpha^6)^4 &= 1-\alpha^5+\alpha^6+\alpha(\alpha^{\mathbb{Z}_\alpha(6)})^4 \\ &= \alpha^{Z_\alpha(5)}+\alpha^6+\alpha^{1+12} \\ &= \alpha^7+\alpha^6+\alpha^5 \\ &= \alpha^5(1+\alpha)+\alpha^7 \\ &= \alpha^5(1-\alpha^5)+\alpha^7 \\ &= \alpha^4+\alpha^7 \\ &= \alpha^4(1+\alpha^3) \\ &= \alpha^4(1-\alpha^7) \\ &= \alpha \end{aligned}$$

• On cherche les racines du polynôme $Q = X^3+1+\alpha^7$ dans $\mathbb{F}_9$. Or $Q = X^3+1+\alpha^7 = X^3+1-\alpha^3 = X^3+\alpha^6$. Alors $-\alpha^i$ est racine de Q ($i \in \{1,\cdots,7\}$) si et seulement si $\alpha^{3i} = \alpha^6$, si et seulement si $3i \equiv 6 (\text{mod } 8)$, ou encore (comme $(3,8)=1$), si et seulement si $i \equiv 2 (\text{mod } 8)$, d'où une seule solution : $i = 2$. L'élément $-\alpha^2$ est l'unique racine de Q. On obtient alors la décomposition en facteurs irréductibles dans $\mathbb{F}_9[X]$:

$$Q = (X+\alpha^2)(X^2-\alpha^2X-1).$$

Exercice 39.
Il faut déterminer la factorisation en polynômes irréductibles de $P = X^5+X^2+2X+1$ sur $\mathbb{F}_3$.
On note tout d'abord que $P(0)$, $P(1)$ et $P(-1)$ sont non nuls, ainsi P n'a pas de racine dans $\mathbb{F}_3$. D'après l'exercice 38, on connaît les polynômes irréductibles de degré 2 sur $\mathbb{F}_3$: X^2+1 ; X^2+X-1 ; X^2-X-1. On note ensuite que X^2+1 divise P (par division euclidienne par exemple) :

$$P = (X^2+1)(X^3-X+1).$$

Le polynôme X^3-X+1 est irréductible sur $\mathbb{F}_3$.
Soit alors k le corps des racines de X^2+1 et k′ celui de X^3-X+1. Comme toute extension finie de corps finis est normale, le corps des racines d'un polynôme irréductible sur $\mathbb{F}_p$ coïncide avec un corps de rupture. Par conséquent, le corps k est de degré 2 sur $\mathbb{F}_3$ et $\text{k} = \mathbb{F}_9$. Le corps k′ est de degré 3 sur $\mathbb{F}_3$ et $\text{k}' = \mathbb{F}_{27}$. Le corps des racines de P est le compositum

kk'. Les extension $\mathrm{k}/\mathbb{F}_3$ et $\mathrm{k}'/\mathbb{F}_3$ étant de degrés premiers entre-elles, elles sont linéairement disjointes, ainsi $[\mathrm{kk}' : \mathbb{F}_3] = 6$ et $\mathrm{kk}' = \mathbb{F}_{3^6}$.

Exercice 40.
1) Soit $P = X^{p^n} - X \in \mathbb{F}_p[X]$. On rappelle que $\mathbb{F}_{p^n}$ est le corps des racines de P.
•. Soit $Q \in S$ et soit α une racine de Q. Alors $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$, où d est le degré de Q. Comme d divise n, on a $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Or $\mathbb{F}_{p^n}$ est l'ensemble des racines de $X^{p^n} - X$. Ainsi, $\alpha^{p^n} - \alpha = 0$, ou encore Q divise P dans $\mathbb{F}_p[X]$. Ainsi $\prod_{Q \in S} Q$ divise P.
• Soit α une racine de P de degré d sur $\mathbb{F}_p$: $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Alors $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$. Par conséquent $d|n$ et $\mathrm{Irr}(\alpha, \mathbb{F}_p) \in S$.
• Pour terminer, il faut noter que P est séparable (la multiplicité de chaque facteur irréductible de P vaut 1) puis que les polynômes en jeu sont unitaires. Au final : $P = \prod_{Q \in S} Q$.

2) En regardant les degrés dans l'égalité de 1), on obtient immédiatement la formule voulue.
$P_2(1)$ est le nombre de polynômes unitaires de degré 1 sur $\mathbb{F}_2$: $P_2(1) = 2$. Ensuite $2^2 = P_2(1) + 2P_2(2)$, d'où $P_2(2) = 1$. Puis $2^4 = P_2(1) + 2P_2(2) + 4P_2(4)$, d'où $P_2(4) = 3$. Et enfin,

$$2^8 = P_2(1) + 2P_2(2) + 4P_2(4) + 8P_2(8),$$

d'où $P_2(8) = 30$.

Exercice 41.
1) Soit $q = p^n$ impair et soit $x \in \mathbb{F}_q$. Considérons les ensembles d'éléments de $\mathbb{F}_q$ suivants :

$$S = \{x - a^2,\ a \in \mathbb{F}_q\}, \quad T = \{b^2,\ b \in \mathbb{F}_q\}.$$

L'ensemble T est l'ensemble des carrés de $\mathbb{F}_q$ et $|S| = |T|$. Or $\mathbb{F}_q^\times = \langle \varepsilon \rangle$. Ainsi pour $z \in \mathbb{F}_q$ non nul, il existe $0 \leq i < q - 1$ tel que $z = \varepsilon^i$. Si i est pair, z est un carré. Réciproquement, si z est un carré, alors $z = \varepsilon^i$ avec i pair. Modulo $q - 1$ on peut s'assurer que $0 \leq i < q - 1$ avec i pair (car $q - 1$ est pair). Ainsi, dans $\mathbb{F}_q$, il y a exactemement $(q - 1)/2$ carrés non

nuls et donc $|T| = 1 + (q-1)/2 = (q+1)/2$ (ne pas oublier que 0 est un carré !).
Comme S et T sont deux sous-ensembles de $\mathbb{F}_q$ et que $|S| + |T| > q$, le sous-ensemble $S \cap T$ est non vide : il existe $a, b \in \mathbb{F}_q$ tels que $x = a^2 + b^2$.
2) Comme p est impair, l'élément -1 est d'ordre 2 dans le groupe $\mathbb{F}_p^*$ qui est cyclique d'ordre $(q-1)/2$. Soit ε un générateur de k^*. L'élément $\varepsilon^{(q-1)/2}$ est l'unique élément du groupe $\mathbb{F}_q^*$ d'ordre 2 et donc $-1 = \varepsilon^{(q-1)/2}$. Dans 1), nous avons vu que ε^j est un carré si et seulement si j est pair, et ainsi -1 est un carré si et seulement si $(q-1)/2$ est pair, c'est-à-dire si et seulement si $q \equiv 1 \pmod 4$.

Exercice 42.
1) a) $f(\alpha + a) = (\alpha + a)^p - (\alpha + a) + 1 = \alpha^p + a^p - \alpha - a + 1 = 0$. Ainsi, les racines de f, au nombre de p, sont les éléments $\alpha + a$, $a \in \mathbb{F}_p$.
b) Le corps K est engendré par les éléments $\alpha + a$, $a \in \mathbb{F}_p$: $\mathrm{K} = \mathbb{F}_p(\alpha)$.
2) a) $f = \prod_{a \in \mathbb{F}_p} (X - \alpha - a)$.
b) Commençons par noter que $\alpha \notin \mathbb{F}_p$: en effet, α, racine de f, vérifie la relation $\alpha^p - \alpha + 1$ et ainsi $\alpha^p \neq \alpha$. Supposons f non irréductible sur $\mathbb{F}_p$. Soit g un facteur irréductible divisant f. Alors, par factorialité dans $\overline{\mathrm{k}}[X]$, il existe $a_1, \cdots, a_r \in \mathbb{F}_p$, $r < p$, tels que

$$g = f = \prod_{i=1}^{r} (X - \alpha - a_i).$$

On développe :

$$g = X^r + (-1)^{r-1} (r\alpha + a_1 + \cdots + a_r) X^{r-1} + \cdots \in \mathbb{F}_p[X].$$

En identifiant les termes en X^{r-1}, il vient $r\alpha + a_1 + \cdots + a_r \in \mathbb{F}_p$, et comme $r \neq 0$, on aboutit à $\alpha \in \mathbb{F}_p$, ce qui est une absurdité. Ainsi f est irréductible sur $\mathbb{F}_p$ et $\mathrm{K} = \mathbb{F}_{p^p}$.
3) Le morphisme de réduction $\Psi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ est un homomorphisme d'anneaux. Comme P est unitaire et que $\psi(P) = g$ est irréductible sur $\mathbb{F}_p$, il est facile d'en déduire l'irréductibilité de P sur $\mathbb{Z}$ (donc sur $\mathbb{Q}$).

Exercice 43.
Si l'on note par $x_1, \cdots, x_n$ les racines de P (comptées avec multiplicité), nous utilisons l'identité de la proposition 5.4.6 :

$$\mathrm{disc}(P) = (-)^{n(n-1)/2} P'(x_1) \cdots P'(x_n).$$

1) Soit $P = X^4 + aX^2 + b$.
S'il existe une racine θ de P nulle, alors cette racine est double et alors $\mathrm{disc}(P) = 0$.
Sinon, il existe deux racines θ_1 et θ_2 telles que les quatre racines de P sont exactement $\pm\theta_i$, $i = 1, 2$. Remarquons que $P'(\theta_i) = 4\theta_i(\theta_i^2 + a/2)$.
Posons $\beta_i = \theta_i^2$. Alors, pour $i = 1, 2$, le complexe β_i est racine de $Q = X^2 + aX + b$, et $\beta_i + a/2$ est racine de $R(X) = Q(X - a/2)$. Comme le terme constant de $R(X)$ est égal à $-a^2/4 + b$, il vient $\beta_1\beta_2 = -a^2/4 + b$.
Alors

$$\begin{aligned}
\mathrm{disc}(P) &= \prod_{i=1}^{4} \Big(4x_i(x_i^2 + a/2)\Big) \\
&= 4^4 \prod_{i=1}^{4} x_i \prod_{i=1}^{2} (\theta_i^2 + a/2)^2 \\
&= 4^4 b(-a^2/4 + b)^2 \\
&= 16b(a^2 - 4b)^2.
\end{aligned}$$

Pour conclure, on observe que la formule est valable lorsque $b = 0$.

2) Procéder comme pour 1).

3) Soit $P = X^n + aX + b$.
Commençons par supposer $ab \neq 0$. Alors toute racine θ de P est non nulle. En utilisant le fait que $\theta^{n-1} = -(a + b/\theta)$, il vient

$$P'(\theta) = -\frac{a(n-1)}{\theta}\left(\theta + \frac{nb}{a(n-1)}\right).$$

Observons ensuite que $\theta + \dfrac{nb}{a(n-1)}$ est racine de $R(X) = P(X - nb/(a(n-1))$. Par conséquent, en déterminant le terme constant de R, il vient :

$$\prod_{i=1}^{n}\left(\theta_i + \frac{nb}{a(n-1)}\right) = (-1)^n\left((-1)^n \frac{n^n b^n}{a^n(n-1)^n} - \frac{nb}{n-1} + b\right),$$

où les θ_i sont les racines de P. Ainsi

$$\begin{aligned}\operatorname{disc}(P) &= (-1)^{n(n-1)/2}\prod_{i=1}^{n} P'(\theta_i)\\ &= (-1)^{n(n-1)/2}\frac{a^n(n-1)^n}{(-1)^n b}\cdot\Big((-1)^n\frac{n^n b^n}{a^n(n-1)^n}-\frac{nb}{n-1}+b\Big)\\ &= (-1)^{n(n-1)/2}\Big(n^n b^{n-1}+(-1)^{n+1}(a^n(n-1)^{n-1})\Big).\end{aligned}$$

Regardons pour finir les cas particuliers.

Si $b = a = 0$. Alors $P = X^n$ et $\operatorname{disc}(P) = 0$. On observe que la formule est toujours valable dans ce cas.

Si $a = 0$ et $b \neq 0$. Alors $P = X^n + b$. On observe que toute racine θ de P est non nulle et $P'(\theta) = n\theta^{n-1} = -nb/\theta$. Alors

$$\begin{aligned}\operatorname{disc}(P) &= (-1)^{n(n-1)/2}\prod_{i=1}^{n}(-nb/\theta_i)\\ &= (-1)^{n(n-1)/2}(-nb)^n\frac{1}{(-1)^n b}\\ &= (-1)^{n(n-1)/2}b^{n-1}n^n.\end{aligned}$$

Là aussi on observe que la formule est toujours valable pour ce cas particulier.

Si $b = 0$ et $a \neq 0$. Alors 0 est racine simple, et $P'(0) = a$. Pour toute autre racine θ non nulle, il vient $P'(\theta) = n\theta^{n-1} + a = -na + a$, car $\theta^{n-1} = -a$. Alors

$$\begin{aligned}\operatorname{disc}(P) &= (-1)^{n(n-1)/2}\prod_{i=1}^{n} P'(\theta_i)\\ &= (-1)^{n(n-1)/2}a\prod_{\theta_i\neq 0}\Big(a(-n+1)\Big)\\ &= (-1)^{n(n-1)/2}(-1)^{n-1}a^n(n-1)^{n-1}.\end{aligned}$$

Là aussi la formule est toujours valable pour ce cas particulier.

Exercice 44.

1) D'après l'exercice 43, il vient $\operatorname{disc}(P) = (\pm)(p^p - (p-1)^{p-1})$ et clairement $2 \nmid \operatorname{disc}(P)$.

2) On a $\theta^0 = 1$, $\theta^1 = \theta$, $\theta^2 = \theta^2$, $\theta^3 = \theta(\theta+1) = 1$. Ainsi, θ^n est périodique de période 3. Pour $p \equiv 2 (\text{mod } 3)$, il vient $\theta^p = \theta^2$ et ainsi $P(\theta) = 0$. Conclusion : dans $\mathbb{F}_2[X]$, $X^2 + X + 1$ divise P.

3) Par le théorème 5.4.11, on note les points suivants :

(i) l'irréductibilité de P en le premier p (par l'exercice 42) montre que le groupe de Galois $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$ contient un p-cycle,

(ii) comme $2 \nmid \mathrm{disc}(P)$, on sait que

$$P \equiv (X^2 + X + 1)\bar{P}_1 \cdots \bar{P}_t \pmod 2,$$

avec les $\bar{P}_i$ irréductibles et $(X^2 + X + 1) \nmid \bar{P}_i$. Ainsi si les degrés des $\bar{P}_i$ sont impairs, on en déduit que $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$ contient une transposition.

Sous (i) et (ii), la proposition 5.4.2 indique que $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q}) \simeq S_p$.

Pour $p = 5$, on trouve

$$X^5 - X - 1 \equiv (X^2 + X + 1)(X^3 + X^2 + 1) \pmod 2.$$

Pour $p = 11$, on trouve

$$X^{11} - X - 1 \equiv (X^2 + X + 1)(X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1) \pmod 2.$$

CHAPITRE 6

CORPS CYCLOTOMIQUES - THÉORIE DE KUMMER

6.1. Racines de l'unité dans un corps

Définition 6.1.1. — Soit k un corps et soit un entier $n \geq 1$. On appelle $\mu_n(\mathrm{k})$ l'ensemble des racines dans k du polynôme $X^n - 1$.
Si $\overline{\mathrm{k}}$ est une clôture algébrique de k, on note $\mu_n = \mu_n(\overline{\mathrm{k}})$ l'ensemble des rainces de $X^n - 1$ dans $\overline{\mathrm{k}}$.

Remarque 6.1.2. — Comme dans un corps un polynôme n'a qu'un nombre fini de racines, l'ensemble $\mu_n(\mathrm{k})$ est un sous-groupe fini de $(\mathrm{k}^*, \cdot)$: $\mu_n(\mathrm{k})$ est donc cyclique.

Exemple 6.1.3. — $\mu_{2n}(\mathbb{R}) = \{\pm 1\}$; $\mu_{2n+1}(\mathbb{R}) = \{1\}$.

Théorème 6.1.4. — *Soit* k *un corps et soit un entier* $n \geq 1$.
(i) Si la caractéristique de k *est nulle, le groupe* μ_n $(= \mu_n(\overline{\mathrm{k}}))$ *est un groupe cyclique d'ordre* n.
(ii) Supposons la caractéristique de k *égale à* $p > 0$ *et écrivons* $n = p^s d$, *avec* $(d, p) = 1$. *Alors* $\mu_n = \mu_d$ *et* μ_d *est un groupe cyclique d'ordre* d.

Démonstration. — Soit $P = X^n - 1$. Alors $D(P) = nX^{n-1}$ et ainsi, P est séparable si et seulement si $(P, D(P)) = (P, nX^{n-1}) = 1$, c'est-à-dire si et seulement si $n \neq 0$ dans k, c'est-à-dire quand la caractéristique de k est nulle ou bien quand $(n, p) = 1$. Dans ce cas, le nombre de racines distincts 2 à 2 de P est égal au degré de P c'est-à-dire à n.
Supposons $n = p^s d$, où p est la caractéristique de k. Alors sur k, $X^n - 1 = (X^d - 1)^{p^s}$. Ainsi $\zeta \in \overline{\mathrm{k}}$ est racine de P si et seulement si ζ est racine de

$P' = X^d - 1$. Comme $(d, p) = 1$, P' est séparable et a donc exactement d racines 2 à 2 distinctes. □

Remarque 6.1.5. — Dans la suite, lorsque le corps k sera de caractéristique positive p, on supposera **toujours** $(n, p) = 1$.

Définition 6.1.6. — On appelle racine primitive n-ème de l'unité dans $\overline{\mathrm{k}}$ tout générateur ζ de μ_n. Une telle racine est notée ζ_n.

Exemple 6.1.7. — Dans $\mathbb{C}$, $\zeta_n = \exp(2i\pi/n)$ est une racine d'ordre n.

Proposition 6.1.8. — *Dans* $\overline{\mathrm{k}}$, *il y a exactement* $\varphi(n)$ *racines primitives* n*-ème de l'unité, où* φ *est la fonction d'Euler. En particulier, si* ζ *est d'ordre* n, *alors les autres racines d'ordre* n *sont exactement* ζ^i, $1 \leq i \leq n-1$ *et* $(i, n) = 1$.

Démonstration. — C'est immédiat. □

Définition 6.1.9. — Soit k un corps et n un entier (premier donc à la caractéristique du corps k). Le corps $\mathrm{k}(\mu_n)/\mathrm{k}$ s'appelle la n-ème extension cyclotomique de k ; $\mathrm{k}(\mu_n)$ est le corps cyclotomique des racines n-èmes de l'unité.

Théorème 6.1.10. — *L'extension* $\mathrm{k}(\mu_n)/\mathrm{k}$ *est galoisienne (en fait abélienne) et son groupe de Galois est canoniquement isomorphe à un sous-groupe de* $(\mathbb{Z}/n\mathbb{Z})^\times$. *En particulier,* $[\mathrm{k}(\mu_n) : \mathrm{k}]$ *divise* $\varphi(n)$.

Démonstration. — Soit $\zeta = \zeta_n$ une racine primitive d'ordre n : $\mathrm{k}(\mu_n) = \mathrm{k}(\zeta)$. Alors $\mathrm{Irr}(\zeta, \mathrm{k})$ divise $P = X^n - 1$ qui est séparable (sous la condition où n est premier à la caractéristique de k). Ainsi ζ est séparable et il en est de même pour $\mathrm{k}(\zeta)/\mathrm{k}$. D'autre part, $\mathrm{k}(\zeta)$ est le corps des racines de P. L'extension $\mathrm{k}(\zeta)/\mathrm{k}$ est donc galoisienne de groupe de Galois G.
Étant donné $\sigma \in G$, $\sigma(\zeta) = \zeta^{a_\sigma}$, avec $a_\sigma \in \{0, \cdots, n-1\}$. Comme σ est un automorphisme, il existe $\tau \in G$ tel que $\sigma\tau = \mathrm{id}$, c'est-à-dire

$$\begin{aligned} \zeta &= \sigma(\tau(\zeta)) \\ &= \sigma\zeta^{a_\tau} \\ &= \zeta^{a_\sigma a_\tau} \end{aligned}$$

et ainsi, ζ étant d'ordre n, $\overline{a_\sigma} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Soit alors

$$\begin{array}{rccc} \phi : G & \to & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \mapsto & \overline{a_\sigma} \end{array}$$

L'application ϕ est clairement un morphisme de groupes.
Il reste à regarder l'injectivité de ϕ. Soit $\sigma \in \ker(\phi)$. Alors $\overline{a_\sigma} = 1$, $\zeta^{a_\sigma} = 1$, c'est-à-dire $\sigma = \mathrm{id}$.
Au final : $G \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. □

Définition 6.1.11. — On appelle polynôme cyclotomique d'indice n sur k (toujours sous la condition $(p, n) = 1$), et on note Φ_n, le polynôme de k$[X]$ dont les racines sont exactement les racines primitives de l'unité d'ordre n (avec multiplicité 1) :

$$\Phi_n = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (X - \zeta_n^i),$$

où ζ_n est une racine primitive d'ordre n. Le polynôme Φ_n est de degré $\varphi(n)$.

Remarque 6.1.12. — Pour $(j, n) = 1$, un k-conjugué de ζ_n^j est d'ordre n et se trouve donc dans la famille $\{\zeta_n^i,\ 1 \leq i \leq n,\ (i, n) = 1\}$. Ainsi Φ_n est fixe sous l'action de Gal(k(ζ_n)/k) et c'est donc bien un polynôme à coefficients dans k.

Remarque 6.1.13. — Soit ζ_n d'ordre n. Alors $\mathrm{Irr}(\zeta_n, \mathrm{k})$ divise Φ_n.

Proposition 6.1.14. — *Soit* k *un corps de caractéristique* p *et soit* $n \geq 1$, $(n, p) = 1$. *Alors*

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Démonstration. — Soit ζ une racine primitive n-ème de l'unité. Soit x une racine de $X^n - 1$. Alors, x est d'ordre d divisant n, ainsi x est racine de Φ_d.
Réciproquement, si x est racine de Φ_d, $d|n$, alors $x^n = (x^d)^{n/d} = 1$ et donc x est racine de $X^n - 1$.

Par construction, les polynômes Φ_d sont séparables et pour $d \neq d'$, $(\Phi_d, \Phi_{d'}) = 1$. Ainsi $\prod_{d|n} \Phi_d$ est séparable. Il en est de même pour $X^n - 1$. Au final, on a bien l'égalité souhaitée. □

Théorème 6.1.15. — *Soit* k *un corps de caractéristique* p. *Soient* ℓ *un nombre premier et un entier* $n \geq 1$ *vérifiant* $(n\ell, p) = 1$. *On a les formules suivantes :*

(i) $\Phi_\ell(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$;

(ii) Si $\ell \not| n$, $\Phi_n(X^\ell) = \Phi_{n\ell}(X)\Phi_n(X)$;

(iii) Si $\ell | n$, $\Phi_n(X^\ell) = \Phi_{n\ell}(X)$.

(Les polynômes Φ_n *sont vus dans* $\mathrm{k}[X]$.*)*

Démonstration. — (i) On sait que Φ_ℓ est de degré $\varphi(\ell) = \ell - 1$ et que Φ_ℓ divise $X^\ell - 1 = (X-1)(X^{\ell-1} + X^{\ell-2} + \cdots + X + 1)$. D'où le résultat annoncé.
(ii) Calculons tout d'abord les degrés : $\deg(\Phi_n(X^\ell)) = \ell\varphi(n)$ et $\deg(\Phi_{n\ell}(X)\Phi_n(X)) = \varphi(n\ell) + \varphi(n)$. Comme $(n, \ell) = 1$, $\varphi(n\ell) = \varphi(n) \cdot \varphi(\ell) = (\varphi(n))(\ell - 1)$. Ainsi $\deg(\Phi_{n\ell}(X)\Phi_n(X)) = \ell\varphi(n) = \deg(\Phi_n(X^\ell))$. Il suffit alors de montrer qu'un polynôme divise l'autre. C'est immédiat. Comme $(n, \ell) = 1$, si ζ est d'ordre n, alors ζ^ℓ est d'ordre n et ainsi $\Phi_n(\zeta^\ell) = 0$ ou encore ζ est racine de $\Phi_n(X^\ell)$ et donc $\Phi_n(X)$ divise $\Phi_n(X^\ell)$. Puis si ζ' est d'ordre $n\ell$, ζ'^ℓ est d'ordre n et donc $\Phi_{n\ell}(X)$ divise $\Phi_n(X^\ell)$. On conclut en notant que Φ_n et $\Phi_{n\ell}$ sont premiers entre eux (pas de racine commune).
(iii) Comme $\ell | n$, $\varphi(n\ell) = \ell n$. Ainsi, $\deg(\Phi_n(X^\ell)) = \ell\varphi(n) = \varphi(n\ell) = \deg(\Phi_{n\ell})$. On conclut, en notant, comme précédemment, que $\Phi_{n\ell}(X)$ divise $\Phi_n(X^\ell)$. □

Corollaire 6.1.16. — *Soit* $\Phi_n \in \mathbb{Q}[X]$. *Alors* $\Phi_n \in \mathbb{Z}[X]$ *et pour tout nombre premier* p *premier à* n, $\overline{\Phi_n} = \Phi_n \pmod p$ *est le* n*-ème polynôme cyclotomique sur* $\mathbb{F}_p$.

Démonstration. — Ce sont des conséquences immédiates des formules de récurrence du théorème 6.1.15. □

Exemple 6.1.17. — On souhaite calculer Φ_{36}. On part de $\Phi_2 = X + 1$. Ensuite $\Phi_4 = \Phi_2(X^2) = X^2 + 1$, dont les racines sont bien $\pm i$! Puis $\Phi_{12} = \Phi_4(X^3)/\Phi_4 = (X^6 + 1)/(X^2 + 1) = X^4 - X^2 + 1$. Enfin, $\Phi_{36} = \Phi_{12}(X^3) = X^{12} - X^6 + 1$.

6.2. Corps cyclotomiques sur $\mathbb{F}_q$

Soit $\mathrm{k} = \mathbb{F}_q$, $q = p^e$ et soit $n \geq 1$, $(n, p) = 1$. On sait que le corps $\mathbb{F}_q(\mu_n)$ est un corps fini donc de la forme $\mathbb{F}_{q^t}$. On s'intéresse à la question de déterminer l'entier t.

Remarque 6.2.1. — On rappelle que le groupe $\mathrm{Gal}(\mathrm{k}(\mu_n)/\mathrm{k})$ est cyclique et est engendré par l'automorphisme de Frobenius $\varphi_q : x \mapsto x^q$ (voir le théoréme 5.2.7).

Théorème 6.2.2. — *Le corps $\mathbb{F}_q(\mu_n)$ est le corps fini $\mathbb{F}_{q^t}$, où t est l'ordre de $\overline{q}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. — Soit ζ une racine primitive de l'unité d'ordre n.
Soit t l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors $\varphi_q^t(\zeta) = \zeta^{q^t} = \zeta$, et pour tout $s|t$, $\varphi_q^s(\zeta) = \zeta^{q^s} \neq \zeta$. Ceci signifie que $\zeta \in \mathbb{F}_{q^t}$, mais que ζ n'appartient dans aucun des sous-corps stricts de $\mathbb{F}_{q^t}$ (voir le corollaire 5.2.3). Ainsi $\mathrm{k}(\zeta) = \mathbb{F}_{q^t}$. □

Remarque 6.2.3. — Pour la preuve du théorème 6.2.2, on aurait pu procéder de la façon suivante. Le morphisme $\phi : \mathrm{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q) \to (\mathbb{Z}/n\mathbb{Z})^\times$ induit un isomorphisme entre $\mathrm{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q)$ et $\mathrm{Im}(\phi)$. Or $\mathrm{Im}(\phi) = \langle \phi(\varphi_q) \rangle$. Comme $\langle \phi(\varphi_q) \rangle = \langle \overline{q} \rangle$, on retrouve bien le résultat.

Exemple 6.2.4. — Comme 4 est d'ordre 3 dans $(\mathbb{Z}/9\mathbb{Z})^\times$, il vient : $\mathbb{F}_4(\mu_9) = \mathbb{F}_{4^3}$. En particulier, le polynôme $\Phi_9 = \Phi_3(X^3) = X^6 + X^3 + 1$ n'est pas irréductible sur $\mathbb{F}_4$.

6.3. Corps cyclotomiques sur $\mathbb{Q}$

6.3.1. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. —

Théorème 6.3.1. — *L'extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$ est de degré $\varphi(n)$ et $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. — On commence par montrer le lemme suivant :

Lemme 6.3.2. — *Soit ζ une racine primitive n-ème de l'unité et soit ℓ un nombre premier tel que $(\ell, n) = 1$. Alors ζ^ℓ est un $\mathbb{Q}$-conjugué de ζ.*

Remarque 6.3.3. — On rappelle que deux éléments ζ et ζ' sont $\mathbb{Q}$-conjugués si et seulement si $\mathrm{Irr}(\zeta, \mathbb{Q}) = \mathrm{Irr}(\zeta', \mathbb{Q})$.

Démonstration. — Supposons ζ et ζ^ℓ non $\mathbb{Q}$-conjugués. Soit $P = \mathrm{Irr}(\zeta, \mathbb{Q})$ et soit $Q = \mathrm{Irr}(\zeta^\ell, \mathbb{Q})$. Alors $P \neq Q$ et, P et Q divisent $X^n - 1$. Ainsi par division euclidienne, $X^n - 1 = PQ'$, avec $Q' \in \mathbb{Z}[X]$, unitaire, et $Q|Q'$. Donc $\deg(Q') > 0$.
Soit $R(X) = Q'(X^\ell) \in \mathbb{Z}[X]$. Alors $R(\zeta) = Q'(\zeta^\ell) = 0$, ainsi P divise R dans $\mathbb{Z}[X]$. Il existe $S \in \mathbb{Q}[X]$, unitaire (par division euclidienne), tel que $R = PS$. Soit ensuite $\psi_\ell : \mathbb{Z}[X] \to \mathbb{F}_\ell[X]$ le morphisme d'anneaux correspondant à la réduction modulo ℓ. Alors $\psi_\ell(R(X)) = \psi_\ell(Q'(X^\ell)) = \psi_\ell((Q')^\ell)$, mais aussi $\psi_\ell(R) = \psi_\ell(P)\psi_\ell(S)$. Ainsi, par factorialité dans $\mathbb{F}_\ell[X]$, $\psi_\ell(P)$ et $\psi_\ell(Q')$ ne sont pas premiers entre eux, ce qui implique que $X^n - \overline{1} = \psi_\ell(X^n - 1) = \psi_\ell(P)\psi_\ell(Q') \in \mathbb{F}_\ell[X]$ n'est pas séparable. Comme $(n, \ell) = 1$, on aboutit à une contradiction. □

Soit alors $m = \ell_1^{n_1} \cdots \ell_r^{n_r}$, avec $(\ell_i, n) = 1$. D'après le lemme 6.3.2, $\zeta^{\ell_i \ell_j}$ est $\mathbb{Q}$-conjugué à ζ^{ℓ_i} qui lui même est $\mathbb{Q}$-conjugué à ζ, etc ... On voit ainsi que pour tout entier m premier à n, ζ^m est $\mathbb{Q}$-conjugué à ζ.
Ainsi $\deg(\mathrm{Irr}(\zeta, \mathbb{Q})) = \varphi(n)$, et par conséquent $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ et le morphisme ϕ du théorème 6.1.10 est un isomorphisme. □

Corollaire 6.3.4. — *Sur $\mathbb{Q}$, le polynôme cyclotomique Φ_n est irréductible et $\Phi_n = \mathrm{Irr}(\zeta_n, \mathbb{Q})$.*

Démonstration. — Si ζ est une racine primitive de l'unité d'ordre n, alors $\mathrm{Irr}(\zeta, \mathbb{Q})$ divise Φ_n et ces polynômes ont même degré $\varphi(n)$. □

6.3.2. Sous-corps réel maximal. — Soit $\mathrm{K}/\mathbb{Q}$ une extension finie (vue dans $\mathbb{C}/\mathbb{Q}$).

Définition 6.3.5. — L'extension $\mathrm{K}/\mathbb{Q}$ est dite réelle si $\mathrm{K} \subset \mathbb{R}$.

L'extension $K/\mathbb{Q}$ est dite totalement réelle si tous les $\mathbb{Q}$-plongements de K dans $\mathbb{C}$ sont réels.

Remarque 6.3.6. — Soit $K = \mathbb{Q}(\alpha)$. Alors K est réel si et seulement si α est réel et, K est totalement réel si et seulement si toutes les racines de $\mathrm{Irr}(\alpha, \mathbb{Q})$ sont réelles.

Exemple 6.3.7. — Le corps $\mathbb{Q}(\sqrt[3]{3})$ est réel mais n'est pas totalement réel. Le corps $\mathbb{Q}(\sqrt{3})$ est totalement réel.

Proposition 6.3.8. — *Supposons* $K/\mathbb{Q}$ *galoisienne.*
(i) Si $K/\mathbb{Q}$ *est réelle, alors* $K/\mathbb{Q}$ *est totalement réelle.*
(ii) Si K *n'est pas réel, alors aucun* $\mathbb{Q}$*-automorphisme* σ *de* $K/\mathbb{Q}$ *n'est réel. Dans ce cas, on dit que* K *est totalement imaginaire.*

Démonstration. — Soit α un élément primitif de $K/\mathbb{Q}$, c'est-à-dire $K = \mathbb{Q}(\alpha)$. Soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Alors $\sigma(\alpha) \in K$ et $\mathbb{Q}(\alpha) = \mathbb{Q}(\sigma(\alpha))$.
(i) Si K est réel, pour tout élément $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(K) = \mathbb{Q}(\sigma(\alpha)) = \mathbb{Q}(\alpha) \subset \mathbb{R}$.
(ii) Si K n'est pas réel, comme $\mathbb{Q}(\alpha) = \mathbb{Q}(\sigma(\alpha))$, pour tout $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, cela implique, d'après (i), que $\sigma(\alpha) \notin \mathbb{R}$. □

Soit c la conjugaison complexe : c'est un automorphisme de $\mathbb{C}$ d'ordre 2 et $c_{|K}$ est un isomorphisme de K dans $\mathbb{C}$. Soit $K/\mathbb{Q}$ une extension galoisienne. Alors $c \in \mathrm{Gal}(K/\mathbb{Q})$, et nous avons montré que $K/\mathbb{Q}$ est totalement réelle si et seulement si $c_{|K} = \mathrm{id}$.

Définition 6.3.9. — Soit $K/\mathbb{Q}$ une extension galoisienne totalement imaginaire. Alors $K^{\langle c \rangle}$ est appelé sous-réel maximal de K et est noté K^+ ; $[K : K^+] = 2$.

Proposition 6.3.10. — *Soit* $K/\mathbb{Q}$ *une extension galoisienne de groupe de Galois* G*. Supposons* $K/\mathbb{Q}$ *totalement imaginaire. Alors* K^+ *est totalement réel si et seulement si* $\langle c \rangle$ *est distingué dans* G*.*

Démonstration. — Supposons $\langle c \rangle$ distingué. Alors $K^+/\mathbb{Q}$ est galoisienne et réelle. D'après la proposition 6.3.8, $K^+/\mathbb{Q}$ est totalement réelle.
Réciproquement. Supposons $K^+/\mathbb{Q}$ totalement réelle. Soit β tel que $K^+ = \mathbb{Q}(\beta)$. Soit $\sigma \in G$. Alors $\sigma(\beta)$ est un $\mathbb{Q}$-conjugué de β, c'est une racine

de $\mathrm{Irr}(\beta, \mathbb{Q})$, ainsi $\sigma(\beta)$ est réel. Par conséquent, $\mathrm{c}(\sigma(\beta)) = \sigma(\beta)$ et ainsi $\sigma^{-1}\mathrm{c}\sigma(\beta) = \beta$. Ainsi, le sous-groupe $\langle \sigma^{-1}\mathrm{c}\sigma >$ de G (qui est d'ordre 2 car $\mathrm{c}_{|\mathrm{K}}$ n'est pas trivial) laisse fixe $\mathbb{Q}(\beta)$. Par la correspondance de Galois, on obtient $\langle \mathrm{c} \rangle = \mathrm{Gal}(\mathrm{K}/\mathrm{K}^+) = \langle \sigma^{-1}\mathrm{c}\sigma \rangle$ puis $\mathrm{c} = \sigma^{-1}\mathrm{c}\sigma$, d'où le résultat. □

Le cas des corps cyclotomiques est particulièrement agréable à décrire. Tout d'abord, pour $n > 2$, $\mathbb{Q}(\mu_n)$ est totalement imaginaire. Ensuite, la conjugaison complexe c agit par $\zeta_n^{\mathrm{c}} = \zeta_n^{-1}$. Et enfin $\mathbb{Q}(\mu_n)/\mathbb{Q}$ est abélienne, donc $\mathbb{Q}(\mu_n)^+$ est totalement réel.

Proposition 6.3.11. — *Soit $n > 2$ et soit ζ_n une racine primitive n-ème de l'unité. Le corps $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(2\pi/n))$ est le sous-corps réel maximal de $\mathbb{Q}(\mu_n)$. De plus,* $\mathrm{Irr}(\zeta_n, \mathbb{Q}(\mu_n)^+) = X^2 - (\zeta_n + \zeta_n^{-1})X + 1$.

Démonstration. — Posons $z = \zeta_n + \zeta_n^{-1}$. Alors $z^{\mathrm{c}} = z$ et donc $\mathbb{Q}(z)$ est contenu dans le sous-corps réel maximal $\mathbb{Q}(\mu_n)^+$ de $\mathbb{Q}(\mu_n)$. D'autre part, ζ_n est racine de $P(X) = X^2 - zX + 1 \in \mathbb{Q}(z)[X]$, ce qui signifie que $[\mathbb{Q}(\mu_n) : \mathbb{Q}(z)] \leq 2$, d'où le résultat. □

6.3.3. Treillis des sous-extensions cyclotomiques d'une extension cyclotomique. —

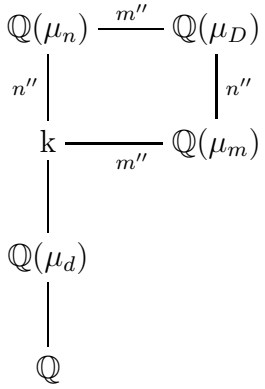
Théorème 6.3.12. — *Soient n et m deux entiers non nuls. Posons $d = pgcd(n, m)$ et $D = ppcm(n, m)$. Alors $\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_D)$ et $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_d)$. On a ainsi le schéma*

$$\begin{array}{ccc} \mathbb{Q}(\mu_n) & \text{———} & \mathbb{Q}(\mu_D) = \mathbb{Q}(\mu_n, \mu_m) \\ | & & | \\ \mathbb{Q}(\mu_d) = \mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) & \text{———} & \mathbb{Q}(\mu_m) \\ | & & \\ \mathbb{Q} & & \end{array}$$

Démonstration. — Posons $n = dn_0$, $m = dm_0$, $D = mm_1 = nn_1$ avec $(m_1, n_1) = (n_0, m_0) = 1$.
On a la formule classique suivante : $\varphi(d)\varphi(D) = \varphi(m)\varphi(n)$.

Nous désignons par ζ_i une racine primitive i-ème de l'unité.

Notons tout d'abord que $\zeta_D^{m_1}$ engendre μ_m et $\zeta_D^{n_1}$ engendre μ_n. Ainsi $\mathbb{Q}(\mu_n, \mu_m) \subset \mathbb{Q}(\mu_D)$. Ensuite, d'après la relation de Bezout, il existe $a, b \in \mathbb{Z}$ tels que $1 = an_1 + bm_1$. Ainsi $\zeta_D = \zeta_D^{an_1}\zeta_D^{bm_1}$, avec $\zeta_D^{m_1} \in \mathbb{Q}(\mu_m)$ et $\zeta_D^{n_1} \in \mathbb{Q}(\mu_n)$. Au total, on obtient bien $\mathbb{Q}(\mu_D) = \mathbb{Q}(\mu_n, \mu_m)$.
Comme $\zeta_n^{n_0}$ est une racine primitive d-ème de l'unité, alors $\mathbb{Q}(\mu_d) \subset \mathbb{Q}(\mu_n)$. Il en est de même pour $\mathbb{Q}(\mu_m)$ et ainsi $\mathbb{Q}(\mu_d) \subset \mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m)$. Soit $\mathrm{k} = \mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m)$. Comme les extensions $\mathbb{Q}(\mu_n)/\mathrm{k}$ et $\mathbb{Q}(\mu_m)/\mathrm{k}$ sont galoisiennes, ces extensions sont linéairement disjointes (voir le corollaire 4.1.5). On a donc le schéma suivant :



Ainsi,

$$\begin{aligned}
\varphi(D) &= [\mathbb{Q}(\mu_D) : \mathbb{Q}] \\
&= [\mathbb{Q}(\mu_D) : \mathrm{k}][\mathrm{k} : \mathbb{Q}] \\
&= [\mathbb{Q}(\mu_D) : \mathbb{Q}(\mu_m)][\mathbb{Q}(\mu_m) : \mathrm{k}][\mathrm{k} : \mathbb{Q}] \\
&= [\mathbb{Q}(\mu_n) : \mathrm{k}][\mathbb{Q}(\mu_m) : \mathrm{k}][\mathrm{k} : \mathbb{Q}] \\
&= \frac{[\mathbb{Q}(\mu_n) : \mathbb{Q}]}{[\mathrm{k} : \mathbb{Q}]} \frac{[\mathbb{Q}(\mu_m) : \mathbb{Q}]}{[\mathrm{k} : \mathbb{Q}]} [\mathrm{k} : \mathbb{Q}] \\
&= \frac{\varphi(n)\varphi(m)}{[\mathrm{k} : \mathbb{Q}]} \\
&= \frac{\varphi(d)\varphi(D)}{[\mathrm{k} : \mathbb{Q}]}
\end{aligned}$$

car $\varphi(n)\varphi(m) = \varphi(d)\varphi(D)$. Ainsi $[\mathrm{k} : \mathbb{Q}] = \varphi(d) = [\mathbb{Q}(\mu_d) : \mathbb{Q}]$, d'où le résultat. □

Corollaire 6.3.13. — *Soient deux entiers non nuls m et n, $m \geq n$. On a $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_m)$ si et seulement si ou bien $m = n$, ou bien $m = 2n$ avec n impair.*

Démonstration. —
•. Supposons que $m = 2n$, avec n impair. Alors ζ_{2n}^2 est une racine primitive n-ème de l'unité, et ainsi $\mathbb{Q}(\zeta_n) \subset \zeta_m$. Comme $(n, 2) = 1$, alors $\varphi(m) = \varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$, ce qui implique $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, d'où $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$.
•. Supposons que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$. Alors, d'après le théorème 6.3.12, $\mathbb{Q}(\zeta_d) = \mathbb{Q}(\zeta_D)$, où $D = ppcm(m, n)$ et $d = pgcd(m, n)$. Écrivons, $D = dr$, $r \in \mathbb{N}$. Alors $\varphi(d) = \varphi(dr)$.
Si $r = 1$, on a $d = D$, d'où $m = n$.
Supposons qu'il existe un nombre premier impair ℓ divisant r. Soit $r' = r/\ell$. Alors $\varphi(d) = \varphi(D) = \varphi(d\ell r') \geq (\ell - 1)\varphi(dr') \geq \varphi(d)$, ce qui n'est pas possible. Ainsi $r = 2^k$ et

$$\varphi(D) = \varphi(2^k d) = \begin{cases} 2^k\varphi(d) & \text{si } 2|d \\ 2^{k-1}\varphi(d) & \text{sinon} \end{cases}$$

On voit ainsi ou bien $k = 0$ ($D = d$ et c'est immédiat), ou bien $k = 1$ et d est impair. Dans ce second cas, $D = 2d$ et comme $mn = Dd$, on obtient $mn = 2d^2$. Comme $d|m$ et $d|n$, on a $m = 2n$, avec $n = d$. □

Corollaire 6.3.14. — *Soient n et m deux entiers non nuls. Alors $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_m)$ si et seulement si ou bien $n|m$, ou bien $n|2m$ avec m est impair.*

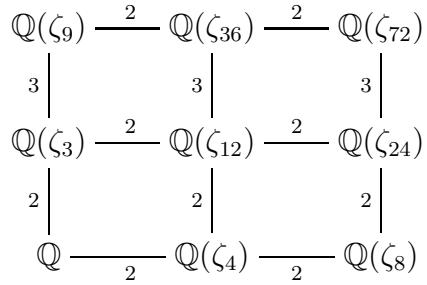
Démonstration. — Un sens est évident.
Supposons $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_m)$. Alors $\mathbb{Q}(\zeta_d) = \mathbb{Q}(\zeta_n)$. D'après le corollaire 6.3.13, ou bien $n = d$ et $n|m$, ou bien $n = 2d$, avec d impair. Dans ce dernier cas, m doit être impair (sinon d est pair) et donc $n|2m$. □

Le théorème 6.3.12 est ses corollaires nous permettent de dresser le treillis des sous-corps cyclotomiques d'une extension cyclotomique donnée.

Exemple 6.3.15. — Soit le corps cyclotomique $\mathbb{Q}(\zeta_{72})/\mathbb{Q}$. Comme $72 = 9 \cdot 8$, l'extension $\mathbb{Q}(\zeta_{72})/\mathbb{Q}$ contient les corps : $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$, $\mathbb{Q}(\zeta_9) = \mathbb{Q}(\zeta_{18})$, $\mathbb{Q}(\zeta_{12})$, $\mathbb{Q}(\zeta_{24})$. D'autre part, $\mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\zeta_9) = \mathbb{Q}$. Ainsi (à l'aide du corollaire 4.2.2)

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{72})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}).$$

Ensuite, $[\mathbb{Q}(\zeta_9):\mathbb{Q}]=6$, $[\mathbb{Q}(\zeta_3):\mathbb{Q}]=2$, $[\mathbb{Q}(\zeta_8):\mathbb{Q}]=4$ et $[\mathbb{Q}(\zeta_4):\mathbb{Q}]=2$.
Le treillis des sous-corps cyclotomiques de $\mathbb{Q}(\zeta_{72})/\mathbb{Q}$ est le suivant



Mais attention, ce n'est pas le treillis des sous-corps de $\mathbb{Q}(\zeta_{72})/\mathbb{Q}$. Pour celui-ci, il faut connaître la structure de $(\mathbb{Z}/72\mathbb{Z})^\times$.

6.3.4. Treillis des sous-corps d'une extension cyclotomique. — Le treillis des sous-corps de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est lié à la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$. Si $n=\prod_{i=1}^{r} p_i^n$, alors par le théorème des restes chinois,

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r}(\mathbb{Z}/p_i^n\mathbb{Z})^\times.$$

La suite repose sur la proposition suivante :

Proposition 6.3.16. —
1) On a $(\mathbb{Z}/2\mathbb{Z})^\times=\{1\}$ *et pour* $k\geq 2$,

$$(\mathbb{Z}/2^k\mathbb{Z})^\times=\langle -\overline{1},\overline{5}\rangle \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{k-2}\mathbb{Z}.$$

2) Soit p *un nombre premier impair. Alors* $(\mathbb{Z}/p\mathbb{Z})^\times\simeq\mathbb{Z}/(p-1)\mathbb{Z}$, *et pour* $k\geq 1$,

$$(\mathbb{Z}/p^k\mathbb{Z})^\times=\langle \overline{a},\overline{1+p}\rangle \simeq \mathbb{Z}/(p-1)\mathbb{Z}\times\mathbb{Z}/p^{k-1}\mathbb{Z},$$

où $\overline{a}$ *est un élément d'ordre* $p-1$.

Démonstration. — On commence par le lemme suivant :

Lemme 6.3.17. — *Soit* $n\geq 1$ *et soit* $p>2$ *un nombre premier. Alors*

- $5^{2^n}\equiv 1+2^{n+2} \pmod{2^{n+3}}$;

- $(1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}$.

Démonstration. — Se montre par récurrence ! □

Suite de la preuve de la proposition 6.3.16.
1) Tout d'abord $(\mathbb{Z}/2^k\mathbb{Z})^\times$ est d'ordre 2^{k-1}. C'est donc un 2-groupe. Ensuite, grâce au lemme 6.3.17, $-\overline{1} \notin \langle\overline{5}\rangle$ et $\overline{5}$ est d'ordre 2^{k-2}. En comparant les ordres, $(\mathbb{Z}/2^k\mathbb{Z})^\times = \langle -\overline{1}, \overline{5}\rangle$.
2) Le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est d'ordre $(p-1)p^{k_1}$. Ensuite, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique (car $\mathbb{Z}/p\mathbb{Z}$ est un corps). Comme $(\mathbb{Z}/p^k\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$, il existe un élément $\overline{a} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ d'ordre $p-1$. Ensuite, d'après le lemme 6.3.17, $\overline{1+p}$ est d'ordre p^{k-1}. Ainsi, en comparant les ordres, $\langle \overline{a}, \overline{1+p}\rangle = (\mathbb{Z}/p^k\mathbb{Z})^\times$. □

Exemple 6.3.18. — On veut déterminer le treillis des sous-corps de $\mathbb{Q}(\zeta_8)$. On se rappelle que $\Phi_8 = X^4+1 = \mathrm{Irr}(\zeta_8, \mathbb{Q})$. On a $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \langle -\overline{1}, \overline{5}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: c'est le groupe de Klein. On a donc 3 sous-corps quadratiques stricts : $\mathbb{Q}(\zeta_8)^{\langle -\overline{1}\rangle} = \mathbb{Q}(\zeta_8)^+$, $\mathbb{Q}(\zeta_8)^{\langle -\overline{5}\rangle}$, $\mathbb{Q}(\zeta_8)^{\langle -\overline{5}\rangle}$. On sait déja que $i = \zeta_4 = \zeta_8^2$. Remarquons ensuite que $\sigma_a(\zeta_4) = \zeta_4$ si et seulement si $2(a-1) \equiv 0 \pmod 8$, ainsi $\zeta_4 \in \mathbb{Q}(\zeta_8)^{\langle\overline{5}\rangle}$ et en comparant les degrés, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\zeta_8)^{\langle\overline{5}\rangle}$.
Ensuite $\mathbb{Q}(\zeta_8)^{\langle -\overline{1}\rangle}$ est le sous-corps réel maximal de $\mathbb{Q}(\zeta_8)$. Soit $z = \zeta_8 + \zeta_8^{-1}$. Alors $z^2 = \zeta_8^2 + 2 + \zeta_8^{-2}$. Comme $\zeta_8^4 = -1$, on a $\zeta_8^2 = -\zeta_8^{-2}$. Et ainsi $z^2 = 2$. Comme z est positif, $z = \sqrt{2}$. D'où $\mathbb{Q}(\zeta_8)^{\langle -\overline{1}\rangle} = \mathbb{Q}(\sqrt{2})$. Ainsi, $\mathbb{Q}(\zeta_8)^{\langle -\overline{5}\rangle} = \mathbb{Q}(\sqrt{-2})$ et $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

Exemple 6.3.19. — On veut dresser le treillis des sous-corps de $\mathbb{Q}(\zeta_{20})$. Commençons par le treillis des sous-corps de $\mathbb{Q}(\zeta_5)/\mathbb{Q}$: $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. On a donc un seul sous-corps strict : c'est le corps quadratique $\mathbb{Q}(\zeta_5)^+$. Posons $w = \zeta_5 + \zeta_5^{-1}$. Il faut se rappeler que $\mathrm{Irr}(\zeta_5, \mathbb{Q}) = X^4 + X^3 + X^2 + X + 1$. Ainsi $\zeta_5^{-2} + \zeta_5^{-1} + 1 + \zeta_5 + \zeta_5^2 = 0$. Alors

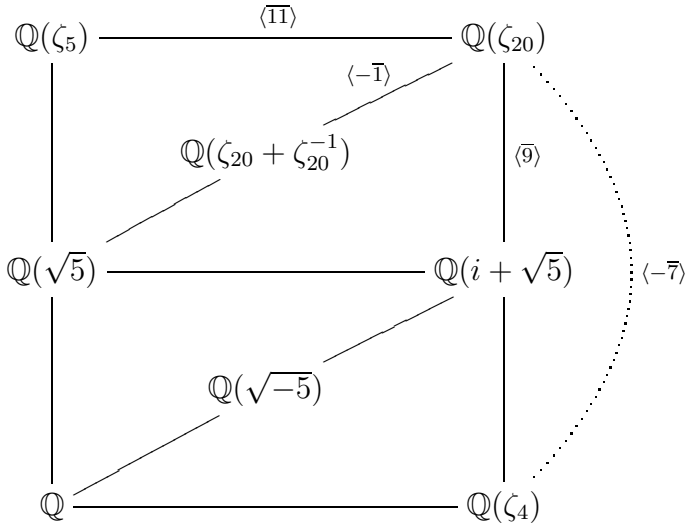
$$w^2 = \zeta_5^2 + \zeta_5^{-2} + 2 = -1 - w + 2.$$

Ainsi $\mathrm{Irr}(w, \mathbb{Q}) = X^2 + X - 1$ puis $w = \dfrac{-1+\sqrt{5}}{2}$ et enfin $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{5})$. Ensuite,

$$(\mathbb{Z}/20\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Le groupe $(\mathbb{Z}/20\mathbb{Z})^\times$ contient :
3 sous-groupes d'ordre 2 : $\langle -\overline{1}\rangle$, $\langle \overline{9}\rangle$ et $\langle \overline{11}\rangle$.
2 sous-groupes cyclique d'ordre 4 : $\langle \overline{7}\rangle$ et $\langle -\overline{7}\rangle$.
1 groupe de Klein : $\langle \overline{9}, -\overline{1}\rangle$.

On peut remarquer que $\zeta_4 = \zeta_{20}^5$ est fixe par σ_{-7}. Ainsi $\mathbb{Q}(\zeta_{20})^{\langle -\overline{7}\rangle} = \mathbb{Q}(\zeta_4)$.
De même $\zeta_5 = \zeta_{20}^4$ est fixe par $\overline{11}$ et ainsi $\mathbb{Q}(\zeta_{20})^{\langle \overline{11}\rangle} = \mathbb{Q}(\zeta_5)$.
Au final, on obtient (en utilisant l'exercice 32) :



6.4. Théorie de Kummer

On rappelle qu'une extension K/k est dite cyclique si elle est galoisienne de groupe de Galois un groupe cyclique.
L'objectif de cette section est de montrer le théorème suivant.

Théorème 6.4.1. — *Soit* k *un corps contenant* μ_n. *(On suppose toujours* n *premier à la caractéristique du corps* k.*)*
(i) Soit $a \in \mathrm{k}^*$. *Alors l'extension* $\mathrm{k}(\sqrt[n]{a})/\mathrm{k}$ *est une extension cyclique de degré* d, *avec* d *divisant* n.
(ii) Réciproquement. Soit K/k *une extension cyclique de degré* d *divisant* n. *Alors il existe* $a \in \mathrm{k}^*$ *tel que* $\mathrm{K} = \mathrm{k}(\sqrt[n]{a})$.

(iii) En outre si $\mathrm{K} = \mathrm{k}(\sqrt[n]{a}) = \mathrm{k}(\sqrt[n]{b})$*, avec* $b \in \mathrm{k}^*$*, alors il existe* $s \in \mathbb{Z}$*,* $(s, n) = 1$*, et* $u \in \mathrm{k}^*$ *tels que* $a = b^s u^n$*.*

La preuve de ce théorème repose sur le théorème 90 de Hilbert. Mais commençons par

***Lemme 6.4.2* (de Dedekind).** — *Soit* K/k *une extension finie dans* $\overline{\mathrm{k}}$/k*. Soient* $\sigma_1, \cdots, \sigma_n$ *des* k*-isomorphismes de* K *dans* $\overline{\mathrm{k}}$*,* 2 *à* 2 *distincts. Alors dans le* $\overline{\mathrm{k}}$*-espace vectoriel des applications de* K *vers* $\overline{\mathrm{k}}$*, les applications* $\sigma_1, \cdots, \sigma_n$ *sont indépendantes.*

Démonstration. — Supposons les $\sigma_1, \cdots, \sigma_n$ liés sur $\overline{\mathrm{k}}$ et n minimal, c'est-à-dire que toute sous-famille de $\sigma_1, \cdots, \sigma_n$ de cardinal au plus $n-1$, est libre. Il existe $\lambda_2, \cdots, \lambda_n \in \overline{\mathrm{k}}$ tels que $\sigma_1 + \lambda_2\sigma_2 + \cdots + \lambda_n\sigma_n = 0$. On a pour tout $x, y \in \mathrm{K}$, $\sigma_i(xy) = \sigma_i(x)\sigma_i(y)$. Ainsi,

$$\sigma_1(x) = -(\lambda_2\sigma_2(x) + \cdots + \lambda_n\sigma_n(x))$$

et

$$\sigma_1(x)\sigma_1(y) + \sum_{i\geq 2} \lambda_i\sigma_i(x)\sigma_i(y) = 0.$$

On obtient

$$\lambda_2 \left(\sigma_1(y) - \sigma_2(y)\right)\sigma_2(x) + \cdots + \lambda_n \left(\sigma_1(y) - \sigma_n(y)\right)\sigma_n(x) = 0.$$

Comme les σ_i sont 2 à 2 distincts, il existe $y \in \mathrm{K}$ tel que $\sigma_1(y) \neq \sigma_2(y)$. Pour un tel y, on a ainsi

$$\lambda_2 \left(\sigma_1(y) - \sigma_2(y)\right)\sigma_2 + \cdots + \lambda_n \left(\sigma_1(y) - \sigma_n(y)\right)\sigma_n = 0,$$

ce qui est une relation de dépendance linéaire sur $\overline{\mathrm{k}}$ non triviale. Ceci contredit la minimalité de n. □

Soit K/k une extension galoisienne de groupe de Galois G et soit $z \in \mathrm{K}$. On rappelle que la norme de z dans K/k (voir section 4.4) est définie par $\mathrm{N}_{\mathrm{K/k}}(z) = \prod_{\sigma\in G} \sigma(z)$.

***Théorème 6.4.3* (Théorème 90 de Hilbert).** — *Soit* K/k *une extension cyclique de groupe de Galois engendré par* σ*. Soit* $z \in \mathrm{K}$*. Alors*

$\mathrm{N}_{\mathrm{K/k}}(z) = 1$ *si et seulement si, il existe* $y \in \mathrm{K}$ *tel que*

$$z = y^{\sigma-1} = \frac{\sigma(y)}{y}.$$

Démonstration. — Soit n le degré de K/k. Posons $\mathrm{N} = \mathrm{N}_{\mathrm{K/k}}$.
•. Supposons que $z = y^{\sigma-1}$. Alors

$$\begin{aligned} \mathrm{N}(y^\sigma) &= (y^\sigma)^{1+\sigma+\cdots+\sigma^{n-1}} \\ &= y^{\sigma+\sigma^2+\cdots+1} \\ &= \mathrm{N}(y) \end{aligned}$$

La norme étant multiplicative, il vient

$$\mathrm{N}(y^{\sigma-1}) = \frac{\mathrm{N}(y^\sigma)}{\mathrm{N}(y)} = 1.$$

• Réciproquement. Soit $z \in \mathrm{K}$ tel que $\mathrm{N}(z) = 1$. Regardons la combinaison linéaire des σ^i

$$\mathrm{id} + z\sigma + z\sigma(z)\sigma^2 + \cdots + z\sigma(z)\cdots\sigma^{n-2}(z)\sigma^{n-1}.$$

D'après le lemme d'indépendance de Dedekind, il existe $x \in \mathrm{K}$, tel que

$$x + z\sigma(x) + z\sigma(z)\sigma^2(x) + \cdots + z\sigma(z)\cdots\sigma^{n-2}(z)\sigma^{n-1}(x) \neq 0.$$

Soit $y = x + z\sigma(x) + z\sigma(z)\sigma^2(x) + \cdots + z\sigma(z)\cdots\sigma^{n-2}(z)\sigma^{n-1}(x)$. Alors

$$\sigma(y) = \sigma(x)+\sigma(z)\sigma^2(x)+\sigma(z)\sigma^2(z)\sigma^3(x)+\cdots+\sigma(z)\cdots\sigma^{n-2}(z)\sigma^{n-1}(z)x$$

puis

$$\begin{aligned} z\sigma(y) &= z\sigma(x) + z\sigma(z)\sigma^2(x) + \cdots + z\sigma(z)\cdots\sigma^{n-2}(z)\sigma^{n-1}(x) + \mathrm{N}(z)x \\ &= y \end{aligned}$$

car $\mathrm{N}(z) = 1$. D'où $z = y^{1-\sigma}$. □

Nous sommes en mesure de démontrer le théorème 6.4.1.

Démonstration. — Posons $\zeta = \zeta_n$.
(i) Les racines du polynôme $X^n - a$ sont $\zeta^i\sqrt{a}$, $i = 1, \cdots, n$. Comme $\zeta \in \mathrm{k}$, les racines de $X^n - a$ sont toutes dans K. L'extension K/k est donc normale (et séparable car n est premier à la caractéristique du corps k). Ainsi K/k est galoisienne de groupe G. Soit $\sigma \in G$. Comme

$\mathrm{Irr}(\sqrt[n]{a}, \mathbb{Q})$ divise $X^n - a$, $\sigma(\sqrt[n]{a}) = \zeta^{a_\sigma}\sqrt[n]{a}$. De plus, comme $\zeta \in \mathrm{k}$, $\sigma_1\sigma_2(\sqrt[n]{a}) = \zeta^{a_{\sigma_1}+a_{\sigma_2}}\sqrt[n]{a}$, ce qui signifie que

$$\begin{array}{rcl} \phi : G & \to & (\mathbb{Z}/n\mathbb{Z}, +) \\ \sigma & \mapsto & a_\sigma \end{array}$$

est un morphisme de groupes. Ce morphisme est clairement injectif. Ainsi $G \hookrightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ et ce dernier est cyclique d'ordre n.

(ii) Soit K/k une extension cyclique de degré d divisant n. Posons $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = G = \langle\sigma\rangle$. Alors $\mathrm{N}(\zeta^{n/d}) = (\zeta^{n/d})^d = 1$. Par le théorème 90 de Hilbert (théorème 6.4.3), il existe $y \in \mathrm{K}^*$ tel que $\zeta^{n/d} = \zeta_d = y^{\sigma-1}$, où $\zeta_d = \zeta^{n/d}$. Ainsi $y^\sigma = \zeta_d y$ puis $\sigma^i(y) = \zeta_d^i y$. On voit ainsi que y a au moins $|d|$ k-conjugués distincts. Or $y \in \mathrm{K}/\mathrm{k}$ avec $[\mathrm{K} : \mathrm{k}] = d$. Ainsi, $\mathrm{K} = \mathrm{k}(y)$. De plus $\sigma(y^n) = \sigma(y)^n = \zeta_d^n y^n = y^n$, ce qui signifie que $y^n \in \mathrm{K}^{\langle\sigma\rangle} = \mathrm{k}$. On pose $a = y^n \in \mathrm{k}$. On a bien $\mathrm{K} = \mathrm{k}(\sqrt[n]{a})$.

Il reste à montrer le dernier point.
(iii) On suppose que $\mathrm{K} = \mathrm{k}(\sqrt[n]{a}) = \mathrm{k}(\sqrt[n]{b})$ et que $[\mathrm{K} : \mathrm{k}] = d$. On sait que $\sigma(\sqrt[n]{a}) = \zeta_d^{a_\sigma}\sqrt[n]{a}$ et que $\sigma(\sqrt[n]{b}) = \zeta_d^{b_\sigma}\sqrt[n]{b}$, où $\zeta_d^{a_\sigma}$ et $\zeta_d^{b_\sigma}$ sont tous les deux d'ordre d. Ainsi, il existe $s \in \mathbb{N}$, $(s, d) = 1$, tel que $\zeta_d^{sb_\sigma} = \zeta_d^{a_\sigma}$. On peut s'assurer que s est aussi premier à n (relèvement des classes inversibles à venir). Par conséquent,

$$\sigma\left(\frac{\sqrt[n]{a}}{\sqrt[n]{b}^s}\right) = \frac{\zeta_d^{a_\sigma}\sqrt[n]{a}}{\zeta_d^{sb\sigma}\sqrt[n]{b}^s} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}^s},$$

et donc $\dfrac{\sqrt[n]{a}}{\sqrt[n]{b}^s} = u \in \mathrm{k}^*$, d'où le résultat.
Pour que la preuve soit complète, il nous reste à rappeler le

Théorème 6.4.4 **(Relèvement des classes inversibles)**
Soit $d|n$. Alors le morphisme de restriction $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$ est surjectif.

Démonstration. — On écrit $n = DN$, avec $d|D$ et $(D, N) = 1$. Soit alors a premier à d. Par le théorème des restes chinois, il existe $x \in \mathbb{Z}$ tel que $x \equiv a \pmod{D}$ et $x \equiv 1 \pmod{N}$. Ainsi $x \equiv a \pmod{d}$ car d divise D et

$(x, n) = 1$: en effet, si un nombre premier ℓ divise x et n, alors ℓ divise x et D ou N, ce qui est absurde. □

□

Corollaire 6.4.5. — *Soit $a \in \mathrm{k}$. (On suppose toujours n premier à la caractéristique du corps* k *et que* k *contient μ_n.) Le polynôme $P = X^n - a$ est irréductible sur k si et seulement si $a \notin \mathrm{k}^\ell$ pour tout premier ℓ divisant n.*

Démonstration. — Ecrivons $n = \ell n_1$.
• Supposons que $a = b^\ell$, $b \in \mathrm{k}^*$. Alors

$$P = X^{\ell n_1} - b^\ell = b^\ell((X^{n_1}/b)^\ell - 1)$$

n'est pas irréductible sur k.
• Supposons P non irréductible sur k. Alors $\mathrm{k}(\sqrt[n]{a})/\mathrm{k}$ est cyclique de degré d divisant n, $d < n$. D'après le théorème 6.4.1, il existe $b \in \mathrm{k}$ tel que $\mathrm{k}(\sqrt[n]{a}) = \mathrm{k}(\sqrt[d]{b}) = \mathrm{k}(\sqrt[n]{b^{n_1}})$, où $n = dn_1$. Toujours d'après le théorème 6.4.1, il existe $u \in \mathrm{k}^*$ tel que $a = b^{sn_1}u^n$, $(s, n) = 1$. Comme $d < n$, l'entier n_1 est strictement plus grand que 1. Soit un premier ℓ divisant n_1 (donc n). Alors $a \in (\mathrm{k}^*)^\ell$. □

Exemple 6.4.6. — Le polynôme $P = X^4 - 3$ est irréductible sur $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$. En effet, il suffit de vérifier que 3 n'est pas un carré dans $\mathbb{Q}(i)$, ou encore que $\sqrt{3} \notin \mathbb{Q}(i)$, ce qui est immédiat.

Exemple 6.4.7. — Soit k un corps de caractéristique différente de 2. Comme k contient ± 1, les extensions quadratiques K/k de k sont en correspondance bijective avec les classes de $\mathrm{k}^*/(\mathrm{k}^*)^2$ (à la classe triviale correspond le corps k). En effet, soit K/k une extension quadratique de k. D'après la théorie de Kummer, il existe $d \in \mathrm{k}$ tel que $\mathrm{K} = \mathrm{k}(\sqrt{d})$. Á K/k, on associe $\overline{d} \in \mathrm{k}^*/(\mathrm{k}^*)^2$. La théorie de Kummer indique de plus que $\mathrm{k}(\sqrt{d}) = \mathrm{k}(\sqrt{d'})$ si et seulement si $\overline{d} = \overline{d'}$.
Quand $\mathrm{k} = \mathbb{Q}$, on peut s'assurer que $d \in \mathbb{Z}$, et même mieux, que d est sans facteur carré (sfc). Dans ce cas, pour d et d' dans $\mathbb{Z}$ et sfc, il vient $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ si et seulement si $d = d'$.

6.5. Exercices

6.5.1. Enoncés. —

Exercice 45. — *Déterminer, sous la forme* $\mathbb{F}_{p^t}$*, les corps finis suivants :* $\mathbb{F}_7(\mu_5)$ *;* $\mathbb{F}_7(\mu_{25})$ *;* $\mathbb{F}_7(\mu_{33})$ *;* $\mathbb{F}_5(\mu_7)$ *;* $\mathbb{F}_{31}(\mu_5)$.

Exercice 46. —
1) Sur $\mathbb{Z}$*, calculer* Φ_{15}.
2) Déterminer, sous la forme $\mathbb{F}_{2^t}$*, le corps fini* $\mathbb{F}_2(\mu_{15})$*. En déduire l'existence de deux polynômes* P_1 *et* P_2*, de degré* 4*, irréductibles et unitaires de* $\mathbb{F}_2[X]$*, tels que* $\Phi_{15} = P_1P_2$*. Trouver* P_1 *et* P_2.

Exercice 47. — *[Étude de* $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$*]*
Soit $\zeta_n = \exp(2i\pi/n)$.
1) Déterminer ϕ_{16} *et* $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}]$.
2) Déterminer la structure de $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$.
3) Déterminer le treillis des sous-groupes de G.
4) Tracer le schéma des sous-corps de $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ *en faisant ressortir les sous-corps cyclotomiques et les sous-corps réels maximaux.*
5) Déterminer un générateur pour chaque sous-corps de $\mathbb{Q}(\zeta_{16})$.

Exercice 48. — *Soit* p *un nombre premier,* $p \neq 2$*, et soit* $\zeta = \zeta_p = \exp(2i\pi/p)$ *une racine primitive* p^{eme} *de l'unité dans* $\mathbb{C}$ *;* $\mathrm{K} = \mathbb{Q}(\zeta)$.
On veut montrer que K *contient* $\sqrt{(-1)^{(p-1)/2}p}$.
Pour $x \in \mathrm{K}$*, on notera* $\mathrm{N}x = \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)$ *la norme de* x *dans l'extension* $\mathrm{K}/\mathbb{Q}$.
1) Calculer $\mathrm{N}(\zeta - 1)$*,* $\mathrm{N}(1 + \zeta)$ *et en déduire* $\mathrm{N}(\zeta - \zeta^{-1})$.
2) Soient $\omega = \prod_{a=1}^{t}(\zeta^a - \zeta^{-a})$ *et* $\omega' = \prod_{a=t+1}^{p-1}(\zeta^a - \zeta^{-a})$*, où* $t = (p-1)/2$.
a) Comparer ω *et* ω'.
b) En déduire ω^2.
c) Conclure.
3) Application.
a) Quel est le nombre d'extensions quadratiques de $\mathbb{Q}$ *contenues dans* $\mathbb{Q}(\zeta_{105})$ *?*
b) Donner toutes les sous-extensions quadratiques $\mathrm{K}/\mathbb{Q}$ *de* $\mathbb{Q}(\zeta_{105})/\mathbb{Q}$.

Exercice 49. — *Soit* $\zeta = \zeta_{15} = \exp(2i\pi/15) \in \mathbb{C}$. *Posons* $\mathrm{K} = \mathbb{Q}(\zeta)$.
1) Soit $\zeta_5 = \zeta^3$. *Calculer* $\zeta_5 + \zeta_5^{-1}$.
2) Déterminer le treillis des sous-corps de $\mathrm{K}/\mathbb{Q}$.
3) Exprimer ζ_5 *à l'aide de racines carrées.*
4) Trouver $\mathrm{Irr}(\zeta_5, \mathbb{Q}(\zeta_{15}))$. *En déduire* ζ_{15} *à partir de racines carrées.*
5) Soit $y = \zeta + \zeta^{-1}$. *Trouver* $\mathrm{Irr}(y, \mathbb{Q}(\sqrt{5}))$. *En déduire une seconde expression de* ζ_{15}.

Exercice 50. — *Soit* K/k *une extension galoisienne. Montrer que l'application* k*-linéaire* $\mathrm{Tr}_{\mathrm{K}/\mathrm{k}} : \mathrm{K} \to \mathrm{k}$ *est surjective.*

Exercice 51. — *Soient* $\mathrm{k} = \mathbb{F}_q$ *et* $\mathrm{K} = \mathbb{F}_{q^d}$.
1) Déterminer $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$.
2) Pour $x \in \mathrm{K}$, *écrire l'expression de* $\mathrm{N}_{\mathrm{K}/\mathrm{k}}(x)$ *(norme de* x*) puis de* $\mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(x)$ *(trace de* x*). (Voir la section 4.4.)*
3) Pour tout y *dans* K, *montrer que* $\mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(y^q - y) = 0$.
4) On considère

$$\begin{array}{rcl} \phi : (\mathrm{K}, +) & \to & (\mathrm{K}, +) \\ y & \mapsto & y^q - y \end{array}$$

a) Montrer que ϕ *est un homomorphisme de groupes.*
b) Déterminer $\ker(\phi)$ *; en déduire* $|\mathrm{Im}(\phi)|$.
c) Montrer que $\mathrm{Tr}_{\mathrm{K}/\mathrm{k}} : (\mathrm{K}, +) \to (\mathrm{k}, +)$ *est un morphisme surjectif.*
d) En déduire que $\mathrm{Im}(\phi) = \ker(\mathrm{Tr}_{\mathrm{K}/\mathrm{k}})$, *puis que* $\mathrm{Tr}_{\mathrm{K}/\mathrm{k}}(x) = 0$ *si et seulement si, il existe* $y \in \mathrm{K}$ *tel que* $x = y^q - y$.

Exercice 52. — *Soient* $\mathrm{k} = \mathbb{F}_q$ *et* $\mathrm{K} = \mathbb{F}_{q^d}$. *Montrer que la norme* $\mathrm{N}_{\mathrm{K}/\mathrm{k}} : \mathrm{K} \to \mathrm{k}$ *est surjective.*

Exercice 53. — *Soit* $a \in \mathbb{Z} - \{0\}$ *et soit* $P = X^n - a \in \mathbb{Z}[X]$. *On désigne par* L *le corps des racines de* P *sur* $\mathbb{Q}$ *dans* $\overline{\mathbb{Q}}$ *et soit* θ *une racine de* P. *Soit* $\mathrm{k} = \mathbb{Q}(\zeta_n)$, *où* $\zeta = \zeta_n = \exp(2i\pi/n)$.
1) Montrer que $\mathrm{L} = \mathbb{Q}(\zeta, \theta)$.
2) On suppose P *irréductible et* n *et* $\varphi(n)$ *étrangers. Que vaut* $[\mathrm{L} : \mathbb{Q}]$ *?*
3) Lorsque P *est réductible dans* $\mathrm{k}[X]$, *montrer que* $X^n - a$ *se décompose dans* $\mathrm{k}[X]$ *en un produit de* δ *polynômes irréductibles de degré* d *(donc* $n = \delta d$*), polynômes tous de la forme* $X^d - c_i$, $c_i \in \mathrm{k}$, *et que chacun de ces polynômes ont le même corps des racines sur* k, *le corps* L.

4) Calculer $[\mathrm{L} : \mathbb{Q}]$ *quand* $P = X^p - p$, $P = X^8 - p$, p *premier,* $P = X^8 + 100$ *puis* $P = X^6 + 3$.

Exercice 54. — *Soit* $P = X^8 - 3$ *et soit* L *le corps des racines de* P *sur* $\mathbb{Q}$. *Soit* θ *une racine de* P *dans* $\overline{\mathbb{Q}}$ *et* $\zeta = \zeta_8 = \exp(2i\pi/8)$.
Posons $\mathrm{K} = \mathbb{Q}(\theta)$ *et* $\mathrm{k} = \mathbb{Q}(\zeta)$.
1) Montrer que $\mathrm{L} = \mathbb{Q}(\theta, \zeta)$ *et déterminer* $[\mathrm{L} : \mathbb{Q}]$.
2) Montrer que $\mathrm{K} \cap \mathrm{k} = \mathbb{Q}$.
3) On rappelle que $\mathrm{k} = \mathbb{Q}(i, \sqrt{2})$.
a) Montrer que $\mathrm{K}/\mathbb{Q}$ *n'est pas galoisienne.*
b) Déterminer $[\mathbb{Q}(\theta^2, i) : \mathbb{Q}]$ *et montrer que* $\mathbb{Q}(\theta^2, i)/\mathbb{Q}$ *est galoisienne.*
c) Déterminer $[\mathbb{Q}(\theta, i) : \mathbb{Q}]$ *et montrer que* $\mathbb{Q}(\theta, i)/\mathbb{Q}$ *n'est pas galoisienne.*
4) Montrer que $G = \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ *est produit semi-direct interne d'un groupe* H *cyclique d'ordre* 8 *par un sous-groupe* Δ *isomorphe au groupe de Klein.*

Exercice 55. — *Soit* k/k_0 *une extension galoisienne de corps de caractéristique différente de* p. ; $\Delta = Gal(\mathrm{k}/\mathrm{k}_0)$.
On suppose que k *contient* ζ_p.
Soit K/k *une extension cyclique de degré* p ; $G = Gal(\mathrm{K}/\mathrm{k})$. *On sait par la théorie de Kummer qu'il existe* $x \in \mathrm{k}$, *tel* $\mathrm{K} = \mathrm{k}(\sqrt[p]{x})$.
1) Montrer que K/k_0 *est galoisienne si et seulement si*

$$\forall \sigma \in \Delta, \exists r \in \mathbb{Z}, (r, p) = 1, \sigma(x)/x^r \in \mathrm{k}^p.$$

2) Soient $\ell > 2$ *et* p *deux nombres premiers distincts et soit l'extension quadratique* $\mathrm{k} = \mathbb{Q}(\sqrt{\ell})/\mathbb{Q}$. *Soit* $x = p + \sqrt{-\ell} \in \mathrm{k}$. *Posons* $\mathrm{K} = \mathrm{k}(\sqrt{x})$.
a) Montrer que $\mathrm{K}/\mathbb{Q}$ *est galoisienne si et seulement si* $\ell = 2p - 1$.
b) Lorsque $\mathrm{K}/\mathbb{Q}$ *est galoisienne, déterminer* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ *puis les sous-corps de* $\mathrm{K}/\mathbb{Q}$.
3) Soit $\mathrm{k} = \mathbb{Q}(j) = \mathbb{Q}(\zeta_3)$ *et soit* $P = X^3 - (1 + \sqrt{-3})$.
Soit θ *une racine de* P *dans* $\overline{\mathbb{Q}}$ *et soit* $\mathrm{K} = \mathrm{k}(\theta)$.
a) Calculer $[\mathrm{K} : \mathbb{Q}]$.
b) Etudier si l'extension $\mathrm{K}/\mathbb{Q}$ *est galoisienne.*

Exercice 56. — *Soit* $n \in \mathbb{N}^*$. *Le but de l'exercice est de montrer l'existence d'une infinité de nombres premiers* p *satisfaisant*

$$p \equiv 1 \ (mod\ n).$$

On note par ϕ_n le n^{eme}-polynôme cyclotomique.
1) Montrer que $\phi_n(0) = \pm 1$.
2) Soit p un nombre premier étranger à n et soit $a \in \mathbb{Z}$.
On veut montrer que $p|\Phi_n(a)$ si et seulement si $a \pmod p$ est d'ordre n dans ${\mathbb{F}_p}^\times$.
a) On suppose que $p|\Phi_n(a)$.
i) Montrer que $a^n \equiv 1 \pmod p$.
ii) Soit k l'ordre de a dans ${\mathbb{F}_p}^\times$. On suppose $k < n$. Montrer que $a^n \equiv 1 \pmod{p^2}$ et que $(a+p)^n - 1 \equiv 0 \pmod{p^2}$. En déduire que $k = n$.
b) Montrer la réciproque.
3) On suppose toujours $(p, n) = 1$. Montrer que $p|\Phi_n(a)$ pour un certain entier a si et seulement si $p \equiv 1 \pmod n$.
4) Supposons qu'il n'existe qu'un nombre fini de premiers $p_1, \cdots, p_r$ congrus à 1 modulo n. Soit $M = p_1 \cdots p_r$ et soit $N \in \mathbb{Z}$.
a) Montrer que $\Phi_n(NM)$ n'est divisible par aucun des p_i.
b) Montrer que pour N assez grand, $\Phi_n(NM) \neq \pm 1$, ainsi qu'il existe un premier p qui divise $\Phi_n(NM)$.
c) Montrer que $p \equiv 1 \pmod n$, puis conclure.

***Exercice 57* (Galois inverse pour les groupes abéliens)**
Le but de l'exercice est de montrer le résultat suivant. Soit G un groupe abélien fini. Alors il existe une extension galoisienne $\mathrm{K}/\mathbb{Q}$ telle que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq G$.
Notons par C_n le sous-groupe cyclique d'ordre n.
1) Supposons G cyclique d'ordre ℓ^r, où ℓ est un nombre premier. En s'appuyant sur l'exercice 56, montrer qu'il existe un premier p tel que $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ contient une sous-extension $\mathrm{K}/\mathbb{Q}$ cyclique de degré n.
2) Supposons $G \simeq C_{\ell^r} \times C_{\ell^s}$. Montrer que l'on peut trouver deux nombres premiers p_1 et p_2 tel que $\mathbb{Q}(\zeta_{p_1 p_2})/\mathbb{Q}$ contient une sous-extension $\mathrm{K}/\mathbb{Q}$ de groupe de Galois isomorphe à G.
3) Montrer le cas général.

Exercice 58. — *On souhaite déterminer tous les entiers $x, y, z \in \mathbb{Z}$ tels que $x^2 + y^2 = z^2$.*
1) Caractériser les éléments de $\mathbb{Q}(i)$ de norme 1.

2) En déduire que les solutions de $x^2+y^2=z^2, z>0$, vérifient

$$(*)\begin{cases} \dfrac{x}{z}=\dfrac{u^2-v^2}{u^2+v^2}\ ,\ \dfrac{y}{z}=\dfrac{2uv}{u^2+v^2} \\ \\ u,v\in\mathbb{Z},\quad (u,v)=1 \end{cases}$$

3) On suppose u et v de parités différentes (et premiers entre eux). Montrer que $x=u^2-v^2$, $y=2uv$, $z=u^2+v^2$ est solution de $(*)$ avec x,y,z premiers entre eux.
4) On suppose u et v impairs (et premiers entre eux) et soit x,y,z vérifiant $(*)$. Démontrer qu'il existe $a,b\in\mathbb{Z}$, $(a,b)=1$, a et b de parités différentes tels que $x=2ab$, $y=a^2-b^2$, $z=a^2+b^2$, et x,y,z premiers entre eux.
5) Résoudre dans $\mathbb{Z}$ l'équation $x^2+y^2=z^2$.

6.5.2. Solutions. —

Exercice 45.
Pour $(n,q)=1$, on rappelle que $\mathbb{F}_q(\mu_n)=\mathbb{F}_{q^t}$, où t est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.
Ainsi $\mathbb{F}_7(\mu_5)=\mathbb{F}_{7^4}$, $\mathbb{F}_7(\mu_{25})=\mathbb{F}_{7^4}$, $\mathbb{F}_7(\mu_{33})=\mathbb{F}_{7^{10}}$, $\mathbb{F}_5(\mu_7)=\mathbb{F}_{5^6}$ et $\mathbb{F}_{31}(\mu_5)=\mathbb{F}_{31}$.

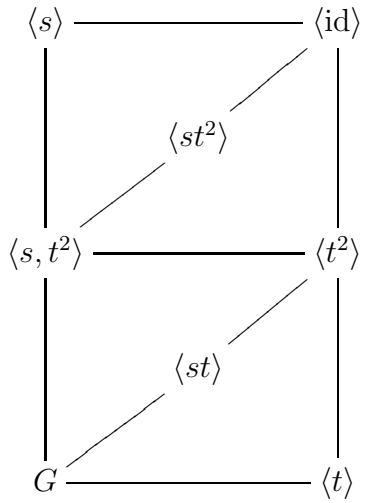
Exercice 46.
1) $\Phi_5=X^4+X^3+X^2+X+1$ et $\Phi_3=X^2+X+1$. De l'égalité $\Phi_3(X^5)=\Phi_{15}\Phi_3$, on en déduit, après division euclidienne, $\Phi_{15}=X^8-X^7+X^5-X^4+X^3-X+1$.
2) Il faut déterminer l'ordre de 2 dans $(\mathbb{Z}/15\mathbb{Z})^\times\simeq(\mathbb{Z}/3\mathbb{Z})^\times\times(\mathbb{Z}/5\mathbb{Z})^\times$. L'élément $2^2=4$ a pour image $(\overline{1},-\overline{1})$ ainsi 2 est d'ordre 4 et donc $\mathbb{F}_2(\mu_{15})=\mathbb{F}_{2^4}$.
3) Le polynôme $\phi_{15}\in\mathbb{F}_2[X]$ est d'ordre 8. Soit α une racine de ϕ_{15} dans $\overline{\mathbb{F}_2}$. Alors α engendre μ_{15} et donc $\mathbb{F}_2(\alpha)=\mathbb{F}_2(\mu_{15})$. D'après la question 2), α est d'ordre 4 sur $\mathbb{F}_2$ et ainsi $\mathrm{Irr}(\alpha,\mathbb{F}_2)$ est de degré 4, d'où le résultat.
On rappelle qu'il n'existe qu'un seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$: X^2+X+1 (cf exercice 40).

Ainsi un polynôme $P \in \mathbb{F}_2[X]$ de degré 4 unitaire, est irréductible si et seulement si, $P(0)$ et $P(1)$ sont non nuls et $P \neq (X^2+X+1)^2 = X^4+X^2+1$.
Ainsi X^4+X^3+1, X^4+X+1 et $X^4+X^3+X^2+X+1$ sont les seuls polynômes de degré 4 irréductibles sur $\mathbb{F}_2$.
On vérifie alors que $\phi_{15} = (X^4+X^3+1)(X^4+X+1)$.

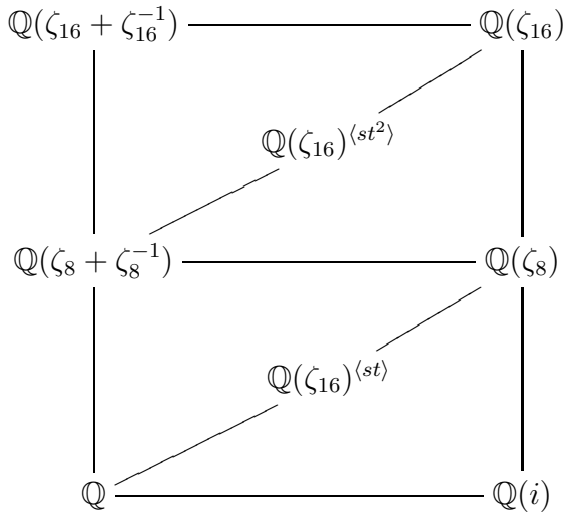
Exercice 47.
1) $\phi_2 = X+1$, $\phi_4 = \phi_2(X^2)$, $\phi_8 = \phi_4(X^2)$ et $\phi_{16} = \phi_8(X^2) = X^8+1$.
Ensuite $[\mathbb{Q}(\zeta_{16})/\mathbb{Q}] = \deg(\phi_{16}) = 8$.
2) D'après la proposition 6.3.16,

$$(\mathbb{Z}/16\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} = \langle -\overline{1}\rangle \oplus \langle \overline{5}\rangle.$$

Posons $s : \zeta_{16} \mapsto \zeta_{16}^{-1}$ et $t : \zeta_{16} \mapsto \zeta_{16}^{5}$. L'élément s est d'ordre 2 et t est d'ordre 4.
3) L'ordre d'un sous-groupe H de G divise 8. On a ainsi
3 sous-groupes d'ordre 2 : $\langle s\rangle$, $\langle t^2\rangle$, $\langle st^2\rangle$;
2 sous-groupes cyclique d'ordre 4 : $\langle t\rangle$, $\langle st\rangle$;
1 groupe de Klein : $\langle s, t^2\rangle$;
1 groupe d'ordre 8 : G.
On obtient le treillis des sous-groupes de G :



4) Les sous-corps cyclotomiques de $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ sont : $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ et $\mathbb{Q}(\zeta_2) = \mathbb{Q}(-1) = \mathbb{Q}$.
On note que $\mathbb{Q}(\zeta_{16})^+ = \mathbb{Q}(\zeta_{16})^{\langle s \rangle}$.
Ensuite $s(\zeta_8) = s(\zeta_{16}^2) = \zeta_{16}^{-2} = \zeta_8^{-1}$ et $t(\zeta_8) = t(\zeta_{16}^2) = \zeta_8^5$. Ainsi $t^2(\zeta_8) = \zeta_8^{25} = \zeta_8$. Par conséquent, $\mathbb{Q}(\zeta_8) \subset \mathbb{Q}(\zeta_{16})^{\langle t^2 \rangle}$. En comparant les degrés, on conclut à $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\zeta_{16})^{\langle t^2 \rangle}$ et $\mathbb{Q}(\zeta_{16})^{\langle s, t^2 \rangle} = \mathbb{Q}(\zeta_8)^+$.
De même, $\zeta_4 = \zeta_{16}^4$, $t(\zeta_4) = \zeta_4^5 = \zeta_4$ et ainsi $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\zeta_{16})^{\langle t \rangle}$, $\mathbb{Q}(\zeta_4)^+ = \mathbb{Q}$.



5) Il nous faut trouver un générateur de $\mathbb{Q}(\zeta_{16})^{st}$ et de $\mathbb{Q}(\zeta_{16})^{\langle st^2 \rangle}$.

Soit $x = \zeta_8 + \zeta_8^{-1}$. Cherchons $\mathrm{Irr}(x, \mathbb{Q})$. On sait que $\mathrm{Irr}(\zeta_8, \mathbb{Q}) = X^4 + 1$, d'où $\zeta_8^2 + \zeta_8^{-2} = 0$. Alors $x^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = 2$ et donc $x = \sqrt{2}$. Par conséquent, $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ et $\mathbb{Q}(\zeta_{16})^{\langle st \rangle} = \mathbb{Q}(\sqrt{-2})$.
Au passage, on a montré que $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

Il reste à étudier $\mathrm{K} = \mathbb{Q}(\zeta_{16})^{\langle st^2 \rangle}$. On sait que $z = \mathrm{Tr}_{\mathbb{Q}(\zeta_{16})/\mathrm{K}}(\zeta_{16}) \in \mathrm{K}$. Vérifions que z n'est pas dans un sous-corps strict de K. Tout d'abord

$$z = (\mathrm{id} + st^2)(\zeta_{16}) = \zeta_{16} + \zeta_{16}^7.$$

Si z était dans un sous-corps strict de K, alors par la théorie de Galois, z serait fixe par $\langle s, t^2\rangle$, en particulier par s et on obtiendrait la relation

$$\zeta_{16} + \zeta_{16}^7 = \zeta_{16}^{-1} + \zeta_{16}^{-7},$$

ou encore $\sin(2\pi/16) = \sin(2 \cdot 7\pi/16)$, ce qui est absurde.
Ainsi $\mathrm{K} = \mathbb{Q}(\zeta_{16})^{\langle st^2\rangle} = \mathbb{Q}(\zeta_{16} + \zeta_{16}^7)$.

Remarque. On pourra noter que l'utilisation de la norme au lieu de la trace n'aurait rien donné puisque $\mathrm{N}_{\mathbb{Q}(\zeta_{16})/\mathrm{K}}(\zeta_{16}) = -1$ est dans un sous-corps strict de K !

Exercice 48.
1) On a $\mathrm{K} = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta + 1) = \mathbb{Q}(\zeta - 1)$. Ainsi (d'après le corollaire 4.4.6) $\mathrm{N}(1 + \zeta) = \mathrm{Irr}(1 + \zeta, \mathbb{Q})(0)$ et $\mathrm{N}(1 - \zeta) = \mathrm{Irr}(\zeta - 1, \mathbb{Q})(0)$.
On rappelle que $P = \mathrm{Irr}(\zeta, \mathbb{Q}) = X^{p-2} + X^{p-2} + \cdots + 1$.
Le polynôme $Q = P(X - 1)$ admet $1 + \zeta$ comme racine, est unitaire et de degré $p - 1$. Ainsi $Q = \mathrm{Irr}(\zeta, \mathbb{Q})$. De même, $P(X + 1) = \mathrm{Irr}(\zeta - 1, \mathbb{Q})$.
Ainsi $\mathrm{N}(1 + \zeta) = Q(0) = P(-1) = 1$, $\mathrm{N}(\zeta - 1) = P(1) = p$ et enfin

$$\begin{aligned}
\mathrm{N}(\zeta - \zeta^{-1}) &= \mathrm{N}(\zeta^{-1}(\zeta^2 - 1)) \\
&= \mathrm{N}(\zeta^{-1})\mathrm{N}(\zeta - 1)\mathrm{N}(\zeta + 1) \\
&= (\mathrm{N}(\zeta))^{-1}\mathrm{N}(-1)\mathrm{N}(1 - \zeta)\mathrm{N}(1 + \zeta) \\
&= p.
\end{aligned}$$

2) a) Soit $t + 1 \leq a \leq p - 1$. Alors comme $\zeta^p = 1$, il vient

$$\zeta^a - \zeta^{-a} = \zeta^{a-p} - \zeta^{-a+p} = -(\zeta^{-a+p} - \zeta^{a-p}) = -(\zeta^b - \zeta^{-b}),$$

avec $1 \leq b \leq t$, après avoir posé $b = p - a$. Ainsi

$$\omega' = (-1)^t\omega = (-1)^{(p-1)/2}\omega.$$

b) On a

$$(-1)^t\omega^2 = \omega\omega' = \prod_{a=1}^{p-1}(\zeta^a - \zeta^{-a}) = \mathrm{N}(\zeta - \zeta^{-1}) = p,$$

c'est-à-dire $\omega^2 = \sqrt{(-1)^t p}$.
c) Ainsi $\sqrt{(-1)^t p} = \pm\omega \in \mathrm{K}$.

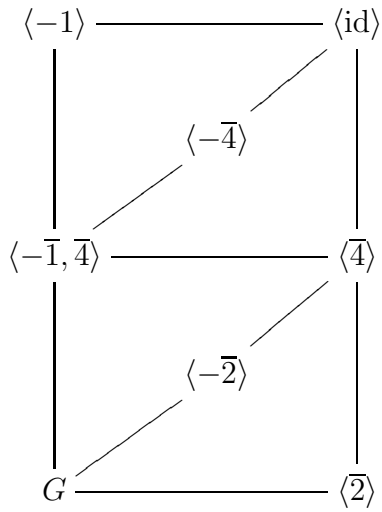
3) a) Commençons par donner la structure de $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{105})/\mathbb{Q})$:

$$\begin{array}{rcl} \mathrm{Gal}(\mathbb{Q}(\zeta_{105})/\mathbb{Q}) & \simeq & (\mathbb{Z}/105\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \\ & \simeq & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}. \end{array}$$

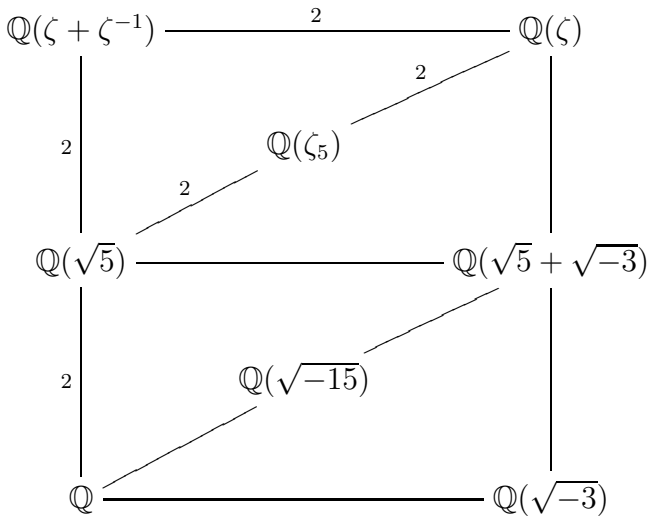
Les extensions quadratiques de $\mathbb{Q}(\zeta_{105})/\mathbb{Q}$ sont fixes par G^2 (voir l'exercice 33). Ainsi, par la théorie de Galois, les extensions quadratiques de $\mathbb{Q}(\zeta_{105})/\mathbb{Q}$ sont en correspondance avec les sous-groupes d'indice 2 de $G/G^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3$. Il faut voir ce dernier quotient comme un espace vectoriel de dimension 3 sur $\mathbb{F}_2$. Alors les sous-groupes d'indice 2 sont en correspondance avec les sous-espaces vectoriels de dimension 2 de $\mathbb{F}_2^3$.
Se donner un sous-espace vectoriel de dimension 2 de $\mathbb{F}_2^3$, c'est se donner une famille libre de deux vecteurs $(\varepsilon_1, \varepsilon_2)$. Pour ε_1, on a à priori $2^3 - 1$ possibilités (ne pas oublier de retire le vecteur nul). Le vecteur ε_2 ne doit pas être parallèle à ε_1, et on a alors $8 - 2$ possibilités (sur $\mathbb{F}_2$, il y a 2 vecteurs parallèles à ε_1). Au total, on obtient $7 \cdot 6 = 42$ possibilités.
Ensuite, il faut noter que deux sous-espaces vectoriels de dimension 2 sont identiques si et seulement si, on passe d'une base à l'autre via une matrice de $\mathrm{Gl}_2(\mathbb{F}_2)$. Comme $|\mathrm{Gl}_2(\mathbb{F}_2)| = 6$ (voir la feuille d'exercice numéro 2), on a donc au total $42/6 = 7$ sous-espaces vectoriels de dimension 2 de $\mathbb{F}_2^3$. Ainsi $\mathbb{Q}(\zeta_{105})/\mathbb{Q}$ contient 7 extensions quadratiques.
b) D'après la question 1), on sait que $\mathbb{Q}(\zeta_{105})$ contient $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-7})$. Puis, par compositum, $\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{21})$, $\mathbb{Q}(\sqrt{-35})$, $\mathbb{Q}(\sqrt{105})$. Ces corps quadratiques sont deux à deux disctincts. Ils sont au nombre de sept : on les a tous !

Exercice 49.
1) Partons du polynôme irréductible de ζ_5 : $\mathrm{Irr}(\zeta_5, \mathbb{Q}) = X^4 + X^3 + X^2 + X + 1$.
Soit $z = \zeta_5 + \zeta_5^{-1}$. Alors $z^2 + z = \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 2 = 1$. Ainsi z est racine de $X^2 + X - 1$. Comme z est positif, on obtient $z = \dfrac{-1 + \sqrt{5}}{2}$.
2) L'extension $\mathrm{K}/\mathbb{Q}$ est galoisienne de groupe de Galois $G \simeq (\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
L'élément $-\overline{1}$ est d'ordre 2. Il nous faut trouver un élément d'ordre 4 ne contenant pas $-\overline{1}$. Par exemple $\overline{2}$. Ainsi $G = \langle -\overline{1} \rangle \times \langle \overline{2} \rangle$. Nous avons le

treillis des sous-groupes de G :



On sait que K contient $\zeta_5 = \zeta^3$ et $\zeta_3 = \zeta^5$.
Soit $\sigma_a : \zeta \mapsto \zeta^a$. Alors σ_a laisse fixe ζ^3 si et seulement si $3a \equiv 3 (\mathrm{mod}\ 15)$, et ainsi $\zeta_5 \in \mathrm{K}^{\langle -\overline{4} \rangle}$. En comparant les degrés, on obtient $\mathbb{Q}(\zeta_5) = \mathrm{K}^{\langle -\overline{4} \rangle}$.
De même, ζ_3 est fixe par σ_a si et seulement si $5a \equiv 5 (\mathrm{mod}\ 15)$. Ainsi, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) = \mathrm{K}^{\langle -\overline{2} \rangle}$.
Le corps $\mathrm{K}^{\langle -\overline{1} \rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$ est le sous-corps réel maximal de K et $\mathrm{K}^{\langle -\overline{1}, \overline{4} \rangle} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$. Enfin $\mathrm{K}^{\langle \overline{4} \rangle}$ est donc l'extension bi quadratique $\mathbb{Q}(\sqrt{-3}, \sqrt{5}) = \mathbb{Q}(\sqrt{5} + \sqrt{-3})$ et donc $\mathrm{K}^{\langle -\overline{2} \rangle} = \mathbb{Q}(\sqrt{-15})$.



3) On rappelle que $z = \zeta_5 + \zeta_5^{-1}$. L'élément ζ_5 est racine de $Q = X^2 - zX + 1$. Le discriminant de Q vaut $z^2 - 4 = -\dfrac{5+\sqrt{5}}{2}$. En notant que la partie imaginaire de ζ_5 est positive, on obtient au final

$$\zeta_5 = \frac{-1+\sqrt{5}+i\sqrt{2(5+\sqrt{5})}}{4}.$$

4) On rappelle tout d'abord que (voir l'exercice 46) : $\Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$.
Posons $\mathrm{k} = \mathbb{Q}(\zeta_5) = \mathrm{K}^{\langle -4\rangle}$. Les k-conjugués de ζ sont $\sigma(\zeta)$, avec $\sigma \in \mathrm{Gal(K/k)}$, c'est-à-dire ζ et $\zeta^{-4} = \zeta^{11}$.
Ainsi $\mathrm{Irr}(\zeta, \mathrm{k}) = (X-\zeta)(X-\zeta^{11}) = X^2 - (\zeta+\zeta^{11})X + \zeta^{12})$. Or $\zeta^{12} = (\zeta^3)^4 = \zeta_5^4 = \overline{\zeta_5} = -(1+\zeta_5+\zeta_5^2+\zeta_5^3)$.
Il reste à exprimer $\zeta + \zeta^{11}$ en fonction de $\zeta_5 = \zeta^3$.
Utilisons maintenant Φ_{15}. Le reste de la division euclidienne de $X^{11}+X$ par Φ_{15} est égal à $-X^6$. Ainsi $\zeta + \zeta^{11} = -\zeta^6 = -\zeta_5^2$. On obtient alors

$$\mathrm{Irr}(\zeta, \mathrm{k}) = X^2 - \zeta_5^2 X + \zeta_5^4.$$

Le polynôme $\mathrm{Irr}(\zeta, \mathrm{k})$ a pour discriminant $\delta = -3\zeta_5^4 = -3\overline{\zeta_5}$.
Ainsi

$$\zeta_{15} = \frac{\zeta_5^2 + i\sqrt{3}\sqrt{\zeta_5}}{2},$$

bien sûr un choix de signe doit être fait au moment de l'extraction de la racine carrée de ζ_5 ... Par exemple, si l'on pose $\zeta_{10} = \exp(2i\pi/10)$, alors $\zeta_{10}^2 = \zeta_5$ et ζ_{10} est une racine carrée de ζ_5 et, en comparant par exemple les parties réelles, on obtient

$$\zeta_{15} = \frac{\zeta_5^2 + i\sqrt{3}\ \zeta_{10}}{2}.$$

Un calcul montre

$$\zeta_5^2 = \frac{-2(1+\sqrt{5}) + i(-1+\sqrt{5})\sqrt{2(5+\sqrt{5})}}{8},$$

et alors

$$\zeta_{15} = \frac{-2(1+\sqrt{5}) + i(-1+\sqrt{5})\sqrt{2(5+\sqrt{5})}}{16} + \frac{i\sqrt{3}\sqrt{-1+\sqrt{5}+i\sqrt{2(5+\sqrt{5})}}}{4}.$$

De cette écriture ne ressort pas immédiatement la partie réelle et la partie imaginaire de ζ_{15}. On peut éviter ce désagrément en passant par $\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$. C'est l'objet de la question 5).

5) Soit $F = \mathbb{Q}(y) = \mathbb{Q}(\zeta + \zeta^{-1})$. D'après le théorème 4.3.1, le groupe de Galois de $F/\mathbb{Q}(\sqrt{5})$ est engendré par $\overline{4}$. Ainsi

$$\begin{aligned} \mathrm{Irr}(y, \mathbb{Q}(\sqrt{5})) &= (X-y)(X-(\zeta^4+\zeta^{-4})) \\ &= X^2 - (\zeta+\zeta^{-1}+\zeta^4+\zeta^{-4})X + \zeta^5+\zeta^{-5}+\zeta^3+\zeta^{-3}. \end{aligned}$$

Nous devons exprimer ce polynôme dans $\mathbb{Q}(z)$, avec $z = \zeta^3 + \zeta^{-3}$. Or $(1, z)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(z)$, ainsi, il existe $a, b \in \mathbb{Q}$ tels que

$$\zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4} = \zeta + \zeta^{14} + \zeta^4 + \zeta^{11} = a + b(\zeta^3 + \zeta^{12}).$$

Modulo Φ_{15}, cette égalité devient

$$-\zeta^7 + \zeta^3 - \zeta^2 + 1 = a + b\zeta^3 - b\zeta^7 - b\zeta^2.$$

Comme $(1, \zeta, \cdots, \zeta^7)$ est $\mathbb{Q}$-libre, on en déduit $a = b = 1$ et ainsi $\zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4} = 1 + z$.

De même, on obtient $\zeta^5 + \zeta^{-5} + \zeta^3 + \zeta^{-3} = -1 + z$.

Ainsi $\mathrm{Irr}(y, \mathbb{Q}(z)) = X^2 - (1+z)X + (-1+z)$. Le discriminant δ de ce polynôme est égal à $\delta = z^2 - 2z + 5 = 3(2-z)$. (Se souvenir que

$z^2 + z - 1 = 0$.) Ainsi

$$y = \frac{1 + \sqrt{5} + \sqrt{3}\sqrt{10 - 2\sqrt{5}}}{4}.$$

En notant que $y/2$ est la partie réelle de ζ, on obtient

$$\zeta_{15} = \frac{1 + \sqrt{5} + \sqrt{3}\sqrt{10 - 2\sqrt{5}} + i\sqrt{28 + 4\sqrt{5} - 2\sqrt{3}(1 + \sqrt{5})\sqrt{10 - 2\sqrt{5}}}}{8}.$$

Exercice 50.
On peut noter que l'application trace $\mathrm{Tr}_{\mathrm{K/k}}$ est bien une application linéaire du k-espace vectoriel K vers k. Il suffit alors de montrer que $\mathrm{Tr}_{\mathrm{K/k}}$ n'est nulle. C'est alors immédiat. En effet, comme $\ker(\mathrm{Tr}_{\mathrm{K/k}}) = \ker(\mathrm{id} + \varphi_q + \cdots + \varphi_q^{t-1})$, d'après le lemme de Dedekind 6.4.2, la combinaison $\mathrm{id} + \varphi_q + \cdots + \varphi_q^{t-1}$ n'est pas triviale.

Exercice 51.
1) Le groupe de Galois Gal(K/k) est engendré par l'automorphisme de Frobenius $\varphi_q : x \mapsto x^q$.
2) $\mathrm{N}_{\mathrm{K/k}}(x) = x^{1+q+\cdots+q^{d-1}}$ et $\mathrm{Tr}_{\mathrm{K/k}}(x) = x + x^q + \cdots + x^{q^{d-1}}$.
3) $\mathrm{Tr}_{\mathrm{K/k}}(y^q - y) = \mathrm{Tr}_{\mathrm{K/k}}(\varphi_q(y)) - \mathrm{Tr}_{\mathrm{K/k}}(y) = \mathrm{Tr}_{\mathrm{K/k}}(y) - \mathrm{Tr}_{\mathrm{K/k}}(y) = 0$.
4) a) Cela provient du fait que φ_q est un homomorphisme de corps.
b) $\ker(\phi) = \{x \in \mathrm{K}, \varphi_q(x) = x\} = \mathbb{F}_q = \mathrm{k}$. Ainsi $|\mathrm{Im}(\phi)| = |\mathrm{K}|/|\mathrm{k}| = q^{d-1}$.
c) Voir l'exercice 50.
d) On sait que $\mathrm{Im}(\phi)$ est un sous-groupe de $\ker(\mathrm{Tr}_{\mathrm{K/k}})$ et que $|\ker(\mathrm{Tr}_{\mathrm{K/k}})| = |\mathrm{K}|/|\mathrm{k}|$. Au final, on obtient $\mathrm{Im}(\phi) = \ker(\mathrm{Tr}_{\mathrm{K/k}})$.

Exercice 52.
On rappelle que l'extension K/k est cyclique et $\mathrm{Gal}(\mathrm{K/k}) = \langle\varphi_q\rangle$, où φ_q est l'automorphisme de Frobenius.
On note tout d'abord que $\mathrm{N}_{\mathrm{K/k}}(0) = 0$. Ainsi, il faut donc vérifier que le morphisme de groupes

$$\begin{array}{rcl} \phi : \mathrm{K}^\times & \to & \mathrm{k}^\times \\ x & \mapsto & \mathrm{N}_{\mathrm{K/k}}(x) \end{array}$$

est surjectif. On a $\ker(\phi) = \{x \in \mathrm{K}^*,\ \mathrm{N}_{\mathrm{K/k}}(x) = 1\}$. Ainsi d'après le théorème 90 de Hilbert, $\ker(\phi) = \{y^{1-\varphi_q},\ y \in \mathrm{K}\}$. Soit alors

$$\begin{array}{rcl} \psi : \mathrm{K}^\times & \to & \mathrm{K}^\times \\ y & \mapsto & y^{1-\varphi_q} \end{array}$$

Clairement, ψ est un morphisme de groupes et $\ker(\psi) = \{y \in \mathrm{K}^*,\ y^{\varphi_q} = y\} = \mathrm{k}^*$.
Au final : $|\ker(\phi)| = |\mathrm{Im}(\psi)| = |\mathrm{K} - 1|/|\mathrm{k} - 1|$, puis $|\mathrm{Im}(\phi)| = |\mathrm{k} - 1|$.

Exercice 53.
1) Posons $\zeta = \zeta_n$. Les racines de P sont $\zeta^i\theta$, $i = 0, n-1$. Ainsi, $\mathrm{L} = \mathbb{Q}(\zeta, \theta) = \mathrm{k}(\theta)$.
2) Soit $\mathrm{K} = \mathbb{Q}(\theta)$. Comme $[\mathrm{K} : \mathbb{Q}] = n$ et $[\mathrm{k} : \mathbb{Q}] = \varphi(n)$ sont premiers entre eux, les extensions $\mathrm{k}/\mathbb{Q}$ et $\mathrm{K}/\mathbb{Q}$ sont linéairement disjointes et $\mathrm{L} = \mathrm{kK}$ est de degré $n\varphi(n)$ sur $\mathbb{Q}$.
3) Soit Q un facteur irréductible de P dans $\mathrm{k}[X]$. Soit β une racine de Q. Alors d'après la question 1), $\mathrm{L} = \mathrm{k}(\theta) = \mathrm{k}(\beta)$. Ainsi, $\deg(Q) = [\mathrm{L} : \mathrm{k}]$ et les facteurs irréductibles Q de P dans $\mathrm{k}[X]$ ont tous le même degré d.

D'après le corollaire 6.4.5, il existe un premier ℓ divisant n tel que $a = b^\ell$, $b \in \mathrm{k}$. Ecrivons $n = \ell n_1$. Alors

$$X^n - a = (X^{n_1})^\ell - b^\ell = (X^{n_1} - b)(X^{n_1} - \zeta^{n_1}b) \cdots (X^{n_1} - (\zeta^{n_1})^{\ell-1}b).$$

Soit Q un facteur irréductible de P dans $\mathrm{k}[X]$. Alors Q divise un des facteurs $X^{n_1} - (\zeta^{n_1})^i b$. Si ce facteur est irréductible, c'est terminé. Sinon, toujours par le corollaire 6.4.5, il existe ℓ' divisant n_1 tel que $b' = (\zeta^{n_1})^i b \in \mathrm{k}^{\ell'}$ et, en reprenant le raisonnement ci-dessus, Q divise un polynôme de la forme $X^{n_2} - b_2$, avec $n_1 = n_2\ell'$ et $b_2 \in \mathrm{k}$. Si $d = n_2$, c'est terminé. Sinon, on continue le processus, pour aboutir à $Q = X^d - c$, avec $c \in \mathrm{k}$.
4) • $P = X^p - p$ est irréductible (critère d'Eisenstein) et $(p, \varphi(p)) = 1$. Alors $[\mathrm{L} : \mathbb{Q}] = p(p-1)$.
• $P = X^8 - p$. On cherche à déterminer le degré de $\sqrt[8]{p}$ sur $\mathrm{k} = \mathbb{Q}(\zeta_8)$. D'après le corollaire 6.4.5, on cherche à savoir si $\sqrt{p} \in \mathrm{k}$. On rappelle que $\mathrm{k} = \mathbb{Q}(i, \sqrt{2})$. Ainsi pour $p \neq 2$, $\sqrt{p} \notin \mathrm{k}$ et ainsi, P est irréductible sur k. Ainsi $[\mathrm{L} : \mathbb{Q}] = 4 \cdot 8 = 32$.

Si $p = 2$, alors $P = X^8 - \sqrt{2}^2 = (X^4 - \sqrt{2})(X^4 + \sqrt{2})$. D'après la question 3), il faut et il suffit de tester l'irréductibilité de $X^4 - \sqrt{2}$ sur $\mathrm{k} = \mathbb{Q}(\sqrt{2}, i)$, ce qui, à l'aide du corollaire 6.4.5, revient à voir si $\sqrt[4]{2} \in \mathrm{k}$. Or $\sqrt[4]{2}$ est de degré 4 sur $\mathbb{Q}$, le corps $\mathbb{Q}(\sqrt[4]{2})$ est un sous-corps de $\mathbb{R}$, il n'est pas égal à $\mathrm{k} = \mathbb{Q}(i, \sqrt{2})$. Ainsi, $X^4 - \sqrt{2}$ est irréductible sur k et $[\mathrm{L} : \mathbb{Q}] = 16$.

• $P = X^8 + 100$. On a

$$P = X^8 + 100 = X^8 - (10i)^2 = (X^4 - 10i)(X^4 + 10i).$$

Il faut tester si $10i \in \mathrm{k}^2$.
Existe-t-il $a, b, c, d \in \mathbb{Q}$ tels que

$$(a + bi + c\sqrt{2} + di\sqrt{2})^2 = 10i \ ?$$

Utilisant le fait que $(1, \sqrt{2})$ est une $\mathbb{Q}(i)$-base de k, on en déduit

$$\begin{cases} (a + bi)^2 + 2(c + di)^2 = 10i \\ 2(a + bi)(c + di) = 0 \end{cases}$$

Si $a + bi = 0$, alors $c^2 + 2cdi - d^2 = 5i$ et on aboutit à une absurdité.
De même si $c + di = 0$.
Ainsi, $10i$ n'est pas un carré dans k et donc $(X^4 - 10i)$ est irréductible sur k et $[\mathrm{K} : \mathbb{Q}] = 16$.

• $P = X^6 + 3$. Ici $\mathrm{k} = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$. Ainsi

$$P = X^6 + 3 = X^6 - (\sqrt{-3})^2 = (X^3 - \sqrt{-3})(X^3 + \sqrt{-3}).$$

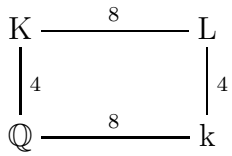
On cherche à voir si $\sqrt{-3}$ est un cube dans $\mathbb{Q}(j)$. Existe-t-il $a, b \in \mathbb{Q}$ tels que

$$\sqrt{-3} = (a + b\sqrt{-3})^3 \ ?$$

Une discussion facile montre que ce n'est pas possible.
Ainsi $[\mathrm{L} : \mathbb{Q}] = 6$.

Exercice 54.
1) On s'inspire de l'exercice précédent : $\mathrm{L} = \mathbb{Q}(\theta, \zeta)$. Ensuite, P un irréductible sur k si et seulement si 3 n'est pas un carré dans $\mathrm{k} = \mathbb{Q}(i, \sqrt{2})$, ce qui est le cas.
Ainsi P est irréductible sur k et $[\mathrm{L} : \mathbb{Q}] = 8 \cdot 4 = 32$.

2) Comme $[\mathrm{L} : \mathrm{k}] = [\mathrm{K} : \mathbb{Q}]$, les extensions $\mathrm{K}/\mathbb{Q}$ et $\mathrm{k}/\mathbb{Q}$ sont linéairement disjointes et ainsi $\mathrm{K} \cap \mathrm{k} = \mathbb{Q}$.



3) a) Supposons $\mathbb{Q}(\theta)/\mathbb{Q}$ galoisienne. Alors tous les $\mathbb{Q}$-conjugués de θ sont dans K, ce qui implique $\mathrm{K} = \mathrm{L}$. Absurdité.
b) L'élément θ^2 est racine de $X^4 - 3$ qui est irréductible sur $\mathbb{Q}$ (critère d'Eisenstein). Ainsi $[\mathbb{Q}(\theta^2) : \mathbb{Q}] = 2$. Comme $i \in \mathrm{k}$ et $\theta \in \mathrm{K}$, il vient

$$\mathbb{Q}(\theta^2) \cap \mathbb{Q}(i) \subset \mathrm{k} \cap \mathrm{K} = \mathbb{Q}.$$

Comme $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, cela suffit pour montrer que les extensions $\mathbb{Q}(\theta)/\mathbb{Q}$ et $\mathbb{Q}(i)/\mathbb{Q}$ sont linéairement disjointes et ainsi $[\mathbb{Q}(\theta^2, i) : \mathbb{Q}] = 8$. On note ensuite que les $\mathbb{Q}$-conjugués de θ^2 sont $\pm\theta^2$ et $\pm i\theta^2$. Ainsi, $\mathbb{Q}(\theta^2, i)$ est le corps des racines de $X^4 - 3$. L'extension $\mathbb{Q}(\theta^2, i)/\mathbb{Q}$ est normale (et séparable car $\mathbb{Q}$ est de caractéristique 0) : l'extension $\mathbb{Q}(\theta^2, i)/\mathbb{Q}$ est galoisienne.
Il vient $\mathrm{Gal}(\mathbb{Q}(i, \theta^2)/\mathbb{Q}) \simeq D_8$ (voir l'exercice 25).
c) De même, on a $[\mathbb{Q}(i, \theta) : \mathbb{Q}] = 16$. Comme pour a), l'extension $\mathbb{Q}(i, \theta)/\mathbb{Q}$ ne contient pas tous les conjugués de P et n'est donc pas normale.
4) Soit $\Delta = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Alors, on sait (théorème 4.3.1) que $\Delta \simeq \mathrm{Gal}(\mathrm{k}/\mathbb{Q})$. Le groupe de Galois Δ est donc isomorphe au groupe de Klein. D'autre part, comme k contient ζ et $\mathrm{L} = \mathrm{k}(\theta) = \mathbb{Q}(\sqrt[8]{3})$, l'extension L/k est galoisienne de groupe de Galois H cyclique d'ordre 8 (voir le théorème 6.4.1).
Ensuite, comme $\mathrm{k}/\mathbb{Q}$ est galoisienne, alors, par le théorème 4.2.4, H est distingué dans G. En particulier, Δ agit sur H par conjugaison.
Enfin, d'après le corollaire 4.2.2,

$$G = \mathrm{Gal}(\mathrm{L}/\mathbb{Q}) = \mathrm{Gal}(\mathrm{L}/\mathrm{K} \cap \mathrm{k}) = \langle \mathrm{Gal}(\mathrm{L}/\mathrm{k}), \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \rangle = \langle H, \Delta \rangle$$

et $\Delta \cap H = \{\mathrm{id}\}$.
Au final, on a bien $G = H \rtimes \Delta$. À noter que ce produit n'est pas direct (car Δ n'est pas distingué dans H).

Exercice 55.
1) Soit $P = X^p - x$. Les k_0-isomorphismes de K sont en correspondance avec les racines des polynomes $\sigma(P) = X^p - \sigma(x)$, $\sigma \in \Delta$. Ainsi, l'extension K/k_0 est galoisienne si et seulement les racines des polynômes $\sigma(P)$ sont dans K, ou encore si et seulement si $\sqrt{\sigma(x)} \in K$, pour tout élément $\sigma \in \Delta$. Comme P est irréductible sur k, les polynômes $\sigma(P)$ sont irréductibles sur k. Ainsi, on obtient : K/k_0 est galoisienne si et seulement si $k(\sqrt[p]{x}) = k(\sqrt[p]{\sigma(x)})$, pour tout $\sigma \in \Delta$. Par le théorie de Kummer (théorème 6.4.1), cette dernière condition équivaut à

$$\sigma(x)/x^{r_\sigma} \in k^p,$$

avec $(r_\sigma, p) = 1$.
2) a) Soit $\sigma : \sqrt{\ell} \mapsto -\sqrt{\ell}$ l'automorphisme engendrant $Gal(k/\mathbb{Q})$. D'après la question 1), $K/\mathbb{Q}$ est galoisienne si et seulement si $x/\sigma(x)^r \in k^2$, avec r impair, ce qui équivaut à $x\sigma(x) \in k^2$. Comme $x\sigma(x) = p^2 - \ell$, la condition équivaut à $p^2 - \ell = (a + b\sqrt{\ell})^2$, avec $a, b \in \mathbb{Q}$. Après identification, on obtient

$$\begin{cases} p^2 - \ell = a^2 + \ell b^2 \\ ab = 0 \end{cases}$$

Supposons $a = 0$. Alors $p^2 = \ell(1 + b^2)$. Ecrivons $b = r/s$, avec $r, s \in \mathbb{Z}$, $(r, s) = 1$. On voit rapidement que nécessairement $s = \pm 1$ et ainsi $b \in \mathbb{Z}$. L'égalité dans $\mathbb{Z}$: $p^2 = \ell(1 + b^2)$ indique alors que ℓ divise p, ce qui est absurde. Donc a est non nul et $b = 0$. On obtient alors $K/\mathbb{Q}$ est galoisienne si et seulement si $p^2 - \ell = a^2 = n^2$, avec $n \in \mathbb{N}$. Cette dernière condition s'écrit également $\ell = p^2 - n^2 = (p - n)(p + n)$. Ainsi, ou bien $p - n = \ell$ et $p + n = 1$, ou bien $p - n = 1$ et $p + n = \ell$. Dans les deux cas, cela implique $\ell = 2p - 1$. Réciproquement, si $\ell = 2p - 1$, alors $\ell = p^2 - (p-1)^2$ et $K/\mathbb{Q}$ est galoisienne.
Par exemple $p = 3$ et $\ell = 5$, ou encore $p = 7$ et $\ell = 13$, etc ...
b) Le groupe de Galois de $K/\mathbb{Q}$ est d'ordre 4. C'est soit le groupe de Klein, soit un groupe cyclique d'ordre 4.
Soient α une racine de $X^2 - x$ et θ une racine de $X^2 - (p - \sqrt{\ell}) = X^2 - \sigma(x)$. On rappelle que $x\sigma(x) = p^2 - \ell = n^2$, avec $n \in \mathbb{N}$. Ainsi $\sigma(x) = n^2/x$ et on peut choisir α et θ tels que $\theta = n/\alpha$.

Les éléments de Gal(K/$\mathbb{Q}$) sont donc

$$\tau_1 \left| \begin{array}{ccc} \sqrt{\ell} & \mapsto & \sqrt{\ell} \\ \alpha & \mapsto & \alpha \end{array} \right. \qquad \tau_2 \left| \begin{array}{ccc} \sqrt{\ell} & \mapsto & \sqrt{\ell} \\ \alpha & \mapsto & -\alpha \end{array} \right.$$

$$\tau_3 \left| \begin{array}{ccc} \sqrt{\ell} & \mapsto & -\sqrt{\ell} \\ \alpha & \mapsto & \theta = n/\alpha \end{array} \right. \qquad \tau_4 \left| \begin{array}{ccc} \sqrt{\ell} & \mapsto & -\sqrt{\ell} \\ \alpha & \mapsto & -n/\alpha \end{array} \right.$$

On vérifie que ces éléments sont d'ordre au plus 2. Ainsi Gal(K/$\mathbb{Q}$) est isomorphe au groupe de Klein.
Notons que α n'est fixe par aucun automorphisme non trivial de Gal(K/$\mathbb{Q}$), ainsi $\mathrm{K} = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{p+\sqrt{\ell}}\right) = \mathbb{Q}\left(\sqrt{p+\sqrt{2p-1}}\right)$.
Il nous reste à trouver les 3 sous-corps quadratiques de K/$\mathbb{Q}$. On en connaît déja un : $\mathbb{Q}(\sqrt{\ell})$.
Notons ensuite que

$$\begin{aligned} (\alpha + \frac{n}{\alpha})^2 &= \alpha^2 + 2n + \frac{n^2}{\alpha^2} \\ &= p + \sqrt{\ell} + 2n + \frac{p^2 - \ell}{p + \sqrt{\ell}} \\ &= p + \sqrt{\ell} + 2n + p - \sqrt{\ell} \\ &= 2(p+n) \end{aligned}$$

et

$$(\alpha + \frac{n}{\alpha})^2 = 2(p-n).$$

Comme $p + n = 1$ ou $p - n = 1$, on voit que $\sqrt{2} \in \mathrm{K}$. Ainsi, on a un second corps quadratique : $\mathbb{Q}(\sqrt{2})$. Le troisième étant $\mathbb{Q}(\sqrt{2\ell})$.
3) a) Il faut tester l'irréductiblité de P sur k. Le polynôme P est irréductible sur k si et seulement si $1+\sqrt{-3}$ n'est pas un cube dans k. Existe-t-il $a, b \in \mathbb{Q}$ tels que

$$(a + b\sqrt{-3})^3 = 1 + \sqrt{-3} \ ?$$

Si oui, on prend la norme dans k/$\mathbb{Q}$ de cette égalité pour obtenir dans $\mathbb{Q}$: $(a^2 + 3b^2)^3 = 4$. Comme 4 n'est pas un cube dans $\mathbb{Q}$, on aboutit à une contradiction.
Ainsi $[\mathrm{K} : \mathbb{Q}] = 3 \cdot 2 = 6$.
b) Soit $\sigma : \sqrt{-3} \mapsto -\sqrt{-3} \in$ Gal(K/$\mathbb{Q}$). Posons $x = 1 + \sqrt{-3}$. Alors d'après 1), K/$\mathbb{Q}$ est galoisienne si et seulement si ou bien $x\sigma(x) \in \mathrm{k}^3$ ou bien $x^2\sigma(x) \in \mathrm{k}^3$.

On a : $x\sigma(x) = 4$. Peut-on avoir $(a + b\sqrt{-3})^3 = 4$? Si oui, on prend la norme dans k/$\mathbb{Q}$ pour aboutir au fait que 16 est un cube dans $\mathbb{Q}$. Contradiction.

Il reste à tester la seconde condition. Peut-on avoir $(a + b\sqrt{-3})^3 = x^2\sigma(x) = 4(1 + \sqrt{-3})$? Si oui, on prend la norme dans k/$\mathbb{Q}$ pour aboutir à $(a^2 + 3b^2)^3 = 4^3$. Ainsi, $a^2 + 3b^2 = 4$. Contrairement à la situation précédente, on n'aboutit pas à une contradiction. Il faut pousser un peu plus loin les calculs.
On développe $(a + b\sqrt{-3})^3 = x\sigma(x) = 4(1 + \sqrt{-3})$ pour aboutir au système

$$\begin{cases} a^3 - 9ab^2 = 4 \\ 3a^2b - 3b^3 = 4 \\ a^2 + 3b^2 = 4 \end{cases}$$

On reporte $a^2 = 4 - 3b^2$ dans la seconde équation pour obtenir $3b^3 - 3b + 1 = 0$. Or les solutions rationnelles de $Q = 3X^3 - 3X + 1$ sont de la forme ± 1 ou $\pm 1/3$. On note que $Q(\pm 1) \neq 0$ et de même que $Q(\pm 1/3) \neq 0$. Ainsi, $x^2\sigma(x)$ n'est pas dans k^3.
L'extension K/$\mathbb{Q}$ n'est pas galoisienne.

Exercice 56.
1) On sait que $\Phi_n \in \mathbb{Z}[X]$ et que Φ_n divise $X^n - 1$. Le polynôme Φ_n étant unitaire, cette division a lieu dans $\mathbb{Z}[X]$: il existe $Q \in \mathbb{Z}[X]$ tel que $X^n - 1 = \Phi_n Q$. Par conséquent, on obtient dans $\mathbb{Z}$: $\Phi_n(0)Q(0) = -1$, ce qui implique $\Phi_n(0) = \pm 1$.
2) a) (i) Il vient $a^n - 1 = \Phi_n(a)Q(a) \equiv 0 (\text{mod } p)$, car p divise $\Phi_n(a)$.
(ii) Soit k l'ordre de a dans $\mathbb{F}_p^\times$. Alors d'après (i), k divise n : $n = \lambda k$. Supposons $\lambda > 1$. On rappelle (proposition 6.1.14) que pour tout entier m,

$$X^m - 1 = \prod_{i|m} \Phi_i.$$

Ainsi le nombre premier p divise un des $\Phi_i(a)$, avec $i|k$. Comme k divise n, i divise strictement n. On total, p divise $\Phi_i(a)$ et $\Phi_n(a)$, et $\Phi_i(a)\Phi_n(a)$

divise $a^n - 1$. On a bien $a^n \equiv 1 (\text{mod } p^2)$. De même, p divise $\Phi_i(a+p)$ et $\Phi_n(a+p)$. Ainsi, p^2 divise $(a+p)^n - 1$.
On montre que ces deux conditions ne sont pas compatibles. En effet, écrivons $a^n = 1 + bp^2$, $b \in \mathbb{Z}$. Alors

$$(a+p)^n \equiv a^n + nap (\text{mod } p^2) \equiv 1 + apn (\text{mod } p^2).$$

Or a (d'après (i)) et n sont premiers à p. Ainsi on obtient $(a+p)^n \not\equiv 1 (\text{mod } p^2)$, d'où une contradiction.
Par conséquent $k = n$.
b) La réciproque est immédiate. Soit $k|n$, $k < n$. Alors $a^k - 1 \not\equiv 0 (\text{mod } p)$. Or pour tout $d|n$,

$$a^d - 1 = \prod_{i|d} \Phi_i(a)$$

et p divise $a^n - 1$. On voit alors que nécessairement p ne divise que $\Phi_n(a)$.
3) Supposons que p divise $\Phi_n(a)$ pour un certain entier a. Alors a est d'ordre n dans $\mathbb{F}_p^\times$. Comme $\mathbb{F}_p^\times$ est un groupe cyclique d'ordre $p-1$, il vient $n|(p-1)$, ou encore $p \equiv 1 (\text{mod} n)$.
Réciproquement. Soit n divisant $p-1$. Si ε est un générateur de $\mathbb{F}_p^\times$, alors $\varepsilon^{(p-1)/n}$ est d'ordre n. Un relèvement quelconque de ε en a dans $\mathbb{Z}$, indique que a est d'ordre n dans $\mathbb{F}_p^\times$, et donc, d'après la question précédente, p divise $\Phi_n(a)$.
4) a) On sait que $\Phi_n(NM)$ divise $(NM)^n - 1$. Par conséquent, tout premier ℓ divisant NM ne peut pas diviser $\Phi_n(NM)$.
b) Le polynôme Φ_n est non constant. Alors $\phi_n(x)$ tend vers $+\infty$ quand x tend vers $+\infty$. Par conséquent, pour N assez grand, $\Phi_n(NM) > 1$. Il existe donc un premier p qui divise $\Phi_n(NM)$.
c) D'après la question 3), le nombre premier p qui divise $\Phi_n(NM)$, est congru à 1 modulo n. Or d'après 4), ce nombre $p \notin \{p_1, \cdots, p_r\}$. D'où une contradiction.

Exercice 57.
1) D'après l'exercice 56, il existe une infinité de nombres premiers p avec $p \equiv 1 (\text{mod } \ell^r)$. Soit un tel nombre premier p. L'extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est galoisienne de groupe de Galois Γ isomorphe à C_{p-1}. Comme ℓ^r divise $p-1$, le groupe Γ a un quotient isomorphe à C_{ℓ^r}, ce qui, via la correspondance

de Galois, assure l'existence d'une (en fait "la") sous-extension $\mathrm{K}/\mathbb{Q}$ de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ de groupe de Galois isomorphe à C_{ℓ^r}.
2) Toujours d'après l'exercice 56, soient p_1 et p_2 deux nombres premiers distincts avec $p_1 \equiv 1 (\mathrm{mod}\ \ell^r)$ et $p_2 \equiv 1 (\mathrm{mod}\ \ell^s)$. Notons par $\mathrm{K}_1/\mathbb{Q}$ la sous-extension de $\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}$ de groupe de Galois isomorphe à C_{ℓ^r} et par $\mathrm{K}_2/\mathbb{Q}$ la sous-extension de $\mathbb{Q}(\zeta_{p_2})/\mathbb{Q}$ de groupe de Galois isomorphe à C_{ℓ^s}. Ces extensions sont contenues dans $\mathbb{Q}(\zeta_{p_1p_2})/\mathbb{Q}$. Or $\mathrm{K}_1 \cap \mathrm{K}_2 \subset \mathbb{Q}(\zeta_{p_1}) \cap \mathbb{Q}(\zeta_{p_2}) = \mathbb{Q}$ par le théorème 6.3.12. Ainsi $\mathrm{K}_1\mathrm{K}_2/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $\mathrm{Gal}(\mathrm{K}_1/\mathbb{Q}) \times \mathrm{Gal}(\mathrm{K}_2/\mathbb{Q}) \simeq C_{\ell^r} \times C_{\ell^s}$.
3) Le cas général se déduit en itérant le point 2) et en utilisant la structure des groupes abéliens finis.

Exercice 58.
1) Soit $X + iY \in \mathbb{Q}(i)$, $X, Y \in \mathbb{Q}$, tel que $X^2 + Y^2 = N_{\mathbb{Q}(i)/\mathbb{Q}}(X + iY) = 1$. Alors, par le théorème 90 de Hilbert, il existe $u, v \in \mathbb{Q}$ tel que $X + iY = \dfrac{u + iv}{u - iv} = \dfrac{u^2 - v^2 + 2iuv}{u^2 + v^2}$. Ainsi $X = \dfrac{u^2 - v^2}{u^2 + v^2}$ et $Y = \dfrac{2uv}{u^2 + v^2}$. Il est immédiat que l'on peut se limiter à $u, v \in \mathbb{Z}$, $(u, v) = 1$.
2) L'égalité $x^2 + y^2 = z^2$ avec $z \neq 0$ s'écrit $\left(\dfrac{x}{z}\right)^2 + \left(\dfrac{y}{z}\right)^2 = 1$, c'est-à-dire $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\dfrac{x}{z} + i\dfrac{y}{z}) = 1$. Il suffit alors d'appliquer la question 1).
3) On suppose u, v premiers entre eux et de parités différentes. Alors $u^2 - v^2$ et $u^2 + v^2$ sont impairs. Supposons qu'il existe un premier ℓ divisant $u^2 - v^2$ et $u^2 + v^2$. Alors $\ell > 2$. Par soustraction, ℓ divise $2u^2$, donc ℓ divise u. Comme ℓ divise $u^2 - v^2$, ℓ divise v, ce qui est en contradiction avec l'hypothèse $(u, v) = 1$. Ainsi de l'égalité $\dfrac{x}{z} = \dfrac{u^2 - v^2}{u^2 + v^2}$, on obtient $x = u^2 - v^2$ et $z = u^2 + v^2$. Et ainsi $y = 2uv$.
4) On suppose u et v impairs, u et v premiers entre eux. Alors $u^2 - v^2$ est divisible par 8, $2uv \equiv 2 (\mathrm{mod}\ 4)$ et $u^2 + v^2 \equiv 2 (\mathrm{mod}\ 8)$. Ainsi $(u^2 - v^2, u^2 + v^2) = 2$ et $(u^2 - v^2, 2uv) = 2$. Posons $a = \dfrac{u + v}{2}, b = \dfrac{u - v}{2}$. Alors a et b sont des entiers premiers entre eux et $\dfrac{x}{z} = \dfrac{2ab}{a^2 + b^2}$. Ainsi $x = 2ab$, $z = a^2 + b^2$ et $y = a^2 - b^2$.

5) Grâce aux point 3) et 4), la résolution de l'équation $x^2 + y^2 = z^2$ est alors immédiate. Les solutions sont (à ordre près)

$$\begin{cases} x = 2\lambda uv & \lambda \in \mathbb{Z},\ u, v \in \mathbb{Z} \\ y = \lambda(u^2 - v^2) & (u, v) = 1 \\ z = \lambda(u^2 + v^2) & u, v \text{ de parités différentes} \end{cases}$$

Par exemple, pour $u = 23$, $v = 30$, $\lambda = 1$, on trouve $1380^2 + 371^2 = 2042041 = 1429^2$.

Pour finir, il convient de noter que l'équation de Fermat $x^n + y^n = z^n$, $n \geq 3$, $x, y, z \in \mathbb{Z}$ n'a pas de solution autre que les solutions triviales. Durant ces trente dernières années, cette équation fut l'objet de travaux très profonds de la part de nombreux mathématiciens. Le résultat a été prouvé dans les années 90 par Wiles et Taylor. Les méthodes utilisées font actuellement tomber d'autres conjectures....

CHAPITRE 7

CONSTRUCTIONS À LA RÈGLE ET AU COMPAS

Dans ce chapitre, on étudie les figures géométriques planes constructibles seulement avec une règle et un compas.

7.1. Définitions

Soit le plan usuel $\mathcal{P}$ et soient deux points A et B de $\mathcal{P}$. Nous souhaitons décrire les points de $\mathcal{P}$ obtenus à partir de A et B après une succession finie de constructions géométriques n'utilisant qu'une règle et un compas.

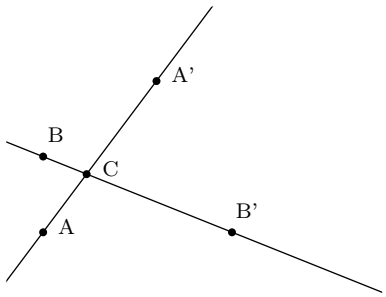
Définition 7.1.1. — Toute famille $\mathcal{A}$ de points de $\mathcal{P}$ obtenue à partir de A et B par une succession de constructions géométriques n'utilisant qu'une règle et un compas s'appelle une construction à la règle et au compas absolue (CRCA). Le segment $[A, B]$ définit le segment unité.

Remarque 7.1.2. — On peut élargir la notion en partant d'un ensemble fini de points $A_1, \cdots, A_n$ de $\mathcal{P}$ (au lieu seulement de deux points). Dans ce cas, on parle de construction à la régle et au compas relative (CRCR).

Définition 7.1.3. — Une figure $\mathcal{F}$ de $\mathcal{P}$ est un ensemble fini de points de $\mathcal{P}$. On dit que $\mathcal{F}$ est constructible à la règle et au compas de façon absolue (CRCA) si $\mathcal{F}$ est contenue dans une CRCA $\mathcal{A}$.

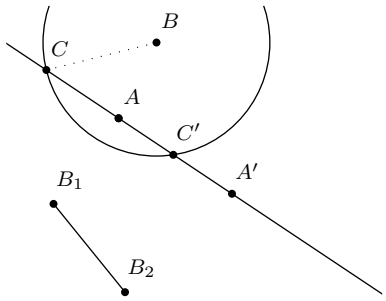
Il convient maintenant de préciser les opérations géométriques permises. Une CRCA est une suite de famille de points $\mathcal{A}_0 = \{A, B\} \subset \mathcal{A}_1 \subset \cdots \subset$

$\mathcal{A}_r$ pour laquelle on a $\mathcal{A}_{i+1} = \mathcal{A}_i \cup \{C\}$, où C est un point de $\mathcal{P}$ obtenu à partir de $\mathcal{A}_i$ de l'une des façons suivantes :
• le point C est obtenu comme intersection de deux droites passant par des points de $\mathcal{A}_i$:



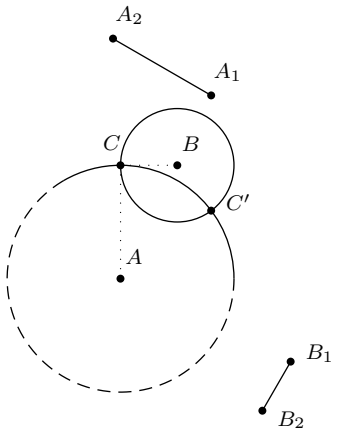
les points A, A', B et B' sont dans $\mathcal{A}_i$, ils permettent de construire C.

• le point C est obtenu comme intersection d'une droite passant par deux points de $\mathcal{A}_i$ et d'un cercle dont le centre est un point de $\mathcal{A}_i$ et dont le rayon correspond à la longueur d'un segment ayant pour extrémités deux points de $\mathcal{A}_i$:



les points A, A', B, B_1 et B_2 sont dans $\mathcal{A}_i$. Le cercle de centre B et de rayon B_1B_2 coupe la droite (AA'), ce qui permet de construire C et C'.

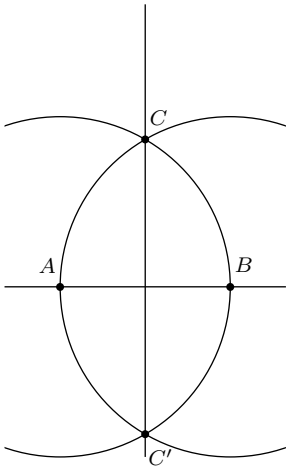
• le point C est obtenu comme intersection de deux cercles ayant chacun pour centre un point de $\mathcal{A}_i$ et pour rayon, la longueur d'un segment ayant pour extrémités deux points de $\mathcal{A}_i$:



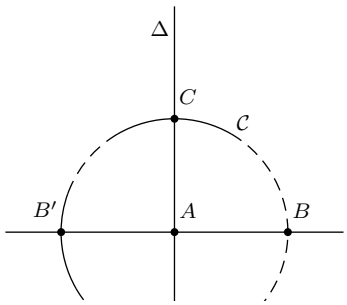
les points A, A_1, A_2, B, B_1 et B_2 sont dans $\mathcal{A}_i$.
L'intersection du cercle de centre A et de rayon A_1A_2 avec le cercle de centre B et de rayon B_1B_2 permet de construire les points C et C'.

7.2. Les constructions fondamentales

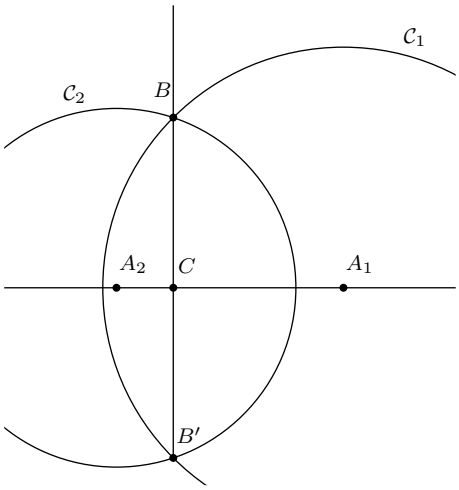
7.2.1. La médiatrice. — On se donne deux points A et B de $\mathcal{P}$. On trace les cercles de centre A et B et de même rayon AB. Ces cercles se coupent en C et C'. La droite (CC') est la médiatrice du segment $[A, B]$.



7.2.2. Le repére orthonormé. — On se donne deux points A et B. Le segment $[A, B]$ définit la longeur unité. On veut construire un repère orthonormé. L'intersection du cercle $\mathcal{C}$ de centre A et de rayon AB avec la droite (AB) donne B', le symétrique de B par rapport à A. En utilisant le point précédent, on construit la médiatrice Δ de $[B, B']$. L'intersection de $\mathcal{C}$ avec Δ donne le point C. Le repère $(A, \vec{AB}, \vec{AC})$ est orthonormé.

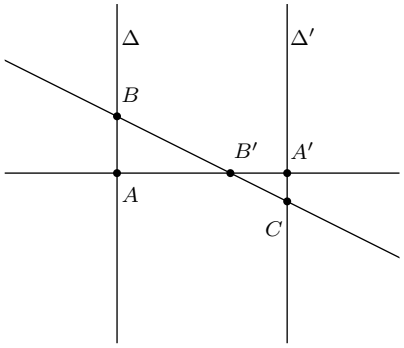


7.2.3. La projection orthogonale. — On se donne trois points A_1, A_2 et B de $\mathcal{P}$. On veut construire la projection orthogonale de B sur la droite (A_1A_2). Soit le cercle $\mathcal{C}_1$ de centre A_1 et de rayon A_1B et le cercle $\mathcal{C}_2$ de centre A_2 et de rayon A_2B. Alors $\mathcal{C}_1$ et $\mathcal{C}_2$ se coupent en B et B'. Les points A_1 et A_2 sont sur la médiatrice de $[B, B']$. Ainsi la droite (BB') est perpendiculaire à la droite (A_1A_2) et l'intersection C de ceux droites donne la solution au problème.



Cette méthode permet de donner la perpendiculaire à une droite donnée passant par un point donné.

7.2.4. L'inversion. — Soit le segment unité $[A, B]$ et soit un segment donné de longueur α. On souhaite construire un segment de longueur $1/\alpha$. On construit la perpendiculaire Δ passant par A à la droite (AB). Sur cette droite, en utilisant le compas, on place B' a une longueur α de A puis A' a une longeur $\alpha+1$ (de A). On construit ensuite la perpendiculaire Δ' à la droite Δ passant par A'. Soit alors C le point d'intersection des droites (BB') et Δ'. Par le théorème de Thalès dans $BCA'A$, il vient $A'C = A'C/AB = A'B/B'A = 1/\alpha$. Ainsi, le segment $[A', C]$ donne une solution au problème.

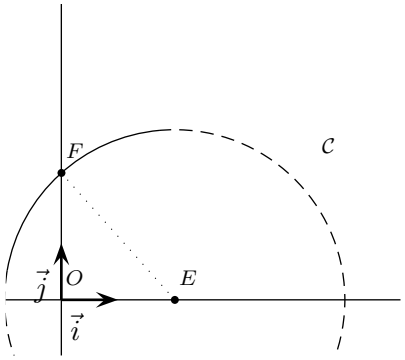


7.2.5. La multiplication. — On se donne deux segments de longueur α et β. On veut construire un segment de longueur $\alpha\beta$. Il suffit alors de reprendre le dessin précédent avec $AB' = 1/\alpha$ et $B'A' = \beta$. Le segment $[A', C]$ a pour longueur $\alpha\beta$.

7.2.6. La racine carrée. — On se donne un segment de longueur $\alpha > 0$. On veut construire un segment de longeur $\sqrt{\alpha}$. Grâce à l'inversion, on peut supposer $\alpha \geq 1$. Puis, grâce aux points précédents, on peut construire un segment de longeur $(\alpha - 1)/2$. Dans le repère orthonormé $(O, \vec{i}, \vec{j})$, on place le point E de coordonnées $((\alpha - 1)/2, 0)$. Soit alors $\mathcal{C}$ le cercle de centre E et de rayon $(\alpha + 1)/2$. L'intersection de $\mathcal{C}$ avec l'axe $(O\vec{j})$ donne le point F. Par le théorème de Pythagore, le segment $[E, F]$

a pour longueur

$$\sqrt{(\frac{\alpha+1}{2})^2-(\frac{\alpha-1}{2})^2}=\sqrt{\alpha}.$$



Définition 7.2.1. — Une longueur α est CRCA s'il existe une figure CRCA $\{A, B\}$ de $\mathcal{P}$ telle que $AB = \alpha$.

Définition 7.2.2. — Un angle θ est CRCA s'il existe une figure CRCA $\{A, B, C\}$ de $\mathcal{P}$ telle que $\widehat{ABC}$ soit égal à θ.

Exemple 7.2.3. — Le réel $\sqrt{2}$ et l'angle $\pi/2$ sont CRCA.

7.3. Extensions et CRCA

7.3.1. Nombres complexes constructibles à la règle et au compas. — On munit maintenant le plan $\mathcal{P}$ d'un repère orthonormé. Commençons par le résultat suivant qui se déduit immédiatement de la section précédente.

Proposition 7.3.1. — *Un point est CRCA si et seulement si ses points projections sur les axes du repère orthonormé le sont.*

On identifie maintenant le plan $\mathcal{P}$ avec le plan complexe.

Définition 7.3.2. — Un nombre complexe $z = x + iy$ $(x, y \in \mathbb{R})$ est CRCA, si et seulement les longeurs $|x|$ et $|y|$ sont CRCA.

Proposition 7.3.3. — *Soient z et z' deux nombres complexes CRCA. Alors $1/z$, $z + z'$ et zz' sont CRCA.*

Démonstration. — Soit $z = x+iy$. Alors $1/z = x/(x^2+y^2) - iy/(x^2+y^2)$. On applique successivement des poins de la section précédente : x^2+y^2 est CRCA (section 7.2.5), puis $1/(x^2+y^2)$ est CRCA (section 7.2.4) et enfin $x/(x^2+y^2)$ est CRCA (section 7.2.5). De même pour la partie imaginaire.
Pour $z+z'$: c'est évident.
Enfin, écrivons $z' = x'+iy'$, avec $x', y' \in \mathbb{R}$. Alors $zz' = xx' - yy' + i(xy' + x'y)$ est CRCA (section 7.2.5). □

Corollaire 7.3.4. — *Soient les complexes $z_1, \cdots, z_r$ CRCA. Alors tout élément du corps $\mathbb{Q}(z_1, \cdots, z_r)$ est CRCA.*

Démonstration. — On note tout d'abord que, grâce à l'inversion, tout rationnel m/n est CRCA. Ensuite, il suffit de noter qu'un élément α de $\mathbb{Q}(z_1, \cdots, z_r)$ s'écrit comme une fraction rationnelle sur $\mathbb{Q}$ en les z_i puis d'appliquer la proposition 7.3.3. □

Corollaire 7.3.5. — *Si tout élément du corps* K *est CRCA et que $z_1, \cdots, z_r$ sont des nombres complexes CRCA, alors tout élément de* $\mathrm{K}(z_1, \cdots, z_r)$ *est CRCA.*

Démonstration. — Identique à la preuve du corollaire 7.3.4. □

Remarque 7.3.6. — Si on se donne des complexes $z_1, \cdots, z_r$, tout élément du corps $\mathbb{Q}(z_1, \cdots, z_r)$ est CRCR.

7.3.2. Le résultat principal. —

Définition 7.3.7. — Soit $\mathcal{F} = \{A_1, \cdots, A_r\}$ une figure de $\mathcal{P}$. On note par $\mathbb{Q}(\mathcal{F})$ le corps engendré par les coordonnés des points A_i : si $A_i = (x_i, y_i)$, alors $\mathbb{Q}(\mathcal{F}) = \mathbb{Q}(x_1, \cdots, x_r, y_1, \cdots, y_r)$.

Avant de donner le résultat principal, définissons la notion d'extension 2-décomposable.

Définition 7.3.8. — Une extension finie K/k est 2-décomposable s'il existe une suite finie de corps $\mathrm{k} = \mathrm{K}_0 \subset \cdots \subset \mathrm{K}_d = \mathrm{K}$, où les extensions $\mathrm{K}_{i+1}/\mathrm{K}_i$ sont de degré 2.

Remarque 7.3.9. — Soient K/k et K′/k deux extensions 2-décomposables. Alors KK′/k est 2-décomposable.

Remarque 7.3.10. — Si K/k est une extension galoisienne de degré 2^t, alors K/k est 2-décomposable.

Théorème 7.3.11. — *Une figure $\mathcal{F}$ est CRCA si et seulement si $\mathbb{Q}(\mathcal{F})/\mathbb{Q}$ est contenue dans une extension* K/k *2-décomposable.*

Corollaire 7.3.12. — *Si $\mathcal{F}$ est CRCA, alors $[\mathbb{Q}(\mathcal{F}) : \mathbb{Q}]$ est une puissance de* 2.

Remarque 7.3.13. — Plus généralement, on a le résultat suivant. Soit la figure $\mathcal{F} = \{A_1, \cdots, A_r\}$. Alors $\mathcal{F}'$ est CRCR à partir de $\mathcal{F}$ si et seulement si l'extension $\mathbb{Q}(\mathcal{F}')/\mathbb{Q}(\mathcal{F})$ est contenue dans une extension 2-décomposable.

Remarque 7.3.14. — Le groupe de Galois de la clôture galoisienne d'une extension K/k 2-décomposable est un 2-groupe. Comme un 2-groupe est résoluble, on peut vérifier qu'une extension K/k est 2-décomposable si et seulement si elle est contenue dans une extension 2-décomposable L/k.

Démonstration. — (du théorème 7.3.11.)
Supposons $\mathcal{F}$ CRCA. Il existe donc une suite $\mathcal{A}_0 \subset \cdots \subset \mathcal{A}_d$ de figures CRCA avec $\mathcal{F} \subset \mathcal{A}_d$ et $\mathcal{A}_{i+1} = \mathcal{A}_i \cup \{C_i\}$, où le point C_i est obtenu par l'une des trois opérations de la section 7.1.
• Le point C_i est obtenu comme intersection de deux droites. Soient $A = (x, y), A' = (x', y'), B = (s, t), B' = (s', t') \in \mathcal{A}_i$ tels que $C_i = (\alpha, \beta)$ est l'intersection de (AA') avec (BB'). Alors

$$\alpha = \frac{\begin{vmatrix} s-x & s-s' \\ t-y & t-t' \end{vmatrix}}{\begin{vmatrix} x-x' & s-s' \\ y-y' & t-t' \end{vmatrix}}$$

et

$$\beta = \frac{\begin{vmatrix} x-x' & s-x \\ y-y' & t-y \end{vmatrix}}{\begin{vmatrix} x-x' & s-s' \\ y-y' & t-t' \end{vmatrix}}.$$

Ainsi $\alpha, \beta \in \mathbb{Q}(\mathcal{A}_i)$ et donc $[\mathbb{Q}(\mathcal{A}_{i+1}) : \mathbb{Q}(\mathcal{A}_i)] = 1$.

• Soient $A = (x, y)$, $A' = (x', y')$ et $B = (s, t) \in \mathcal{A}_i$. Le point $C_i = (\alpha, \beta)$ est obtenu comme l'intersection de la droite (AA') avec le cercle de centre B et de rayon r, où r est la longueur d'un segment $[B_1, B_2]$ se trouvant dans $\mathcal{A}_i$. On peut noter que $r^2 \in \mathbb{Q}(\mathcal{A}_i)$. On obtient alors le système

$$\begin{cases} \lambda(x-x', y-y') + (x, x') = (\alpha, \beta) \\ (\alpha - s)^2 + (\beta - t)^2 = r^2 \end{cases}$$

où l'on cherche à déterminer λ. On voit alors que λ vérifie

$$(\lambda(x-x') + x)^2 + (\lambda(y-y') + x')^2 = r^2.$$

C'est une identité de degré 2 en λ ((car $(x-x')^2 + (y-y')^2 \neq 0$) à coefficients dans $\mathbb{Q}(\mathcal{A}_i)$. Ainsi $[\mathbb{Q}(\mathcal{A}_i)(\lambda) : \mathbb{Q}(\mathcal{A}_i)] \leq 2$. Comme $\mathbb{Q}(\mathcal{A}_i)(\lambda) = \mathbb{Q}(\mathcal{A}_i)(C_i)$, on a bien au final $[\mathbb{Q}(\mathcal{A}_{i+1}) : \mathbb{Q}(\mathcal{A}_i)] \leq 2$.

• Soient $A = (x, y)$ et $B = (s, t)$ deux points distincts de $\mathcal{A}_i$ et soient r et v deux longueurs de segments de $\mathcal{A}_i$. (Alors r^2 et $v^2 \in \mathbb{Q}(\mathcal{A}_i)$.) Le point $C_i = (\alpha, \beta)$ est l'une des intersections du cercle de centre A et de rayon r avec le cercle de centre B et de rayon v. Il vient les équations

$$\begin{cases} (\alpha - x)^2 + (\beta - y)^2 = r^2 \\ (\alpha - s)^2 + (\beta - t)^2 = v^2 \end{cases}$$

On en tire $2\alpha(s-x) + 2\beta(t-y) = r^2 - v^2$. Comme A et B sont distincts, on peut supposer, par exemple, que $x \neq s$. Alors $\alpha \in \mathbb{Q}(\mathcal{A}_i, \beta)$ et β est racine d'un polynôme de degré 2 à coefficients dans $\mathbb{Q}(\mathcal{A}_i)$:

$$((x-s)^2 + (y-t)^2)\beta + m\beta + n = 0,$$

$m, n \in \mathbb{Q}(\alpha_i)$. Ainsi $[\mathbb{Q}(\mathcal{A}_i, \beta) : \mathbb{Q}(\mathcal{A}_i)] \leq 2$ puis $[\mathbb{Q}(\mathcal{A}_{i+1}) : \mathbb{Q}(\mathcal{A}_i)] \leq 2$.

Réciproquement. Raisonnons par récurrence. Supposons $\mathcal{A}_i$ CRCA et $[\mathbb{Q}(\mathcal{A}_{i+1}) : \mathbb{Q}(\mathcal{A}_i)] = 2$. Comme $-1 \in \mathbb{Q}(\mathcal{A}_i)$, par la théorie de Kummer,

il existe $x \in \mathbb{Q}(\mathcal{A}_i) \subset \mathbb{R}$ tel que $\mathbb{Q}(\mathcal{A}_{i+1}) = \mathbb{Q}(\mathcal{A}_i)(\sqrt{x})$. Comme tout élément de $\mathbb{Q}(\mathcal{A}_i)$ est CRCA, il en est de même pour x. Or d'après la section 7.2.6, $\sqrt{x}$ est CRC, par conséquent, $\sqrt{x}$ est CRCA. D'après le corollaire 7.3.5, tout élément de $\mathbb{Q}(\mathcal{A}_{i+1})$ est CRCA et ainsi les coordonnées des points de $\mathcal{A}_{i+1}$ sont CRCA. □

On peut garder l'identification de $\mathcal{P}$ à $\mathbb{C}$.

Proposition 7.3.15. — *Soit le nombre complexe $z = x + iy$, $x, y \in \mathbb{R}$. Alors $\mathbb{Q}(z)/\mathbb{Q}$ est contenue dans une extension 2-décomposable si et seulement si $\mathbb{Q}(x, y)/\mathbb{Q}$ est contenue dans une extension 2-décomposable.*

Démonstration. — Commençons par noter que le nombre complexe z est racine de $X^2 - 2xX + x^2 + y^2 \in \mathbb{Q}(x, y)[X]$. Ainsi $[\mathbb{Q}(x, y, z) : \mathbb{Q}(x, y)] \leq 2$. Supposons $\mathbb{Q}(x, y)/\mathbb{Q}$ contenue dans une extension $\mathrm{K}/\mathbb{Q}$ 2-décomposable. Alors $[\mathrm{K} \cap \mathbb{Q}(x, y, z) : \mathbb{Q}(x, y)] \leq 2$. Alors ou bien, $\mathbb{Q}(x, y, z) \subset \mathrm{K}$ et on a le résultat. Ou bien, $\mathrm{K} \cap \mathbb{Q}(x, y, z) = \mathbb{Q}(x, y)$ et alors $\mathrm{K}(z)$ est une extension quadratique de K (donc $\mathrm{K}(z)/\mathbb{Q}$ est 2-décomposable) qui contient $\mathbb{Q}(z)$. D'où le résultat.
Réciproquement. Supposons $\mathbb{Q}(z)$ contenue dans une extension $\mathrm{K}/\mathbb{Q}$ 2-décomposable.

Lemme 7.3.16. — *Soit $\mathrm{K}/\mathbb{Q}$ une extension 2-décomposable et soit $\sigma : \mathrm{K} \mapsto \mathbb{C}$ un isomorphisme du corps K. Alors $\sigma(\mathrm{K})$ est 2-décomposable.*

Démonstration. — C'est immédiat. Soit $\mathrm{K}_0 = \mathbb{Q} \subset \cdots \subset \mathrm{K}_r = \mathrm{K}$ une suite d'extensions quadratiques rendant $\mathrm{K}/\mathbb{Q}$ 2-décomposable. Alors, $\mathbb{Q} = \sigma(\mathbb{Q}) = \subset \cdots \sigma(\mathrm{K}_r) = \sigma(\mathrm{K})$ est aussi une suite d'extensions quadratiques : l'extension $\mathrm{K}/\mathbb{Q}$ 2-décomposable. □

Ainsi $\mathbb{Q}(\overline{z})$ est contenu également dans une extension $\mathrm{K}'/\mathbb{Q}$ 2-décomposable. Le compositum $\mathrm{KK}'/\mathbb{Q}$ est 2-décomposable et ainsi $\mathbb{Q}(z + \overline{z}) = \mathbb{Q}(x)$ est contenu dans une extension 2-décomposable $\mathrm{KK}'/\mathbb{Q}$. De même, $\mathbb{Q}(iy) \subset \mathbb{Q}(i, z - \overline{z})$ est contenu dans une extension 2-décomposable et comme $\mathbb{Q}(y) \subset \mathbb{Q}(i, iy)$, $\mathbb{Q}(y)$ est également contenue dans une extension 2-décomposable. □

Corollaire 7.3.17. — *Les nombres complexes $z_1, \cdots, z_r$ sont CRCA si et seulement si $\mathbb{Q}(z_1, \cdots, z_r)/\mathbb{Q}$ est contenue dans une extension 2-décomposable.*

Démonstration. — Tout d'abord, les nombres complexe $z_1, \cdots, z_r$ sont CRCA si et seulement si les coordonnés $x_i, y_i, i = 1, \cdots, r$ sont CRCA, c'est-à-dire si et seulement si $\mathbb{Q}(x_1, \cdots, x_r, y_1, \cdots, y_r)/\mathbb{Q}$ est contenue dans une extension 2-décomposable.

Supposons $\mathbb{Q}(x_1, \cdots, x_r, y_1, \cdots, y_r)/\mathbb{Q}$ contenue dans une extension 2-décomposable. Pour $1 \leq i \leq r$, l'extension $\mathbb{Q}(x_i, y_i)/\mathbb{Q}$ est une sous-extension de $\mathbb{Q}(x_1, \cdots, x_r, y_1, \cdots, y_r)/\mathbb{Q}$ et ainsi est contenue dans une extension 2-décomposable. D'après la proposition 7.3.15, $\mathbb{Q}(z_i)/\mathbb{Q}$ est contenue dans une extension 2-décomposable. Ainsi le compositum $\mathbb{Q}(z_1, \cdots, z_r)$ est aussi contenu dans une extension 2-décomposable.
Réciproquement.
C'est identique au sens précédent. Supposons $\mathbb{Q}(z_1, \cdots, z_r)/\mathbb{Q}$ contenue dans une extension 2-décomposable. Alors $\mathbb{Q}(z_{i+1})/\mathbb{Q}$ est une sous-extension de $\mathbb{Q}(z_1, \cdots, z_r)/\mathbb{Q}$ et ainsi est contenue dans une extension 2-décomposable. D'après la proposition 7.3.15, $\mathbb{Q}(x_i, y_i)$ est contenu dans une extension 2-décomposable, etc ... □

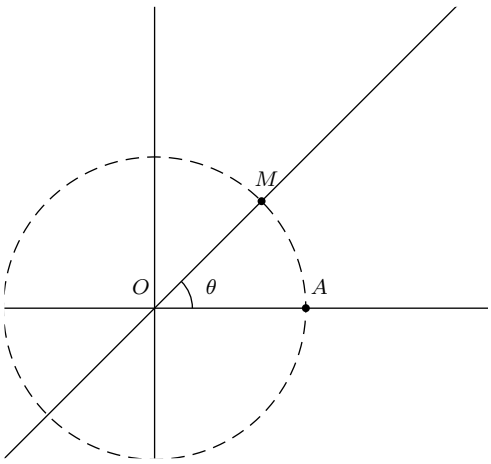
7.4. Exemples

7.4.1. La quadrature du cercle. — Étant donné le cercle unité, peut-on construire à la règle et au compas un carré de même aire ?
On cherche donc une solution CRCA a de l'équation $X^2 = \pi$. Soit a une telle solution. Comme π est transcendant, a l'est aussi, par conséquent, $\mathbb{Q}(a)/\mathbb{Q}$ ne peut pas être contenue dans une extension 2-décomposable. D'où l'impossibilité de la quadrature du cercle...

7.4.2. La duplication du cube. — C'est la construction (du patron) d'un cube de côté de longueur ℓ tel son volume soit le double de celui d'un cube donné de côté a. Cela revient, étant donné a, à constuire une longueur ℓ vérifiant $\ell^3 = 2a^3$. C'est une construction à la règle et au compas relative (CRCR). Le problème a une solution si et seulement si

$\mathbb{Q}(a,\ell)/\mathbb{Q}(a)$ est contenue dans une extension 2-décomposable. L'élément ℓ est racine de $X^3 - 2a^3$. Ainsi, ℓ est de degré 1, 2 ou 3 sur $\mathbb{Q}(a)$. On voit assez facilement que $\mathbb{Q}(a,\ell) = \mathbb{Q}(a, \sqrt[3]{2})$. La question est donc de déterminer le degré de $\sqrt[3]{2}$ sur le corps (réel) $\mathbb{Q}(a)$. Comme $\mathbb{Q}(a)$ est réel, le degré 2 est à exclure. Ainsi $[\mathbb{Q}(a, \sqrt[3]{2}) : \mathbb{Q}(a)] = 1$ ou 3. Le problème admet une solution si et seulement si $\sqrt[3]{2} \in \mathbb{Q}(a)$. Par exemple, pour $a \in \mathbb{Q}$, le problème n'a pas de solution.

7.4.3. La trisection de l'angle. — On se donne un angle θ, on cherche à construire à la règle et au compas l'angle $\theta/3$. Sur le cercle unité, on place le point M de coordonnées $(\cos\theta, \sin\theta)$. Soit A le point $(1, 0)$. On veut donc trisecter l'angle $\widehat{AOM}$.



Pour ce faire, il faut et il suffit de construire la longueur $\cos\theta/3$. À partir des formules trigonométriques, on a la relation $4\cos^3\theta/3 - 3\cos\theta/3 - \cos\theta = 0$. Ainsi, $\cos\theta/3$ est racine de $P = 4X^3 - 3X - a \in \mathbb{Q}(a)[X]$, où $a = \cos\theta$. La trisection de θ est alors possible si et seulement si $[\mathbb{Q}(a, \cos\theta/3) : \mathbb{Q}] \leq 2$, c'est-à-dire si et seulement si P est réductible sur $\mathbb{Q}(a)$. Par exemple,

(i) si $\theta = \pi/2$, alors $P = 4X^3 - X = X(4X^2 - 1)$ est réductible sur $\mathbb{Q}$, d'où une CRCA de $\pi/6$

(ii) si $\theta = \pi/3$, alors $P = 4X^3 - X - 1/2$ est irréductible sur $\mathbb{Q}$ (le polynôme P n'a pas de racine rationnelle) donc $\pi/9$ n'est pas CRCA.

(On rappelle qu'une CRCR de la bisection d'angle est possible, voir la section 7.2.1.)

7.4.4. Les polygones réguliers. — Soit P_n le polygone régulier à n cotés inscrit dans le cercle unité. Le polygone P_n est défini par n points A_k d'affixe $z_k = \exp(2ik\pi/n)$, $k = 1 \cdots, n$.
Il est immédiat de voir que le polygone P_n est CRCA si et seulement si $z = \zeta_n = \exp(2i\pi/n)$ est CRCA, c'est-à-dire, d'après le corollaire 7.3.17, si et seulement si, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est contenue dans une extension 2-décomposable. Comme $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est abélienne, la condition sur la 2-décomposabilité équivaut à $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^t$, où encore à $\varphi(n) = 2^t$.
Ecrivons $n = 2^u p_1^{u_1} \cdots p_s^{u_s}$, $u_i \geq 1$, et où les p_i sont premiers distincts impairs. Alors $\varphi(n) = 2^{u-1} \prod_{i=1}^{s} p_i^{u_i-1}(p_i - 1)$. Par conséquent, il est nécessaire et suffisant que l'on ait $u_i = 1$ et $p_i = 1 + 2^{k_i}$, $i = 1, \cdots, s$.
On peut préciser les nombres premiers p de la forme $1 + 2^u$.

Lemme 7.4.1. — *Soit $p > 2$ un nombre premier tel que $p - 1 = 2^t$. Alors t est une puissance de 2.*

Démonstration. — Ecrivons $p = 1 + 2^{rs}$ avec r impair et $s = 2^k$. Nous montrons que $r = 1$. Soit le polynôme $P = X^s + 1$. Alors $X^{rs} + 1 \equiv (-1)^r + 1 \equiv 0 (\text{mod } P)$. Ainsi P divise $X^{rs} + 1$ et donc $2^s + 1 = P(2)$ divise $2^{rs} + 1 = p$. Comme p est premier cela implique ou bien $2^s + 1 = 1$ (impossible) ou bien $2^s + 1 = 2^{rs} + 1$. Ce dernier point implique $r = 1$. □

Définition 7.4.2. — Les nombres $F_m = 1 + 2^{2^m}$ sont appelés nombres de Fermat.

Les nombres $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sont premiers, mais $F_5 = 641 \cdot 6700417$.

Exemple 7.4.3. — Le triangle équilatéral ($n = 3$), la carré ($n = 4$), le pentagone ($n = 5$), l'hexagone ($n = 6$), l'octogone ($n = 8$), P_{15} sont CRCA.

Lorsque c'est possible, la construction de P_n repose sur l'extraction puis la construction de racines carrées. Pour P_5 et P_{15} voir l'exercice 49.

7.5. Exercices

7.5.1. Enoncés. —

Exercice 59. — *Donner les angles $\theta = 2\pi/n$ admettant une trisection CRCA.*

Exercice 60. — *Donner les angles θ CRCA ayant une valeur entière en degré.*

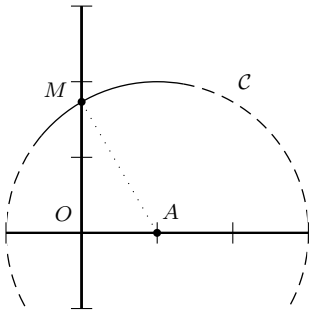
Exercice 61. — *Donner une CRCA de $\sqrt[4]{3}$.*

7.5.2. Corrigés. —

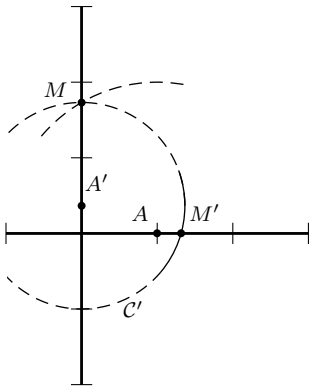
Exercice 59. Soit $\beta = \theta/3 = 2\pi/3n$ et soit $z = \zeta_{3n} = \cos\beta + i\sin\beta$. Alors β est CRCA si et seulement si z est CRCA, c'est-à-dire si et seulement si $\mathbb{Q}(z)/\mathbb{Q}$ est contenue dans une extension 2-décomposable. Comme $\mathbb{Q}(z)/\mathbb{Q}$ est une extension galoisienne de groupe de Galois un groupe abélien, cela équivaut à $[\mathbb{Q}(z) : \mathbb{Q}] = 2^t$. Ainsi z est CRCA si et seulement si $\varphi(3n) = 2^t$. Ecrivons $n = 2^u p_1^{u_1} \cdots p_s^{u_s}$, $u_i \geq 1$ et $p_i > 2$ étant des premiers deux à deux distincts. Alors, z est CRCA si et seulement si $n = 2^u p_1 \cdots p_s$, $p_i > 3$, et les nombres premiers p_i sont des nombres de Fermat. Par exemple, la trisection de $2\pi/3$ n'est pas CRCA.

Exercice 60
Soit θ et soit $r \in \{1, 2, \cdots, 360\}$ sa valeur en degré. Alors $2\pi r/360$ est la valeur de θ en radian. Ainsi θ est CRCA si et seulement si $z = \exp(2ir\pi/360)$ est CRCA. L'élément $z \in \mu_{360}$; soit n son ordre. L'entier n divise $360 = 2^3 3^2 5$; $n = 2^a 3^b 5^c$, avec $a \leq 3$, $b \leq 2$ et $c \leq 1$. Alors z est CRCA si et seulement si $\varphi(n)$ est une puissance de 2, c'est-à-dire si et seulement si $b \leq 1$. Par conséquent l'angle θ est CRCA si et seulement si 3 divise r.

Exercice 61
Soit le point A de coordonnées $(1, 0)$ et soit $\mathcal{C}$ le cercle de centre A et de rayon 2. Notons par M l'un des points d'intersection de $\mathcal{C}$ avec l'axe des ordonnées. Alors, la distance OM vaut exactement $\sqrt{3}$.



Ensuite, soit le point A' de coordonnées $(0, \dfrac{\sqrt{2}-1}{2})$ et soit $R = \dfrac{\sqrt{2}+1}{2}$. On trace le cercle $\mathcal{C}'$ de centre A' et de rayon R. Son intersection avec l'axe des abscisses donne le point M' et $OM' = \sqrt[4]{2}$.



CHAPITRE 8

DEVOIRS MAISON ET ANNALES

Devoir numéro 1

Exercice 1.
Soit $P = X^3 - X + 1 \in \mathbb{Q}[X]$ et soit α une racine de P dans $\mathbb{C}$.
1) Déterminer $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
2) Soit $\beta = \dfrac{1}{2\alpha^2 - 3\alpha + 2}$.
   a) Déterminer $x, y, z \in \mathbb{Q}$ tels que $\beta = x + y\alpha + z\alpha^2$.
   b) Déterminer $\mathrm{Irr}(\beta, \mathbb{Q})$.

Exercice 2.
Les corps sont vus comme sous-corps de $\mathbb{C}$.
Soit $\mathrm{k} = \mathbb{Q}(i)$ puis $\mathrm{K} = \mathrm{k}(\theta)$, où $\theta^2 + i = 0$.
1) Déterminer $[\mathrm{K} : \mathbb{Q}]$.
2) En utilisant le théorème du prolongement des $\mathbb{Q}$-isomorphismes, déterminer tous les $\mathbb{Q}$-plongements de K dans $\mathbb{C}$.
3) Montrer que $\mathrm{K}/\mathbb{Q}$ est une extension galoisienne.
4) Déterminer $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$, c'est-à-dire la structure du groupe des $\mathbb{Q}$-automorphismes de K.
5) Montrer que $\mathrm{K} = \mathbb{Q}(\theta)$ et déterminer $\mathrm{Irr}(\theta, \mathbb{Q})$.

Exercice 3.
Soit k un corps de caractéristique différente de 2 et de 3. Notons par $\overline{\mathrm{k}}$ une clôture algébrique de k.

Partie I
Soit P un polynôme unitaire de degré 3 à cofficients dans k. Montrer que P peut se mettre sous la forme

$$P(X) = (X + t)^3 + p(X + t) + q,$$

avec $p, q, t \in \mathrm{k}$.

Partie II

2) Soit $P = X^3 + pX + q \in \mathrm{k}[X]$ irréductible sur k.

a) Soit θ une racine de P dans $\overline{\mathrm{k}}$. Montrer que θ n'est pas racine double de P.

Soient $\theta_1, \theta_2, \theta_3$ les racines de P dans $\overline{\mathrm{k}}$. On pose

$$\delta = (\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta_1),$$

puis $\Delta = \delta^2$.

b) Exprimer Δ en fonction de p et q.

c) Montrer que $\mathrm{k}(\theta_1, \theta_2, \theta_3) = \mathrm{k}(\theta_1, \theta_2) = \mathrm{k}(\theta_1, \delta)$.

d) Soit K le corps des racines de P. Calculer [K : k] en distinguant deux cas : $\delta \in \mathrm{k}$; $\delta \notin \mathrm{k}$.

3) Montrer que $\mathrm{k}(\theta)/\mathrm{k}$ est galoisienne si et seulement si $\delta \in \mathrm{k}$.

4) Suivant que δ appartient à k ou non, déterminer le groupe $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$. (*Indication. On pourra utiliser le fait que* $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) \hookrightarrow S_3$*).*

5) Déterminer $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ pour $P = X^3 - 3X - 1$ puis pour $P = X^3 + X + 1$.

Devoir numéro 2

Exercice 1.
Soit p un nombre premier *impair*, $n \geq 1$ un entier et $q = p^n$.

1) Déterminer le nombre de carrés du corps fini $\mathbb{F}_q$.

2) Soit $P_{a,b}(X) = X^2 + aX + b$ un polynôme unitaire du second degré à coefficients dans $\mathbb{F}_q$. Calculer le nombre de couples (a, b) tels que

a) $P_{a,b}(X)$ ait une racine double dans $\mathbb{F}_q$.

b) $P_{a,b}(X)$ ait deux racines distinctes dans $\mathbb{F}_q$.

c) $P_{a,b}(X)$ soit irréductible dans $\mathbb{F}_q$.

3) a) Montrer que le polynôme $X^2 + 1$ est irréductible dans $\mathbb{F}_3[X]$.
On note i une racine de ce polynôme dans une clôture algébrique fixée $\overline{\mathbb{F}_3}$ de $\mathbb{F}_3$, et on prend $\mathbb{F}_9 = \mathbb{F}_3(i)$.

b) Montrer que les seuls carrés de $\mathbb{F}_9$ sont 0, ± 1 et $\pm i$.

4) a) Montrer que le polynôme $X^2 + X + i$ est irréductible dans $\mathbb{F}_9[X]$.

b) Soit α une racine du polynôme $X^2 + X + i = 0$ dans $\overline{\mathbb{F}_3}$. Déterminer $\mathrm{Irr}(\alpha, \mathbb{F}_3)$.

Exercice 2.
Soit k un corps de caractéristique différente de 3, $\mathrm{K} = \mathrm{k}(X)$ et $\overline{\mathrm{K}}$ une clôture algébrique de K.
Considérons $P(Y) = Y^3 - X + 1 \in \mathrm{K}[Y]$.
1) Soit k^{alg} la réunion des extensions algébriques de k contenues dans $\overline{\mathrm{K}}$. Montrer que k^{alg} est une clôture algébrique de k.
2) Montrer que P est irréductible sur K.
3) Montrer que P est séparable (dans $\overline{\mathrm{K}}$).
4) Notons par L le corps des racines de P dans $\overline{\mathrm{K}}$.

a) Déterminer les racines de P.

b) Déterminer $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ pour $\mathrm{k} = \mathbb{F}_5$ puis pour $\mathrm{k} = \mathbb{F}_7$.

c) Pour ces deux cas, préciser toutes les sous-extensions de L/K.

Exercice 3. Soit $n \geq 2$ et soit $P = X^n + aX^{n-1} + b \in \mathbb{Z}[X]$.
1) Montrer que $\mathrm{disc}(P) = (-1)^{n(n+1)/2} n^n b^{n-2} \Big(b + (-1)^{n+1} \dfrac{a^n (n-1)^{n-1}}{n^n} \Big)$.

2) Soit $P = X^5 + 5X^4 + 64$ et soit $\mathbb{Q}_P$ le corps des racines de P sur $\mathbb{Q}$. Déterminer $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$. *(Indic. Factoriser P modulo 3 et modulo 7.)*

Problème.

Soient k un corps et $\mathrm{K} = \mathrm{k}(X)$ le corps des fractions rationnelle sur k.

1) Soient P et Q deux polynomes de $\mathrm{k}[X]$ premiers entre eux (non tous les deux constants) et soit $Y = \dfrac{P}{Q} \in \mathrm{K}$.

Montrer que K est une extension algébrique de $\mathrm{k}(Y)$ de degré $\max(\deg(P), \deg(Q))$.

2) Soit $\mathrm{Gl}_2(\mathrm{k}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathrm{k}), ad - bc \neq 0\}$ le groupe des matrices inversibles 2×2 à coefficients dans k.

Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(\mathrm{k})$, on définit $A \cdot X \in \mathrm{k}(X)$ par

$$A \cdot X = \frac{aX + b}{cX + d}$$

a) Montrer que, via cette opération, $\mathrm{Gl}_2(\mathrm{k})$ opère sur $\mathrm{k}(X)$.

b) Montrer que le stabilisateur de X est exactement le centre $\mathrm{H}_2(\mathrm{k})$ de $\mathrm{Gl}_2(\mathrm{k})$. (On rappelle que $\mathrm{H}_2(\mathrm{k}) \simeq \mathrm{k}^*$.)

c) En utilisant 1), montrer que le groupe $G = \mathrm{Aut}(\mathrm{K}/\mathrm{k})$ des k-automorphismes de K est isomorphe au quotient $\mathrm{PGl}_2(\mathrm{k})$ de $\mathrm{Gl}_2(\mathrm{k})$ par son centre $\mathrm{H}_2(\mathrm{k}) \simeq \mathrm{k}^\times$.

3) On prend $\mathrm{k} = \mathbb{F}_p$.

a) Montrer que $|G| = p(p^2 - 1)$.

b) Soit H_1 le sous-groupe de G engendré par $X \mapsto X + b$, $b \neq 0$, et soit $Z = X^p - X$.

(i) Déterminer $|H_1|$.

(ii) Déterminer $[\mathrm{k}(X) : \mathrm{k}(Z)]$.

(iii) Montrer que $Z = X^p - X \in \mathrm{K}^{H_1}$.

(iv) En déduire : $\mathrm{K}^{H_1} = \mathrm{k}(Z)$.

c) Soit H_2 le sous-groupe de G engendré par $X \mapsto aX + b$, $ab \neq 0$. Montrer que $\mathrm{K}^{H_2} = \mathrm{k}(T)$, où $T = (X^p - X)^{p-1}$.

Devoir numéro 3

Tous les éléments de ce devoir sont vus dans $\mathbb{C}$.

Exercice 1.
Soit ℓ un nombre premier.
Soient $\mathrm{k} = \mathbb{Q}(\sqrt{\ell})$, $\theta = \sqrt{\ell + \sqrt{\ell}}$ et $\mathrm{K} = \mathbb{Q}(\theta)$.

1) a) Déterminer $P = \mathrm{Irr}(\theta, \mathbb{Q})$ et en déduire $[\mathrm{K} : \mathbb{Q}]$.
b) Montrer que $\mathrm{k} \subset \mathrm{K}$ et déterminer $\mathrm{Irr}(\theta, \mathrm{k})$.
c) Soit $\beta = \sqrt{\ell - \sqrt{\ell}}$. Déterminer tous les $\mathbb{Q}$-isomorphismes de K dans $\mathbb{C}$.
d) Calculer $\theta\beta$.

2) Montrer que $\mathrm{K}/\mathbb{Q}$ est galoisienne si et seulement si $\ell - 1 = n^2$, avec $n \in \mathbb{N}$.

3) On suppose que $\ell - 1 = n^2,\ n \in \mathbb{N}$. Déterminer $G = \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ puis tous les sous-corps de $\mathrm{K}/\mathbb{Q}$.

4) On suppose que $\ell - 1 \notin \mathbb{N}^2$. Soit L le corps des racines de P sur $\mathbb{Q}$.
a) Déterminer $[\mathrm{L} : \mathbb{Q}]$.
b) Trouver $d \in \mathbb{Z}$ tel que L soit le composé des deux extensions linéairement disjointes suivantes : $\mathbb{Q}(\theta)/\mathbb{Q}$ et $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$.

Exercice 2.
Soit un nombre premier ℓ. Soit $\mathrm{k} = \mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$, où $j = \exp(2i\pi/3)$. Soit $P = X^6 - \ell \in \mathbb{Q}[X]$ et soit θ une racine de P dans $\mathbb{C}$. Posons $\mathrm{K} = \mathbb{Q}(\theta)$ et $\mathrm{L} = \mathrm{k}(\theta) = \mathrm{Kk}$.

1) Déterminer $[\mathrm{K} : \mathbb{Q}]$.
2) Déterminer $[\mathrm{L} : \mathrm{k}]$.
3) En déduire que les extensions $\mathrm{k}/\mathbb{Q}$ et $\mathrm{K}/\mathbb{Q}$ sont linéairement disjointes.
4) Montrer que l'extension $\mathrm{L}/\mathbb{Q}$ est galoisienne.

5) Montrer que $\mathrm{Gal}(\mathrm{L}/\mathbb{Q}) = \mathrm{Gal}(\mathrm{L}/\mathrm{k}) \rtimes \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \simeq D_{12}$, où D_{12} est le groupe diédral d'ordre 12.
6) Déterminer toutes les sous-extensions galoisiennes $\mathrm{F}/\mathbb{Q}$ de $\mathrm{L}/\mathbb{Q}$.

Exercice 3.
On considère le corps cyclotomique $\mathrm{K} = \mathbb{Q}(\mu_{189})$.

1) Déterminer $[\mathrm{K} : \mathbb{Q}]$.
2) Déterminer la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.
3) Déterminer les sous-corps cyclotomiques inclus dans K et tracer leur treillis.
4) Déterminer Φ_{189}.

Master de mathématiques
2009-2010
Université de Franche-Comté
CTU
Epreuve préliminaire
Durée 1h15

Exercice 1
Soit $\mathbb{F}_2$ le corps à deux éléments et soit $\overline{\mathbb{F}_2}$ une clôture algébrique de $\mathbb{F}_2$.

1) Déterminer les polynômes irréductibles et unitaires de degré 2 sur $\mathbb{F}_2$.

2) Déterminer les polynômes irréductibles et unitaires de degré 4 sur $\mathbb{F}_2$.

3) Pour $x \in \overline{\mathbb{F}_2}$, soit $n(x)$ l'unique entier défini par $\mathbb{F}_{2^{n(x)}} = \mathbb{F}_2(x)$.
Soit $\theta \in \overline{\mathbb{F}_2}$ une racine de $X^4 + X + 1 \in \mathbb{F}_2[X]$. Déterminer $n(x)$ quand :
(i) $x = \theta$;
(ii) $x = \theta^2 + 1$;
(iii) $x = \theta^2 + \theta$.
(iv) x est une racine de $P = X^2 + X + \theta^3$.

Exercice 2.
Soit ζ une racine primitive 225-ème de l'unité.

1) Déterminer $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

2) Déterminer le treillis des sous-corps cyclotomiques de $\mathbb{Q}(\zeta)/\mathbb{Q}$ (ne pas oublier de préciser le degré des extensions relatives).

Exercice 3.
Soient ℓ_1 et ℓ_2 deux nombres premiers distincts.
Posons $\mathrm{k}_1 = \mathbb{Q}(\sqrt{\ell_1})$ et $\mathrm{k}_2 = \mathbb{Q}(\sqrt{\ell_2})$.

1) Déterminer $[\mathrm{k}_1 : \mathbb{Q}]$.

2) Montrer que $\sqrt{\ell_2} \notin \mathrm{k}_1$. En déduire $[\mathrm{k}_1\mathrm{k}_2 : \mathbb{Q}]$.

3) Montrer que l'extension $k_1k_2/\mathbb{Q}$ est galoisienne.

4) Déterminer $\mathrm{Gal}(k_1k_2/\mathbb{Q})$.

5) En déduire tous les sous-corps de $\mathbb{Q}(\sqrt{\ell_1}, \sqrt{\ell_2})/\mathbb{Q}$.

Master de mathématiques
2009-2010
Université de Franche-Comté
CTU
Epreuve principale
Durée 2h

Exercice 1
Soit p un nombre premier et soit le corps fini $\mathbb{F}_p$ à p éléments. Fixons une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$.

Partie A
Soit $P = X^p - X + 1 \in \mathbb{F}_p[X]$ et soit α une racine de P dans $\overline{\mathbb{F}_p}$.

1) Montrer que $\alpha \notin \mathbb{F}_p$.

2) Montrer que les racines de P sont de la forme $\alpha + a$, avec $a \in \mathbb{F}_p$.

3) En déduire que $\mathbb{F}_p(\alpha)$ est le corps des racines de P dans $\overline{\mathbb{F}_p}$.

4) On cherche à déterminer $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$.

a) Soit $Q \in \mathbb{F}_p[X]$ un facteur unitaire de P de degré au moins 1. Montrer qu'il existe $a_1, \cdots, a_r$ des éléments de $\mathbb{F}_p$ tels que

$$Q = \prod_{i=1}^{r} (X - \alpha - a_i).$$

b) En regardant les termes de degré $r-1$, montrer que $r\alpha \in \mathbb{F}_p$.

c) En déduire que le polynôme Q est de degré p puis que $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^p}$.

Partie B
Soit le corps $\mathrm{k} = \mathbb{F}_p(X)$. Fixons une clôture algébrique $\overline{\mathrm{k}}$ de k.

5) Montrer que $\mathbb{F}_p$ est aussi l'ensemble des racines de $Y^p - Y$ dans $\overline{\mathrm{k}}$.

Soit le polynôme $P = Y^p - Y - f \in \mathrm{k}[Y]$, où $f \in \mathbb{F}_p[X] - \{0\}$ (ou encore f est un polynôme non nul !).
Soit θ une racine de P dans $\overline{\mathrm{k}}$.

6) Montrer que $\theta \in \mathrm{k}$ si et seulement si, il existe une fraction rationnelle $g \in \mathbb{F}_p(X)$ telle $f = g^p - g$.
En déduire que $\theta \in \mathrm{k}$ si et seulement si, $f = g^p - g$, avec $g \in \mathbb{F}_p[X]$.
Indication.
Ecrire $g = \dfrac{g_1}{g_2}$, $g_i \in \mathbb{F}_p[X]$, $(g_1, g_2) = 1$, *et montrer que* $g_2 \in \mathbb{F}_p^*$.
En déduire que $\alpha \notin \mathrm{k}$ dès que $\deg(f) \not\equiv 0 (\mathrm{mod}\ p)$.

6) Montrer que les racines de P sont de la forme $\alpha + a$, avec $a \in \mathbb{F}_p$.

7) En s'inspirant de la partie A, montrer que si $\alpha \notin \mathrm{k}$ alors $[\mathrm{k}(\theta) : \mathrm{k}] = p$.

8) On suppose que $\alpha \notin \mathrm{k}$.

a) Montrer que $\mathrm{k}(\alpha)/\mathrm{k}$ est une extension galoisienne de groupe de Galois cyclique d'ordre p engendré par $\sigma : \alpha \mapsto \alpha + 1$.
Soit $f_1 \in \mathbb{F}_p[X] - \{0\}$ et soit α_1 une racine de $P_1(Y) = Y^p - Y - f_1$ dans $\overline{\mathrm{k}}$.

b) On suppose que $\mathrm{k}(\alpha) = \mathrm{k}(\alpha_1)$. Montrer qu'il existe $a \in \mathbb{F}_p^*$ tel que $\sigma(\alpha_1) = \alpha_1 + a$ puis que $\alpha_1 - a\alpha \in \mathrm{k}$.

c) En déduire que $\mathrm{k}(\alpha) = \mathrm{k}(\alpha_1)$ si et seulement si, il existe $a \in \mathbb{F}_p^*$, $h \in \mathbb{F}_p[X]$, tels que $f_1 = af + h^p - h$.

d) Posons $f = X$ et $f_1 = (X + 1)$.

(i) Vérifier que α et α_1 ne sont pas dans k.

(ii) Déterminer $\mathrm{k}(\alpha) \cap \mathrm{k}(\alpha_1)$.

(iii) En déduire que $\mathrm{k}(\alpha, \alpha_1)/\mathrm{k}$ est galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 2.
L'ensemble des éléments de cet exercice sont vus dans $\mathbb{C}$.

Soit $p > 2$ un nombre premier et soit ζ une racine primitive p-ème de l'unité. Posons $\mathrm{k} = \mathbb{Q}(\zeta)$.

On rappelle que $\mathrm{k}/\mathbb{Q}$ est une extension galoisienne cyclique d'ordre $p-1$ de groupe de Galois Δ engendré par $s : \zeta \mapsto \zeta^a$, où a est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Soit le polynôme $P = X^p - p \in \mathbb{Q}[X]$ et soit $\theta = \sqrt[p]{p}$ la racine réelle de P. Posons $\mathrm{K} = \mathrm{k}(\theta) = \mathbb{Q}(\zeta, \sqrt[p]{p})$.

1) Quel est le degré de $\mathbb{Q}(\theta)/\mathbb{Q}$? En déduire que P est irréductible sur k.

2) Montrer que K/k est une extension galoisienne cyclique de degré p, de groupe de Galois engendré par $t : \theta \mapsto \zeta\theta$.

3) Montrer que l'extension $\mathrm{K}/\mathbb{Q}$ est galoisienne. Quel est l'ordre de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$?

4) Soient les éléments σ et τ de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ définis par :

$$\sigma \left| \begin{array}{ccc} \zeta & \mapsto & \zeta^a \\ \theta & \mapsto & \theta \end{array} \right. \; ; \; \tau \left| \begin{array}{ccc} \zeta & \mapsto & \zeta \\ \theta & \mapsto & \zeta\theta \end{array} \right.$$

a) Montrer que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est engendré par σ et τ.

b) Montrer que $\sigma^{-1}\tau\sigma = \tau^{a^{-1}}$, où a^{-1} est l'inverse de a dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

c) En déduire que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$.

Soit k^+ le sous-corps réel maximal de k. On rappelle que $\mathrm{k}^+ = \mathbb{Q}(\zeta+\zeta^{-1})$.

5) Soit $c = \sigma^{\frac{p-1}{2}}$.

a) Vérifier que c est la conjugaison complexe sur K.

b) Vérifier que c laisse fixe $\zeta + \zeta^{-1}$. En déduire que $\mathrm{Gal}(\mathrm{K}/\mathrm{k}^+)$ est engendré par τ et c.

c) Vérifier que $c\tau c = \tau^{-1}$. En déduire que $\mathrm{Gal}(\mathrm{K}/\mathrm{k}^+) \simeq D_{2p}$, où ici D_{2p} est le groupe diédral à $2p$ éléments.

d) Vérifier que $< c >$ n'est pas distingué dans $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

e) Soit $\mathrm{K}^+ = \mathrm{K}^{<c>}$ le sous-corps réel maximal de K. Montrer que $\mathrm{K}^+ = \mathbb{Q}(\zeta + \zeta^{-1}, \sqrt[p]{p})$ puis que K^+ n'est pas totalement réel.

Master de mathématiques
2009-2010
Université de Franche-Comté
CTU
Epreuve préliminaire - Seconde Session
Durée 1h15

Soit $\mathbb{F}_3 = \{0, \pm 1\}$ le corps à trois éléments et soit $\overline{\mathbb{F}_3}$ une clôture algébrique de $\mathbb{F}_3$.
Soit $\sigma : x \mapsto x^3$ l'automorphisme de Frobenius.

1) Déterminer les polynômes irréductibles et unitaires de degré 2 sur $\mathbb{F}_3$.

Soit $\theta \in \overline{\mathbb{F}_3}$ une racine de $P = X^2 + X - 1 \in \mathbb{F}_2[X]$.

2) Montrer que $\mathbb{F}_3(\theta) = \mathbb{F}_9$ et déterminer l'ordre de θ dans $\mathbb{F}_9^\times$.
Exprimer les racines de P dans la $\mathbb{F}_3$-base $\{1, \theta\}$.

3) Soit $Q_b = X^2 + X + \theta + b \in \mathbb{F}_9[X]$, où $b \in \mathbb{F}_3$ est un paramètre.
Soit β une racine de Q_b.

a) Montrer que Q_b est réductible si et seulement si, il existe x et $y \in \mathbb{F}_3$ tels que $\beta = x + y\theta$.

b) Montrer que Q_b est réductible si et seulement si le système suivant (en x et y) a des solutions dans $\mathbb{F}_3$:

$$\begin{cases} x^2 + y^2 + x + b &= 0 \\ xy + y^2 - y - 1 &= 0 \end{cases}$$

c) Montrer que $\mathbb{F}_3(\beta) = \mathbb{F}_{81}$ si et seulement si $b = \pm 1$.

4) Dans cette question, on suppose $b = 1$.

a) Calculer le produit $Q_1 \cdot \sigma(Q_1)$.

b) En déduire $\mathrm{Irr}(\beta, \mathbb{F}_3)$.

Master de mathématiques
2009-2010
Université de Franche-Comté
CTU
Epreuve principale
Seconde session
Durée 2h

Soit $\zeta = \zeta_{20} = \exp(2i\pi/20) \in \mathbb{C}$ une racine primtivie 20-ème de l'unité et soit $\zeta_5 = \zeta^4$.

Soient $\mathrm{K} = \mathbb{Q}(\zeta)$ et $\mathrm{k} = \mathbb{Q}(\zeta_5)$.

1) Déterminer $\mathrm{Irr}(\zeta_5, \mathbb{Q})$.

2) Déterminer $\mathrm{Irr}(\zeta_5 + \zeta_5^{-1}, \mathbb{Q})$. En déduire une expression de $\zeta_5 + \zeta_5^{-1}$ en fonction de $\sqrt{5}$. Montrer que $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$.

3) Déterminer $[\mathrm{K} : \mathbb{Q}]$.

4) Déterminer la structure du groupe de Galois G de $\mathrm{K}/\mathbb{Q}$.

5) Montrer que les extensions quadratiques de $\mathbb{Q}$ contenues dans $\mathrm{K}/\mathbb{Q}$ sont $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(\sqrt{-5})$.

6) Montrer que $(\mathbb{Z}/20\mathbb{Z})^\times = \langle\overline{-1}\rangle \oplus \langle\overline{3}\rangle$.

Pour $\overline{a} \in (\mathbb{Z}/20\mathbb{Z})^\times$, on note σ_a l'élément de $G = \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ défini par $\sigma_a : \zeta \mapsto \zeta^a$.

7) Vérifier que $\mathbb{Q}(\zeta_5) = \mathrm{K}^{\langle\sigma_{-9}\rangle}$.

8) Montrer que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}(\sqrt{5})) = \langle\sigma_{-1}\rangle \oplus \langle\sigma_9\rangle$.

9) Soit $x = \zeta^4 + \zeta^{-4}$ et soit $y = \zeta + \zeta^{-1}$.

a) Justifier le fait que $\mathbb{Q}(\sqrt{5})$ est un sous-corps de $\mathbb{Q}(y)$. Quel est le degré de y sur $\mathbb{Q}(\sqrt{5})$?

b) Déterminer les $\mathbb{Q}(\sqrt{5})$-conjugués de y.

c) Montrer que

$$\mathrm{Irr}(y, \mathrm{k}) = X^2 - X(\zeta + \zeta^{-1} + \zeta^9 + \zeta^{-9}) + \zeta^{10} + \zeta^{-10} + \zeta^8 + \zeta^{-8}.$$

d) Montrer les égalités suivantes :

$$\zeta^{10} = -1, \quad \zeta^9 = -\zeta^{-1}, \quad \zeta^8 + \zeta^{-8} = x^2 - 2 = -x - 1.$$

En déduire que $\mathrm{Irr}(y, \mathrm{k}) = X^2 - (3 + x)$.

10) Montrer l'égalité :

$$\cos(2\pi/20) = \frac{1}{2}\sqrt{3 + \frac{-1 + \sqrt{5}}{2}}.$$

Master de mathématiques
2010-2011
Université de Franche-Comté
CTU
Epreuve préliminaire
Première session
Durée 1h15

Le document "Corps" et les calculatrices sont autorisés

Soit $\mathbb{F}_2 = \{0, 1\}$ le corps à 2 éléments et soit $\overline{\mathbb{F}_2}$ une clôture algébrique de $\mathbb{F}_2$.

1) Déterminer les polynômes irréductibles et unitaires de degré 3 sur $\mathbb{F}_2$.

2) Déterminer les polynômes primitifs de degré 3 sur $\mathbb{F}_2$.

Soit $\theta \in \overline{\mathbb{F}_2}$ une racine de $P = X^3 + X + 1 \in \mathbb{F}_2[X]$.
Soit $\mathrm{K} = \mathbb{F}_2(\theta)$.

3) Déterminer le cardinal $|\mathrm{K}|$ de K.

4) Pour $i \in \{1, 6\}$, soit $a_i \in \{1, \cdots, 6\}$ défini par $1 + \theta^i = \theta^{a_i}$.

Calculer $a_1, \cdots, a_6$.

5) Soit $P_a = X^2 + \theta^2 X + a + \theta \in \mathrm{K}[X]$, où $a \in \mathbb{F}_2$ est un paramètre.

a) Posons $\theta^\infty = 0$. En s'aidant de la question 4), pour $i \in \{0, \cdots, 6, \infty\}$, déterminer les éléments $b_i \in \{0, \cdots, 6, \infty\}$ définis par $P_a(\theta^i) = a + \theta^{b_i}$.

b) Suivant les valeurs de a, déterminer la factorisation de P_a dans $\mathrm{K}[X]$.

c) Si β_a désigne une racine de P_a dans $\overline{\mathbb{F}_2}$, déterminer $|\mathrm{K}(\beta_a)|$.

6) Soit un entier n tel que $2^n - 1 = \ell$, où ℓ est un nombre premier.

a) Donner quelques exemples de tels entiers n.

b) Montrer que tout polynôme irréductible de degré n sur $\mathbb{F}_2[X]$ est primitif.

c) Soit le corps fini $\mathbb{F}_p$ où $p > 2$ est un nombre premier impair. Soit un nombre premier m. Montrer qu'il existe au moins un polynôme irréductible de $\mathbb{F}_p[X]$, de degré m, qui n'est pas primitif.

Master de mathématiques
2010-2011
Université de Franche-Comté
CTU
Epreuve principale
Première session
Durée 2h

Le document "Corps" et les calculatrices sont autorisés

Tous les corps sont vus dans $\mathbb{C}$.

Soit $\zeta = \zeta_{21} = \exp(2i\pi/21) \in \mathbb{C}$ une racine primitive 21-ème de l'unité.
Soit $\mathrm{K} = \mathbb{Q}(\zeta)$.

1) Déterminer $[\mathrm{K} : \mathbb{Q}]$.

2) Déterminer la structure du groupe de Galois G de $\mathrm{K}/\mathbb{Q}$.

3) Déterminer le treillis des sous-corps cyclotomiques de $\mathbb{Q}(\zeta_{21})/\mathbb{Q}$. Pour chaque sous-corps cyclotomique $\mathbb{Q}(\zeta_t)$ de $\mathrm{K}/\mathbb{Q}$, déterminer le polynôme cyclotomique Φ_t.

4) *Etude de* $\mathbb{Q}(\zeta_7)/\mathbb{Q}$.

Posons $z = \zeta_7$ et $\mathrm{F} = \mathbb{Q}(z)$.

a) Déterminer la structure du groupe de Galois H de $\mathrm{F}/\mathbb{Q}$.

b) Vérifier que $(\mathbb{Z}/7\mathbb{Z})^\times = < \overline{-2} >$.

Pour $\overline{a} \in (\mathbb{Z}/7\mathbb{Z})^\times$, on note σ_a l'élément de H défini par

$$\sigma_a : z \mapsto z^a.$$

c) Donner un générateur de H puis déterminer tous les sous-groupes de H. En déduire le treillis des sous-corps de $\mathrm{F}/\mathbb{Q}$.

d) Quel est l'ordre de σ_4 ? Quel est le degré de $F^{<\sigma_4>}/\mathbb{Q}$? Montrer que $z + z^2 + z^4 \in \mathrm{F}^{<\sigma_4>}$.

e) Simplifier $(z + z^2 + z^4)^2$. En déduire le polynôme $\mathrm{Irr}(z + z^2 + z^4, \mathbb{Q})$ puis montrer que $\mathrm{F}^{<\sigma_4>} = \mathbb{Q}(\sqrt{-7})$.

f) Soit $y = z + z^{-1}$ et soit $\mathrm{F}^+ = \mathrm{F}(y)$ le sous-corps réel maximal de F. Calculer $y^3 + y^2$ puis déterminer $\mathrm{Irr}(y, \mathbb{Q})$.

5) Déterminer tous les sous-corps quadratiques de $\mathrm{K}/\mathbb{Q}$.

6) Représenter, sous forme de pavé, le treillis des sous-corps de $\mathrm{K}/\mathbb{Q}$. Donner un élément générateur pour chaque sous-corps L de $\mathrm{K}/\mathbb{Q}$.
Indication : pour la seconde partie de la question, on pourra utiliser un exercice du chapitre 4 du polycopié "Corps".

Master de mathématiques - CTU
2010-2011
Epreuve préliminaire (seconde session)
Durée 1h15
Le document "Corps" et les calculatrices sont autorisés

---

1) Soit le corps $\mathrm{k} = \mathbb{F}_7$.

a) Pour tout élément $a \in \mathrm{k}$, calculer a^2 et a^3.

b) Montrer que dans k l'équation $X^3 + Y^3 = 3Z^3$ (d'inconnues donc $X, Y, Z \in \mathrm{k}$) n'a pas de solution avec $Z \neq 0$.

c) Déterminer toutes les solutions dans k de l'équation $X^2 + Y^2 = 3Z^2$.

2) Soit $\mathrm{k} = \mathbb{F}_q$ le corps fini de cardinal q et soit $\overline{\mathrm{k}}$ une clôture algébrique de k.
Soit $n > 0$ un entier naturel premier à q. Posons $d = \mathrm{pgcd}(q-1, n)$.
Soit θ le morphisme de groupes :

$$\begin{array}{rcl} \theta : \overline{\mathrm{k}}^\times & \to & \overline{\mathrm{k}}^\times \\ x & \mapsto & x^n \end{array}$$

a) Déterminer l'entier r tel que $\mathbb{F}_q(\ker(\theta)) = \mathbb{F}_{q^r}$. Montrer que $\ker(\theta)$ est engendré par un certain élément ε.

b) Soit $d_0 = n/d$. Montrer que $\mathrm{k}^\times \cap \ker(\theta) = < \varepsilon^{d_0} >$.

c) Posons $k^n = \{x^n,\ x \in \mathrm{k}\}$. Montrer que $|\mathrm{k}^n| = \dfrac{q-1}{d} + 1$.

3) Dans $\mathrm{k} = \mathbb{F}_q$, soit l'équation $X^n + aY^n + bZ^n = 0$, où n est un entier naturel premier à q et a, b sont des éléments non nuls de k.
Soit $d = \mathrm{pgcd}(n, q-1)$.

a) Montrer que $|\{ay^n + b,\ y \in \mathrm{k}\}| \geq \dfrac{q-1}{d} + 1$.

b) Montrer que si $0 \in \{ay^n + b,\ y \in \mathrm{k}\}$, alors l'équation diophantienne $X^n + aY^n + bZ^n = 0$ a une solution non triviale dans k (i.e. autre que le triplet $(0,0,0)$).

c) On suppose ici $n = 2$. Montrer que

$$\{ay^2 + b,\ y \in \mathrm{k}\} \cap \mathrm{k}^2 \neq \emptyset.$$

En déduire que l'équation $X^2 + aY^2 + bZ^2 = 0$ a une solution non triviale dans k.

Master de mathématiques - CTU
2009-2010
Université de Franche-Comté
CTU
Epreuve príncipale (seconde session)
Durée 2h

Le document "Corps" et les calculatrices sont autorisés

Les corps sont vus dans $\mathbb{C}$.

Soit $\mathrm{k} = \mathbb{Q}(\zeta)$, avec $\zeta = \zeta_{17} = \exp(2i\pi/17)$.
Pour $\overline{a} \in (\mathbb{Z}/17\mathbb{Z})^\times$, on note σ_a l'élément de $G = \mathrm{Gal}(\mathrm{k}/\mathbb{Q})$ défini par

$$\sigma_a : \zeta \mapsto \zeta^a.$$

1) Déterminer $[\mathrm{k} : \mathbb{Q}]$ et le polynôme irréductible $\mathrm{Irr}(\zeta, \mathbb{Q})$ de ζ sur $\mathbb{Q}$.

2) Déterminer la structure du groupe G. Montrer que G est engendré par σ_3. Déterminer tous les sous-groupes de G.

3) Soit H_1 le sous-groupe de G engendré par σ_4 et $\mathrm{k}_1 = \mathrm{k}^{H_1}$. Déterminer la structure de H_1, le degré de k_1/k et le groupe de Galois de $\mathrm{k}_1/\mathbb{Q}$.

Soit $x = \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4}$.

4) Vérifier que $x \in \mathrm{k}_1$.

5) Soit $\mathrm{k}_2 = \mathrm{k}^{<\sigma_2>}$. Vérifier que $x \notin \mathrm{k}_2$. En déduire que $\mathrm{k}_1 = \mathbb{Q}(x)$.

6) Montrer que $G/H_1 = < \overline{\sigma_1}, \overline{\sigma_3}, \overline{\sigma_9}, \overline{\sigma_{10}} >$.
En déduire les $\mathbb{Q}$-conjugués de x.

Soit $\mathrm{Irr}(x, \mathbb{Q}) = X^4 + aX^3 + bX^2 + cX + d$ le polynôme irréductible de x sur $\mathbb{Q}$.

7) Exprimer a, b, c, d à l'aide des $\mathbb{Q}$-conjugués de x.
Calculer a.

8) Soit $y = x + \sigma_2(x)$. Montrer que $\mathrm{k}_2 = \mathbb{Q}(y)$.

9) Calculer $y^2 + y$. En déduire $\mathrm{Irr}(y, \mathbb{Q})$. Exprimer y à partir de $\sqrt{17}$. Montrer que $\mathrm{k}_2 = \mathbb{Q}(\sqrt{17})$.

10) Déterminer l'ensemble des sous corps de $\mathrm{k}/\mathbb{Q}$.

11) Calculer $x\sigma_2(x)$. En déduire $\mathrm{Irr}(x, \mathrm{k}_2)$, puis une expression de x à l'aide de racines carrées.

12) Exprimer les $\mathbb{Q}$-conjugués de x à l'aide de racines carrées.

13) *Question bonus...* Retour à la question 7) : déterminer b, c, d.

Université de Franche-Comté
Master mathématiques et applications
1 ère année

Examen de l'unité "Corps"
Première session - 2011 /2012

Durée 3h

Seul le document "Corps" est autorisé

Exercice 1
Soit $\zeta = exp(2i\pi/48) \in \mathbb{C}$ une racine primitive 48-ème de l'unité.

1) Déterminer le treillis des **sous-corps cyclotomiques** de $\mathbb{Q}(\zeta)/\mathbb{Q}$. Préciser le degré de chaque extension.

2) Pour chaque corps cyclotomique $\mathbb{Q}(\zeta_m)$ qui apparaît dans la question 1), déterminer le polynôme cyclotomique Φ_m associé.

Exercice 2
Soit le nombre réel

$$\theta = \sqrt{1+\sqrt{2}}.$$

1) Montrer que θ est racine du polynôme $P = X^4 - 2X^2 - 1 \in \mathbb{Z}[X]$.

On notera par K le corps des racines de P.

2) Déterminer les polynômes irréductibles (unitaires) de degré 2 sur $\mathbb{F}_3$. Montrer que le polynôme $R = X^4 + X^2 + 2 \in \mathbb{F}_3[X]$ est irréductible (sur $\mathbb{F}_3$).

3) En déduire que P est irréductible sur $\mathbb{Q}$ et déterminer $[\mathbb{Q}(\theta) : \mathbb{Q}]$.

4) Montrer que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\theta)$ et déterminer le polynôme irréductible de θ sur $\mathbb{Q}(\sqrt{2})$.

Soit $\beta \in \mathbb{C}$ une racine de $X^2 - (1 - \sqrt{2}) \ \in \mathbb{Q}(\sqrt{2})[X]$.

5) Montrer que $\mathrm{K} = \mathbb{Q}(\theta, \beta)$.

6) Notons par $i \in \mathbb{C}$ une racine de $X^2 + 1$. Calculer $\theta\beta$.
En déduire : $\mathrm{K} = \mathbb{Q}(\theta, i)$, puis : $[\mathrm{K} : \mathbb{Q}] = 8$.

7) Pourquoi le groupe $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ n'est-il pas commutatif ? À isomorphisme près, quelles sont les structures possibles pour $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$?

8) Soit $\mathrm{k} = \mathbb{Q}(i)$. Déterminer le polynôme irréductible de θ sur k.

9) Soient les éléments σ et τ du groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$:

$$\sigma \left| \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \theta & \mapsto & -\theta \end{array} \right. ; \ \tau \left| \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \theta & \mapsto & i/\theta \end{array} \right.$$

Montrer que $\mathrm{Gal}(\mathrm{K}/\mathrm{k})$ est engendré par σ et τ.
En déduire que $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ puis que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq D_8$.

10) Montrer que $\theta + i/\theta \ \in \mathrm{K}^{<\tau>}$ et que $\theta + i/\theta \ \notin \mathrm{k}$.
Calculer $(\theta + i/\theta)^2$ et en déduire le polynôme irréductible de $\theta + i/\theta$ sur k.

11) Montrer que les corps

$$\mathrm{k}(\sqrt{2}), \ \mathrm{k}(\sqrt{2(i-1)}), \ \mathrm{k}(\sqrt{i-1})$$

sont les sous-corps stricts de K/k.

Exercice 3
Soit $\mathbb{F}_3$ le corps à 3 éléments.

1) Montrer que le polynôme $P = X^2 + 1 \in \mathbb{F}_3[X]$ est irréductible sur $\mathbb{F}_3$.

Soit θ une racine de P dans une clôture algébrique $\overline{\mathbb{F}_3}$ de $\mathbb{F}_3$.
Soit $\mathrm{k} = \mathbb{F}_3(\theta)$.

2) Quel est le cardinal de k ? Que vaut θ^2 ?

3) Pour $a, b \in \mathbb{F}_3$, soit $P_{a,b} = X^2 + aX + b\theta \ \in \mathrm{k}[X]$.

Soit $t = t(a, b)$ l'unique entier pour lequel $\mathbb{F}_{3^t}$ est le corps des racines sur k de $P_{a,b}$.

a) Montrer que les valeurs possibles pour t sont $t = 2$ et $t = 4$.

b) Si $x \in$ k est une racine double de $P_{a,b}$, déterminer x. En déduire $t(0, 0)$.

c) Soit $x = a_0 + b_0\theta$, $a_0, b_0 \in \mathbb{F}_3$. Exprimer $P_{a,b}(x)$ dans la $\mathbb{F}_3$-base $\{1, \theta\}$ de k.

d) Montrer que pour $b = 0$ le polynôme $P_{a,b}$ est réductible sur k. Montrer qu'il en est de même quand $a = 0$.

e) Déterminer les couples (a, b) pour lesquels P est irréductible sur k.

f) En déduire les couples (a, b) pour lesquels $t(a, b) = 2$.

Université de Franche-Comté - CTU
Master mathématiques et applications
1 ère année

Examen de l'unité "Corps"
Seconde session - 2011 /2012

Durée 3h

Le document "Corps" et les calculatrices sont autorisés

Exercice 1
Soient deux entiers strictement positifs a et b vérifiant $a^2 - b = 1$.

1) Montrer que b n'est pas un carré.

Pour toute la suite, on suppose de plus que le nombre entier a est tel que le polynôme $R = X^3 - 3X - 2a$ est irréductible sur $\mathbb{Q}$.

2) Donner une infinité de nombres a vérifiant la condition précédente.

Soit le nombre réel

$$\theta = \sqrt[3]{a + \sqrt{b}}.$$

3) Montrer que θ est racine du polynôme $P = X^6 - 2aX^3 + 1 \ \in \mathbb{Z}[X]$.

4) Montrer que si θ ou θ^2 est un élément de $\mathbb{Q}$, alors $\sqrt{b} \in \mathbb{Q}$. Conclure.

5) Montrer que $\theta + 1/\theta$ est racine du polynôme $R = X^3 - 3X - 2a$. En déduire que $\theta + 1/\theta \ \notin \mathbb{Q}$.

6) Montrer que si $x \in \mathbb{C}$ est une racine de P alors $1/x$ est aussi une racine de P. En déduire que les racines de P dans $\mathbb{C}$ sont les nombres

$$\theta, \quad j\theta, \quad j^2\theta, \quad 1/\theta, \quad j/\theta, \quad j^2/\theta$$

où $j \in \mathbb{C}$ est une racine primitive cubique de l'unité. (Ne pas oublier de vérifier que ces racines sont 2 à 2 distinctes.)

7) Déterminer la factorisation de P sur $\mathbb{R}[X]$. En déduire que P est irréductible sur $\mathbb{Q}$. (On pourra utiliser les conclusions des questions 4) et 5).)

On notera par K le corps des racines de P.

8) Montrer que $\mathrm{K} = \mathbb{Q}(j, \theta)$. En déduire que $[\mathrm{K} : \mathbb{Q}] = 12$

9) Soit $\mathrm{k} = \mathbb{Q}(j)$. Déterminer le polynôme irréductible de θ sur k.

10) Quel est l'ordre du groupe de Galois Gal(K/k) ?

11) Soient les éléments σ et τ de Gal(K/k) définis par

$$\sigma : \theta \mapsto j\theta \quad ; \quad \tau : \theta \mapsto 1/\theta.$$

a) Calculer $\sigma \circ \tau$ et $\tau \circ \sigma$.
b) Montrer que Gal(K/k) est engendré par σ et τ.
c) Montrer que $\mathrm{Gal(K/k)} \simeq D_6$.

12) Soit $\mathrm{c} \in \mathrm{Gal(K/\mathbb{Q})}$ la conjugaison complexe.
a) Montrer que le sous-groupe $< c >$ n'est pas distingué dans Gal(K/$\mathbb{Q}$).
b) Montrer que le groupe Gal(K/$\mathbb{Q}$) est engendré par les sous-groupes $< \mathrm{c} >$ et Gal(K/k).
c) Montrer que Gal(K/k) est distingué dans Gal(K/$\mathbb{Q}$) puis que $\mathrm{Gal(K/\mathbb{Q})} \simeq \mathbb{Z}/2\mathbb{Z} \ltimes D_6$. En déduire que $\mathrm{Gal(K/\mathbb{Q})} \simeq D_{12}$.

Exercice 2
Soit p un nombre premier et soit le corps fini $\mathbb{F}_p$ à p éléments.
Fixons une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$.

Soit $P = X^p - X + a \in \mathbb{F}_p[X]$, où a est un élément non nul de $\mathbb{F}_p$.

Soit α une racine de P dans $\overline{\mathbb{F}_p}$.

1) Montrer que $\alpha \notin \mathbb{F}_p$.

2) Montrer que les racines de P sont de la forme $\alpha + b$, avec $b \in \mathbb{F}_p$.

3) En déduire que $\mathbb{F}_p(\alpha)$ est le corps des racines de P dans $\overline{\mathbb{F}_p}$.

4) On va déterminer le degré $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$.

a) Soit $Q \in \mathbb{F}_p[X]$ un facteur unitaire de P de degré au moins 1. Montrer qu'il existe $b_1, \cdots, b_r$ des éléments de $\mathbb{F}_p$ tels que

$$Q = \prod_{i=1}^{r} (X - \alpha - b_i).$$

b) En regardant les termes de degré $r - 1$, montrer que $r\alpha \in \mathbb{F}_p$.

c) En déduire que le polynôme Q est de degré p puis que $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^p}$.

5) Application. Montrer que pour tout nombre premier p, le polynôme $X^p - X + 1 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$.

Université de Franche-Comté
Master mathématiques et applications - 1 ère année

Examen de l'unité "Corps"
CTU

29 mai 2013

Le document "Corps" et les calculatrices sont autorisés

Exercice 1.
Soit $\zeta \in \mathbb{C}$ une racine primitive 1125-ème de l'unité.

1) Déterminer $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

2) Déterminer le treillis des sous-corps cyclotomiques de $\mathbb{Q}(\zeta)/\mathbb{Q}$ en indiquant le degré des extensions relatives.

3) Déterminer les p-Sylow du groupe de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Exercice 2.
Soit K/k une extension galoisienne finie de groupe de Galois G. On note par Tr la trace de K/k : pour $x \in$ K,

$$\mathrm{Tr}(x) = \sum_{\sigma \in \mathrm{G}} \sigma(x).$$

1) Montrer que Tr est une application k-linéaire sur le k-espace vectoriel K.

2) Montrer que pour tout $x \in$ K, $\mathrm{Tr}(x) \in$ k.

3) Montrer que l'application Tr n'est pas nulle.

4) En déduire que l'image de Tr est exactement le corps k.

Exercice 3.
Soit $\mathrm{k} = \mathbb{F}_q$ le corps fini de cardinal q et soit $\overline{\mathrm{k}}$ une clôture algébrique de k.
Soit $n > 0$ un entier naturel premier à q. Posons $d = \mathrm{pgcd}(q-1, n)$.

Soit φ le morphisme de groupes :

$$\begin{array}{rcl} \varphi : \overline{\mathrm{k}}^{\times} & \to & \overline{\mathrm{k}}^{\times} \\ x & \mapsto & x^n \end{array}$$

1) Déterminer $|\ker(\varphi)|$ et montrer que $\ker(\varphi)$ est engendré par un certain élément ε.

2) Déterminer l'entier r tel que $\mathbb{F}_q(\ker(\varphi)) = \mathbb{F}_{q^r}$.

3) Soit $d_0 = n/d$. Montrer que $\mathrm{k}^{\times} \cap \ker(\varphi) =< \varepsilon^{d_0} >$.

4) Posons $\mathrm{k}(n) = \{x^n,\ x \in \mathrm{k}\}$. Montrer que $|\mathrm{k}(n)| = \dfrac{q-1}{d} + 1$.
Application : Déterminer $|\mathbb{F}_{49}(15)|$.

On suppose maintenant q impair.

On considère sur $\mathbb{F}_q$ la forme quadratique $q(X, Y, Z) = X^2 + aY^2 + bZ^2$, où a et b sont deux éléments non-nuls de $\mathbb{F}_q$.

5) Montrer que $|\{x^2 + a,\ x \in \mathrm{k}\}| = \dfrac{q-1}{2} + 1$.

6) En déduire que $\{x^2 + a,\ x \in \mathrm{k}\} \cap \mathrm{k}(2) \neq \emptyset$ puis que la forme q admet un zéro non trivial : il existe $(x, y, z) \in \mathbb{F}_q^3 \backslash (0, 0, 0)$ tel que $q(x, y, z) = 0$.

Exercice 4.
Les extensions considérées sont dans $\mathbb{C}$.

Soit $m \in \mathbb{Z}\backslash\{0, 1\}$ un entier (relatif) sans facteur carré.
On suppose que l'entier m est de la forme $m = a^2 - b^2$, $a, b \in \mathrm{N}\backslash\{0\}$.

1) Montrer que m est nécessairement impair.

Soit le polynôme $P = X^4 - 4aX^2 + 4m \ \in \mathbb{Q}[X]$.

2) Montrer que si $\alpha \in \mathbb{Q}$ est une racine de P alors $\alpha = \pm 1$. Arriver à une contradiction.

Soient $\mathrm{k} = \mathbb{Q}(\sqrt{m})$ et $\mathrm{K} = \mathbb{Q}(\sqrt{a + \sqrt{m}})$. Posons $\theta = \sqrt{a + \sqrt{m}}$.

3) Déterminer $[\mathrm{k} : \mathbb{Q}]$ et montrer que $\mathrm{k} \subset \mathrm{K}$.

4) Supposons que $a + \sqrt{m} = (x + y\sqrt{m})^2$, avec $x, y \in \mathbb{Q}$. A l'aide de la question 1) arriver à une contradiction. En déduire $[\mathrm{K} : \mathbb{Q}]$ puis le polynôme irréductible de θ sur $\mathbb{Q}$.

5) Soient σ_0 et σ_1 les deux automorphismes de $\mathrm{k}/\mathbb{Q}$ définis par $\sigma_0(\sqrt{m}) = \sqrt{m}$ et $\sigma_1(\sqrt{m}) = -\sqrt{m}$.

a) Déterminer les $\mathbb{Q}$-plongements $\sigma_{i,j}$ de $\mathrm{k}(\theta)$ dans $\mathbb{C}$ prolongeant σ_i (ici $i = 0, 1$, $j = 0, 1$).

b) Calculer le produit $\sigma_{0,0}(\theta)\sigma_{1,0}(\theta)$. En déduire que $\mathrm{K}/\mathbb{Q}$ est une extension galoisienne.

c) Déterminer $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

6) Soit $\beta = \sigma_{0,0}(\theta) + \sigma_{1,0}(\theta)$.

a) Calculer β^2 et montrer que $\beta^2 \notin \mathbb{Q}$.

b) Déterminer tous les sous-corps de $\mathrm{K}/\mathbb{Q}$.

Université de Franche-Comté
Master mathématiques et applications
1 ère année

Examen de l'unité "Corps"

2nde session - 2012/2013

Durée 3h

Le document "Corps" et les calculatrices sont autorisés

Exercice 1.
Donner un exemple d'un polynôme irréductible non séparable. Justifier.

Exercice 2.
Si $\mathbb{F}_q$ désigne le corps fini à q éléments et n un entier, on note $I(q,n)$ l'ensemble des polynômes unitaires irréductibles de degré n à coefficients dans $\mathbb{F}_q$ et on pose

$$A(q,n) = \#I(q,n)$$

Fixons $\mathbb{F}_q$ et un **nombre premier** ℓ.

1) Soit $x \in \mathbb{F}_{q^\ell}$. Quels sont les degrés possibles pour l'extension $\mathbb{F}_q(x)/\mathbb{F}_q$?

2) En déduire l'égalité $A(q,\ell) = \dfrac{q^\ell - q}{\ell}$.

3) Après avoir calculé $A(2,2)$ et $A(2,3)$, déterminer tous les polynômes irréductibles (unitaires) de degré 2 et 3 sur $\mathbb{F}_2$.

4) Soit θ une racine de $X^2 + X + 1 \in \mathbb{F}_2[X]$ dans une clôture algébrique de $\mathbb{F}_2$.
a) Quel est le cardinal de $\mathbb{F}_2(\theta)$?

b) Après avoir calculé $A(4,2)$, déterminer tous les polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.

5) Déterminer, de deux faccons différentes, les polynômes irréductibles de degré 4 sur $\mathbb{F}_2$.
Indication. Utiliser les questions 3) et 4).

6) Déterminer les polynômes primitifs de degré 4 sur $\mathbb{F}_2$.

Exercice 3.
Fixons le nombre complexe a.
Soit $\mathrm{K} = \mathbb{C}\left(\dfrac{X^3}{X+2a}\right)$ le corps des fractions rationnelles en $Y = \dfrac{X^3}{X+2a}$.

1) Montrer que $\mathbb{C}(X)$ est une extension algébrique de $\mathbb{C}(Y)$.

Fixons $\overline{\mathrm{K}}$ une clôture algébrique de K (contenant X).

2) On suppose $a = 0$.
a) Montrer que Y n'est pas un carré dans $\mathrm{K} = \mathbb{C}(Y)$.

b) En déduire le degré $[\mathbb{C}(X) : \mathbb{C}(Y)]$.

c) Montrer que $\mathbb{C}(X)/\mathbb{C}(Y)$ est une extension galoisienne. Déterminer alors $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(Y))$.

3) On suppose $a \neq 0$.
a) Montrer que le polynôme $P(Z) = Z^3 - YZ - 2aY \in \mathrm{K}[Z]$ est irréductible (sur K).

b) Soient X_1, X_2, X_3 les racines de P dans $\overline{\mathrm{K}}$ et soit P' le polynôme dérivé de P. Calculer de deux faccons différentes le produit $P'(X_1)P'(X_2)P'(X_3)$.

c) En déduire l'égalité $[(X_1 - X_2)(X_2 - X_3)(X_3 - X_1)]^2 = 4Y^2(Y - 27a^2)$.

d) Déterminer le groupe de Galois de $\mathrm{K}(X_1, X_2, X_3)/\mathrm{K}$.

e) En déduire le treillis des sous-corps de $\mathbb{C}(X_1, X_2, X_3, Y)/\mathbb{C}(Y)$.

Université de Franche-Comté
Master mathématiques et applications - 1ère année

Examen de l'unité "Corps"
Première session - 2013 /2014

Durée 3h

Seul le document "Corps" est autorisé - Calculatrice interdite

---

Exercice 1
Soit $\mathbb{F}_2$ le corps à deux éléments et soit $P = X^5 + X^4 + 1 \in \mathbb{F}_2[X]$.
Soit $\mathrm{K} = \mathbb{F}_{2^t}$ le corps des racines de P sur $\mathbb{F}_2$. Déterminer l'entier t.

Excercice 2.
Dans cet exercice les éléments sont vus dans le corps des nombres complexes $\mathbb{C}$.

Soient deux nombres premiers (impairs) distincts p et ℓ.
Soit $\sqrt[p]{p}$ (respectivement $\sqrt[\ell]{\ell}$) la racine réelle du polynôme $X^p - p$ (respectivement de $X^\ell - \ell$).

1) Montrer que le degré sur $\mathbb{Q}$ de l'élément $\sqrt[p]{p} + \sqrt[\ell]{\ell}$ divise $p\ell$.

Soit ζ_p (respectivement ζ_ℓ) une racine primitive p-ème de l'unité (respectivement ℓ-ème de l'unité) et soit le corps de nombres $\mathrm{k}_\ell = \mathbb{Q}(\zeta_\ell)$.

2) Rappeler le polynôme irréductible P de ζ_p sur $\mathbb{Q}$.
En déduire que le polynôme $P(X+1)$ est le polynôme irréductible de $\zeta_p - 1$ sur $\mathbb{Q}$ puis que $\mathrm{N}_{\mathrm{k}_p/\mathbb{Q}}(\zeta_p - 1) = p$, où $\mathrm{N}_{\mathrm{k}_p/\mathbb{Q}}$ est la norme dans $\mathrm{k}_p/\mathbb{Q}$.

Soit $\mathrm{K} = \mathbb{Q}(\zeta_p, \zeta_\ell) = \mathrm{k}_p\mathrm{k}_\ell$.

3) Déterminer $[\mathrm{K} : \mathbb{Q}]$ et donner la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

4) Montrer que $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\zeta_p - 1) = p^{\ell-1}$.

Soit le corps $\mathrm{L} = \mathrm{K}(\sqrt[p]{p}, \sqrt[\ell]{\ell})$.

5) Montrer que $\sqrt[p]{p} \notin \mathrm{K}$. En déduire $[\mathrm{L} : \mathrm{K}]$.

6) Montrer que L/K est galoisienne et déterminer $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$.

7) Soit $\sigma \in \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Montrer qu'il existe deux entiers $j \in \{0, \cdots, p-1\}$ et $k \in \{0, \cdots, k-1\}$ tels que $\sigma(\sqrt[p]{p} + \sqrt[\ell]{\ell}) = \zeta_p^j \sqrt[p]{p} + \zeta_\ell^k \sqrt[\ell]{\ell}$.

8) Montrer que $\sigma(\sqrt[p]{p} + \sqrt[\ell]{\ell}) = \sqrt[p]{p} + \sqrt[\ell]{\ell}$ si et seulement si, $\sigma = id$. En déduire que $\mathrm{L} = \mathrm{K}(\sqrt[p]{p} + \sqrt[\ell]{\ell})$.

(Indication. Utiliser la question 4).)

9) Montrer que l'élément $\sqrt[p]{p} + \sqrt[\ell]{\ell}$ est de degré $p\ell$ sur $\mathbb{Q}$.

Exercice 3.
Dans cet exercice les éléments sont vus dans le corps des nombres complexes $\mathbb{C}$. On désignera par $i \in \mathbb{C}$ une racine primitive 4-ème de l'unité.

Soient deux entiers positifs a et b tels que

- $a > 1$ est sans facteur carré ;
- $b^2 = a + 1$;
- $2b + 2$ n'est pas un carré.

1) Montrer que nécessairement b est pair. Donner deux exemples de tels couples (a, b).

Soit θ le nombre réel

$$\theta = \sqrt[4]{b + \sqrt{a}}$$

et soit $P = X^8 - 2bX^4 + 1 \in \mathbb{Q}[X]$.

2) Montrer que θ et $1/\theta$ sont deux racines distinctes de P. En déduire toutes les racines de P.

Soit le corps $\mathrm{k} = \mathbb{Q}(\sqrt{a})$.

3) Soit le polynôme $Q = X^4 - (b + \sqrt{a}) \in \mathrm{k}[X]$.

a) Montrer que $\mathrm{k}/\mathbb{Q}$ est une extension galoisienne engendrée par l'automorphisme $\sigma : \sqrt{a} \mapsto -\sqrt{a}$.

b) Supposons que Q admette une racine α dans le corps k.

(i) Montrer que le polynôme $(X - \alpha)(X - \sigma(\alpha))$ est à coefficients dans $\mathbb{Q}$ et que ce celui-ci divise P dans $\mathbb{Q}[X]$.

(ii) Montrer que $\theta^2 \notin \mathbb{Q}$. De même, montrer que $\theta \pm \dfrac{1}{\theta} \notin \mathbb{Q}$.

(iii) En déduire que Q n'a pas de racine dans le corps k.

c) Montrer que le polynôme Q est irréductible sur k.

Soit $\mathrm{K} = \mathrm{k}(\theta)$, $\mathrm{L} = \mathrm{K}(i)$ et $\mathrm{N} = \mathbb{Q}(i)$.

4) Déterminer $[\mathrm{K} : \mathbb{Q}]$, $[\mathrm{L} : \mathbb{Q}]$ et $[\mathrm{L} : \mathrm{N}]$. En déduire le polynôme irréductible de θ sur N.

5) Montrer que L est le corps des racines de P sur $\mathbb{Q}$.

6) Soit $\mathrm{G} = \mathrm{Gal}(\mathrm{L}/\mathrm{N})$.

a) Déterminer tous les éléments de $\mathrm{G} = \mathrm{Gal}(\mathrm{L}/\mathrm{N})$.

b) Soient les deux éléments s et t de G définis par $s(\theta) = 1/\theta$ et $t(\theta) = i\theta$.
Vérifier que s est d'ordre 2, que t est d'ordre 4 et que $sts = t^{-1}$.

En déduire que $G =< s, t > \simeq D_8$, où D_8 est le groupe diédral d'ordre 8.

7) Soit $\Gamma = \mathrm{Gal}(L/\mathbb{Q})$ et soit $H = \mathrm{Gal}(L/K)$. Notons par τ un générateur de H.

a) Montrer que $G \lhd \Gamma$. Expliciter $\tau s \tau$ et $\tau t \tau$.

b) Montrer que $\Gamma = H \ltimes G \simeq \mathbb{Z}/2\mathbb{Z} \ltimes D_8$.

Université de Franche-Comté
Master mathématiques et applications - 1 ère année

Examen de l'unité "Corps"
CTU

Seconde session - 2013 /2014

Durée 3h

Seul le document "Corps" est autorisé - Calculatrice interdite

---

Exercice 1
Soit $\mathbb{F}_2$ le corps fini à 2 éléments et soit $\overline{\mathbb{F}_2}$ une clôture algébrique de $\mathbb{F}_2$. Soit $\omega \in \overline{\mathbb{F}_2}$ vérifiant $\omega^2 + \omega + 1 = 0$.

1) Montrer que $\mathbb{F}_2(\omega) = \mathbb{F}_4$.

2) Déterminer l'ensemble des polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.

3) Soit $\theta \in \overline{\mathbb{F}_2}$ une racine de $X^2 + X + \omega$. Déterminer l'ordre de θ dans $\overline{\mathbb{F}_2}^\times$.

4) Donner un polynôme primitif de degré 4 sur $\mathbb{F}_2$.

Excercice 2.
Soit $\mathbb{Q}(T)$ le corps des fractions rationnelles à coefficients dans $\mathbb{Q}$.
Fixons une clotûre algébrique $\overline{\mathbb{Q}(T)}$ de $\mathbb{Q}(T)$. Tous les éléments de cet exercice sont vus dans $\overline{\mathbb{Q}(T)}$.

1) Soit une fraction rationnelle $x \in \mathbb{Q}(T)^\times$.
Montrer que x est algébrique sur $\mathbb{Q}$ si et seulement si, $x \in \mathbb{Q}^\times$.

Soit $p > 2$ un nombre premier et soit $\zeta \in \overline{\mathbb{Q}(T)}$ une racine primitive p-ème de l'unité : $\zeta \neq 1$ et $\zeta^p = 1$.

2) Montrer que l'extenstion $\mathbb{Q}(T,\zeta)/\mathbb{Q}(T)$ est galoisienne et déterminer son groupe de Galois.

Soit le polynôme $P = X^p - T \in \mathbb{Q}(T)[X]$ et soit θ une racine de P dans $\overline{\mathbb{Q}(T)}$. Soit $\mathrm{K} = \mathbb{Q}(T,\zeta,\theta)$.

3) Quel est le degré de $\mathbb{Q}(T,\theta)/\mathbb{Q}(T)$? En déduire que P est irréductible sur $\mathbb{Q}(T,\zeta)$.

4) Montrer que $\mathrm{K}/\mathbb{Q}(T,\zeta)$ est une extension galoisienne cyclique de degré p, de groupe de Galois engendré par $\tau : \theta \mapsto \zeta\theta$.

5) Montrer que l'extension $\mathrm{K}/\mathbb{Q}(T)$ est galoisienne.

6) Soient les éléments σ et τ de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}(T))$ définis par :

$$\sigma \left| \begin{array}{ccc} \zeta & \mapsto & \zeta^a \\ \theta & \mapsto & \theta \end{array} \right. ; \ \tau \left| \begin{array}{ccc} \zeta & \mapsto & \zeta \\ \theta & \mapsto & \zeta\theta \end{array} \right.$$

où $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un élément d'ordre $p-1$.

a) Montrer que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}(T))$ est engendré par σ et τ.

b) Montrer que $\sigma^{-1}\tau\sigma = \tau^{a^{-1}}$, où a^{-1} est l'inverse de a dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

c) En déduire que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}(T)) \simeq \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$.

7) Que devient l'extension $\mathbb{Q}(T,\zeta,\theta)/\mathbb{Q}(T)$ quand on remplace l'indéterminée T par

a) l'entier 0 ?

b) l'entier 1 ?

c) l'entier -1 ?

d) un entier $m > 1$ non divisible par une puissance p-ème d'un entier différent de 1 ?

(Quand l'extension obtenue est galoisienne, déterminer son groupe de Galois.)

Université de Franche-Comté
Master mathématiques et applications
1ère année (CTU)

Examen de l'unité "Corps"
Première session - 2018 /2019

Durée 3h

Seul le document "Corps" est autorisé (sans annotation) - Calculatrice interdite

---

Exercice 1
Soit $\mathbb{F}_2$ le corps à deux éléments.
Notons par θ une racine de $P = X^2 + X + 1$ dans une clôture algébrique de $\mathbb{F}_2$. On pose $\mathrm{K} = \mathbb{F}_2(\theta)$.

1) Montrer que $\{1, \theta\}$ forme une $\mathbb{F}_2$-base de K.

2) Exprimer θ^3 et $(\theta + 1)^3$ dans $\{1, \theta\}$.

Pour $\alpha \in \mathrm{K}$, soit le polynôme $P_\alpha = X^3 + \theta X + \alpha \in \mathrm{K}[X]$ (de paramètre α).

3) Déterminer les valeurs de α pour lesquelles le polynôme P_α est irréductible.

4) Factoriser P_α lorsqu'il est réductible.

5) On note par L le corps des racines de P_α sur K. Déterminer, suivant α, l'entier t tel que $\mathrm{L} = \mathbb{F}_{2^t}$.

Exercice 2.
Dans cet exercice les éléments sont vus dans le corps des nombres complexes $\mathbb{C}$. On désignera par $i \in \mathbb{C}$ une racine primitive 4-ème de l'unité.

Soit le polynôme $P = X^8 - 10X^4 + 1 \in \mathbb{Q}[X]$, et soit le nombre réel

$$\theta = \sqrt{\sqrt{2} + \sqrt{3}}.$$

On pose $\mathrm{K} = \mathbb{Q}(\theta)$ puis $\mathrm{L} = \mathrm{K}(i) = \mathbb{Q}(\theta, i)$.

1) Montrer que θ et $1/\theta$ sont des racines distinctes de P.

2) En déduire toutes les racines de P (en fonction de θ), puis que L est le corps des racines de P.

Soit le corps $\mathrm{k} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

3) Quel est le degré de l'extension $\mathrm{k}/\mathbb{Q}$? Montrer que la famille $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ forme une $\mathbb{Q}$-base de k.

4) Montrer que $\sqrt{2} + \sqrt{3}$ n'est pas un carré dans k, c'est à dire qu'il n'existe pas d'élément $\alpha \in \mathrm{k}$ tel que $\alpha^2 = \sqrt{2} + \sqrt{3}$. Quel est le polynôme irréductible R de θ sur k ?

5) En déduire le degré de l'extension $\mathrm{K}/\mathbb{Q}$, puis que P est irréductible sur $\mathbb{Q}$. Donner tous les $\mathbb{Q}$-plongements de K dans $\mathbb{C}$.

6) Montrer que $[\mathrm{L} : \mathbb{Q}] = 16$ et donner tous les $\mathbb{Q}$-automorphismes de L.

7) Montrer que l'extension $\mathrm{k}/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et engendré par les automorphismes σ_2 et σ_3 définis par :

$$\sigma_2 \left| \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array} \right. \; ; \; \sigma_3 \left| \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array} \right. .$$

Montrer que $\mathrm{k} = \mathbb{Q}(\theta^2)$.

7) Vérifier que les $\mathbb{Q}$-plongements $\sigma_{2,+}$ et $\sigma_{2,-}$ de K dans $\mathbb{C}$ définis par $\sigma_{2,+}(\theta) = 1/\theta$ et $\sigma_{2,-}(\theta) = -1/\theta$ sont ceux qui prolongent σ_2.
Vérifier que les $\mathbb{Q}$-plongements $\sigma_{3,+}$ et $\sigma_{3,-}$ de K dans $\mathbb{C}$ définis par $\sigma_{3,+}(\theta) = i/\theta$ et $\sigma_{3,-}(\theta) = -i/\theta$ sont ceux qui prolongent σ_3.

8) Soit $\sigma \in \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ défini par $\sigma = \left| \begin{array}{ccc} i & \mapsto & i \\ \theta & \mapsto & i\theta \end{array} \right.$.
Vérifier que $\sigma_{|\mathrm{K}} = \sigma_{2,+} \circ \sigma_{3,+}$ et montrer que σ est d'ordre 4.

9) Soit $\tau \in \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ défini par $\tau = \left| \begin{array}{ccc} i & \mapsto & i \\ \theta & \mapsto & 1/\theta \end{array} \right.$.
On note $H = \langle \sigma, \tau \rangle$ le sous-groupe de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ engendré par σ et τ.
a) Vérifier que $\tau \circ \sigma \circ \tau = \sigma^{-1}$.
b) Montrer que H est isomorphe au groupe dihédral D_8 d'ordre 8.
c) Quel est le sous-corps F de $\mathrm{L}/\mathbb{Q}$ correspondant par la théorie de Galois au groupe H ?

10) Soit $\gamma \in \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ défini par $\gamma = \left| \begin{array}{ccc} i & \mapsto & -i \\ \theta & \mapsto & 1/\theta \end{array} \right.$.
a) Vérifier que $\gamma \notin H$.
b) Vérifier que γ commute avec tous les éléments de H.

11) Montrer que $\mathrm{Gal}(\mathrm{L}/\mathbb{Q}) = \langle \gamma \rangle \times H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_8$.

12) Montrer que $\theta + i$ est un élément primitif de l'extension $\mathrm{L}/\mathbb{Q}$.

13) Soit Z le sous-groupe de $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ engendré par σ^2 et $\gamma \circ \tau$.
a) Montrer que $Z \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
b) Montrer que k est le sous-corps de L correspondant par la théorie de Galois au groupe Z.

14) On note par N le sous-corps de L correspondant par la théorie de Galois au groupe $\langle \gamma \rangle$.

a) Montrer que l'extension $\mathrm{N}/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à D_8.

b) Soit $\alpha = \theta + 1/\theta$ et $\beta = i(\theta - 1/\theta)$. Vérifier que α et β sont des racines du polynôme $S = X^4 - 4X^2 - 8$.

c) Factoriser S sur $\mathbb{R}$ et en déduire que S est irréductible sur $\mathbb{Q}$.

d) L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est-elle galoisienne ?

e) Montrer que le corps N contient α et β.

f) Montrer que $\mathrm{N} = \mathbb{Q}(\alpha, \beta)$. Suggérer un élément primitif de $\mathrm{N}/\mathbb{Q}$.

Université de Franche-Comté
Master mathématiques et applications
1ère année (CTU)

Examen de l'unité "Corps"
Seconde session - 2018 /2019

Durée 3h

Seul le document "Corps" est autorisé (sans annotation) - Calculatrice interdite

---

Exercice 1

1) Soit $\mathbb{F}_2$ le corps à deux éléments. Déterminer la factorisation du polynôme $P = X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ sur $\mathbb{F}_2$ (c'est à dire, écrire P en produit de polynômes irréductibles sur $\mathbb{F}_2$).

2) En déduire que le polynôme $R = X^4 + X^3 - X^2 + 3 \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$.

Exercice 2.
Soit le corps cyclotomique $\mathrm{K} = \mathbb{Q}(\mu_{75})$.

1) Déterminer $[\mathrm{K} : \mathbb{Q}]$.

2) Déterminer la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

3) Donner les sous-corps cyclotomiques contenus dans K, et tracer leur treillis.

4) Déterminer Φ_{75}.

Exercice 3.
Soit un nombre premier $p > 3$ et soit $\zeta \in \mathbb{C}$ une racine primitive p-ème de l'unité : on a donc $\zeta^p = 1$ et $\zeta \neq 1$.

Soit ℓ un second nombre premier (éventuellement $\ell = p$) et soit le polynôme $P = X^p - \ell \in \mathbb{Q}[X]$.
On pose $\mathrm{K} = \mathbb{Q}(\zeta, \theta)$, où $\theta \in \mathbb{C}$ est une racine de P.

1) Montrer que P est irréductible (sur $\mathbb{Q}$).

2) Montrer que K est le corps des racines de P.

3) Déterminer $[\mathrm{K} : \mathbb{Q}]$.

4) Soit $\mathrm{F} = \mathbb{Q}(\zeta)$. Montrer que K/F est une extension galoisienne cyclique de degré p, de groupe de Galois engendré par $\tau : \theta \mapsto \zeta\theta$.

5) Soient les éléments σ et τ de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ définis par :

$$\sigma \left| \begin{array}{ccc} \zeta & \mapsto & \zeta^a \\ \theta & \mapsto & \theta \end{array} \right. \; ; \; \tau \left| \begin{array}{ccc} \zeta & \mapsto & \zeta \\ \theta & \mapsto & \zeta\theta \end{array} \right.$$

où $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un élément d'ordre $p - 1$.

a) Montrer que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est engendré par σ et τ.

b) Montrer que $\sigma^{-1}\tau\sigma = \tau^{a^{-1}}$, où a^{-1} est l'inverse de a dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

c) En déduire que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$.

Année
2019-2020

Centre de Télé-enseignement Universitaire

UNIVERSITÉ DE FRANCHE-COMTÉ

SESSION 1 D'EXAMEN (mai)

MASTER de MATHÉMATIQUES **VVM7ECOR - CORPS** Durée : 3 heures	**Ce sujet comporte 3 pages** **Documents et/ou matériel autorisés** **Aucun**

Cours de Christian MAIRE

Exercice 1.
Soit $\mathbb{F}_2$ le corps à deux éléments, et soit $P = X^6+X^3+X^2+X+1 \in \mathrm{F}_2[X]$.
Soit $\mathbb{F}_{2^t}$ le corps des racines de P. Déterminer l'entier t.

Exercice 2.
Soit $\zeta = \exp(2i\pi/13) \in \mathbb{C}$ une racine primitive 13-ème de l'unité.
Soit $\mathrm{K} = \mathbb{Q}(\zeta)$.

Pour $\overline{a} \in (\mathbb{Z}/13\mathbb{Z})^\times$, on note σ_a l'élément de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ défini par

$$\sigma_a(\zeta) = \zeta^a.$$

1) Déterminer $[\mathrm{K} : \mathbb{Q}]$ et le polynôme irréductible P de ζ sur $\mathbb{Q}$.

2) Déterminer la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$. Montrer que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est engendré par σ_2.

3) Déterminer tous les sous-groupes de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$. En déduire le treillis des sous-corps de K (on précisera les sous-corps par la suite).

4) Soit $x = \zeta + \zeta^{-1} + \zeta^8 + \zeta^{-8}$.
   a) Vérifier que $\sigma_8(x) = x$.
   b) Montrer que $x \notin \mathbb{Q}$.
   c) En déduire $[\mathbb{Q}(x) : \mathbb{Q}]$.

5) Soit $y = \zeta + \zeta^{-1}$. Déterminer $[\mathbb{Q}(y) : \mathbb{Q}]$.

6) Soit $z = \zeta + \zeta^{-1} + \zeta^3 + \zeta^{-3} + \zeta^4 + \zeta^{-4}$.
   a) Vérifier que $\sigma_4(z) = z$.
   b) Montrer que $z \notin \mathbb{Q}$.
   c) En déduire $[\mathbb{Q}(z) : \mathbb{Q}]$.
   d) Déterminer le polynôme irréductible de z sur $\mathbb{Q}$. En déduire l'expression l'expression de z à partir de $\sqrt{13}$.

7) Soit $w = \zeta + \zeta^3 + \zeta^9$.
   a) Vérifier que $\sigma_3(w) = w$.
   b) Montrer que $w \notin \mathbb{Q}(z)$.

8) Compléter le treillis des sous-corps de K.

Exercice 3.

Soit $a \geq 1$ un entier naturel.

On pose $m = a^2 + 1$ et $n = a^2 + 2$.

Soient les nombres réels $\theta = (m + \sqrt{m})(n + \sqrt{n})$, et $\alpha = \sqrt{\theta}$.

1) Montrer que m et n sont premiers entre eux.

2) Montrer que m et n ne sont pas des carrés d'entiers.

3) Montrer que $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$.

4) Soit $\mathrm{k} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.
   a) Que vaut $[\mathrm{k} : \mathbb{Q}]$? Déterminer une $\mathbb{Q}$-base de k.
   b) Justifier que $\mathrm{k}/\mathbb{Q}$ est galoisienne.
   c) Déterminer les $\mathbb{Q}$-automorphismes de k.

5) Pour chaque $\tau \in \mathrm{Gal}(\mathrm{k}/\mathbb{Q})$, montrer que $\theta\tau(\theta)$ est un carré dans k.

6) Montrer que θ n'est pas un carré dans k.

7) Soit $\mathrm{K} = \mathrm{k}(\alpha)$.
   a) Que vaut $[\mathrm{K} : \mathbb{Q}]$?
   b) Justifier que $\mathrm{K}/\mathbb{Q}$ est galoisienne.
   c) Déterminer les $\mathbb{Q}$-automorphismes de K.

8) Soient les deux $\mathbb{Q}$-automorphismes de K :

$$\sigma \left| \begin{array}{rcl} \sqrt{m} & \mapsto & \sqrt{m} \\ \sqrt{n} & \mapsto & -\sqrt{n} \\ \alpha & \mapsto & \dfrac{\sqrt{mn}(m+\sqrt{m})}{\alpha} \end{array} \right. ; \ \tau \left| \begin{array}{rcl} \sqrt{m} & \mapsto & -\sqrt{m} \\ \sqrt{n} & \mapsto & \sqrt{n} \\ \alpha & \mapsto & \dfrac{a\sqrt{m}(n+\sqrt{n})}{\alpha} \end{array} \right.$$

   a) Déterminer l'ordre de σ et l'ordre de τ.
   b) Montrer que $\sigma \circ \tau \neq \tau \circ \sigma$.
   c) Quel est le groupe $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$?
   d) En déduire le treillis des sous-corps de K.

Année
2019-2020

Centre de Télé-enseignement Universitaire

UNIVERSITÉ DE FRANCHE-COMTÉ

SESSION 2 D'EXAMEN
(août)

MASTER de MATHÉMATIQUES **VVM7ECOR - CORPS** Durée : 3 heures	**Ce sujet comporte 3 pages** **Documents et/ou matériel autorisés** **Aucun**

Cours de Christian MAIRE

Exercice 1. Donner un exemple d'un polynôme irréductible non séparable ; justifier.

Exercice 2.
Soit le polynôme $P = X^6 + X^5 + X^4 + X^3 + 2X^2 + 4X + 1 \in \mathbb{Z}[X]$.

1) Dans $\mathbb{F}_3[X]$, montrer que les polynômes $X^3 - X + 1$ et $X^3 + X^2 - X + 1$ sont irréductibles.

2) Vérifier que l'on a

$$P \equiv (X^3 - X + 1)(X^3 + X^2 - X + 1) \pmod 3.$$

3) Dans $\mathbb{F}_2[X]$, montrer que les polynômes $X^2 + X + 1$ et $X^4 + X + 1$ sont irréductibles.

4) Vérifier que l'on a

$$P \equiv (X^2 + X + 1)(X^4 + X + 1) \pmod 2.$$

5) En déduire que P est un polynôme irréductible (sur $\mathbb{Q}$).

Exercice 3.

Soient $a \neq b$ deux entiers naturels *non nuls*.

On pose $m = a^2 + 1$ et $n = b^2 + 1$.

Soient les nombres réels $\theta = (m + \sqrt{m})(n + \sqrt{n})$, et $\alpha = \sqrt{\theta}$.

1) Donner un exemple de couple (a, b) tel que $(a^2 + 1)(b^2 + 1)$ n'est pas un carré d'entier.
Donner un exemple de couple (a, b) tel que $(a^2 + 1)(b^2 + 1)$ est un carré d'entier.

Pour toute la suite on suppose que a et b sont tels que $(a^2 + 1)(b^2 + 1)$ n'est pas un carré d'entier.

2) Montrer que m et n ne sont pas des carrés d'entiers.

3) Montrer que $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$.

4) Soit $\mathrm{k} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.
   a) Que vaut $[\mathrm{k} : \mathbb{Q}]$? Déterminer une $\mathbb{Q}$-base de k.
   b) Justifier que $\mathrm{k}/\mathbb{Q}$ est galoisienne.
   c) Déterminer les $\mathbb{Q}$-automorphismes de k.

5) Pour chaque $s \in \mathrm{Gal}(\mathrm{k}/\mathbb{Q})$, montrer que $\theta s(\theta)$ est un carré dans k.

6) Montrer que θ n'est pas un carré dans k.

7) Soit $\mathrm{K} = \mathrm{k}(\alpha)$.

a) Que vaut $[\mathrm{K} : \mathbb{Q}]$?

b) Justifier que $\mathrm{K}/\mathbb{Q}$ est galoisienne.

c) Déterminer les $\mathbb{Q}$-automorphismes de K.

8) Soient les trois $\mathbb{Q}$-automorphismes de K :

$$\sigma_1 \left| \begin{array}{rcl} \sqrt{m} & \mapsto & \sqrt{m} \\ \sqrt{n} & \mapsto & -\sqrt{n} \\ \alpha & \mapsto & \dfrac{b\sqrt{n}(m+\sqrt{m})}{\alpha} \end{array} \right. ; \ \sigma_2 \left| \begin{array}{rcl} \sqrt{m} & \mapsto & -\sqrt{m} \\ \sqrt{n} & \mapsto & \sqrt{n} \\ \alpha & \mapsto & \dfrac{a\sqrt{m}(n+\sqrt{n})}{\alpha} \end{array} \right. ;$$

$$\tau \left| \begin{array}{rcl} \sqrt{m} & \mapsto & -\sqrt{m} \\ \sqrt{n} & \mapsto & -\sqrt{n} \\ \alpha & \mapsto & \dfrac{ab\sqrt{mn}}{\alpha} \end{array} \right. .$$

a) Déterminer l'ordre de σ_1, σ_2 et τ.

b) Montrer que $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

c) Pour $i = 1, 2$, montrer que $\sigma_i \circ \tau = \tau \circ \sigma_i$.

9) Quel est le groupe $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$?

10) En déduire le treillis des sous-corps de K.

Année 2020-2021

Centre de Télé-enseignement Universitaire

UNIVERSITÉ DE FRANCHE-COMTÉ

SESSION 1 D'EXAMEN (mai)

MASTER de MATHÉMATIQUES **VVM7ECOR - CORPS** Durée : 3 heures	**Ce sujet comporte 3 pages** **Documents et/ou matériel autorisés** **Aucun**

Cours de Christian MAIRE

Exercice 1.
Soit $\mathbb{F}_2$ le corps à deux éléments, et soit $\overline{\mathbb{F}_2}$ une clôture algébrique de $\mathbb{F}_2$. Soit $\omega \in \overline{\mathbb{F}_2}$ vérifiant $\omega^2 + \omega + 1 = 0$.

1) Déterminer l'entier t tel que $\mathbb{F}_{2^t} = \mathrm{F}_2(\omega)$.

2) Soit $P = X^3 + \omega X^2 + 1 \in \mathbb{F}_{2^t}[X]$. Notons par $\mathbb{F}_{2^s}$ le corps des racines de P sur $\mathbb{F}_{2^t}$. Déterminer l'entier s.

Exercice 2. Soit le polynôme $P(X) = X^5 + 6X^2 + 3X + 3 \in \mathbb{Q}[X]$, et soit K le corps des racines de P sur $\mathbb{Q}$.

1) Montrer que P est irréductible.

2) Soit $\overline{P} = X^5 + X + 1 \in \mathbb{F}_2[X]$. Donner la factorisation de $\overline{P}$ dans $\mathbb{F}_2[X]$.

Indication. On pourra rappeler les polynômes irréductibles de degré 2 *de* $\mathbb{F}_2[X]$.

3) En déduire la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

Exercice 3.
Soit $\zeta = \exp(2i\pi/63) \in \mathbb{C}$ une racine primitive 63-ème de l'unité.
Soit $\mathrm{K} = \mathbb{Q}(\zeta)$.

1) Déterminer $[\mathrm{K} : \mathbb{Q}]$ et le polynôme irréductible P de ζ sur $\mathbb{Q}$.

2) Déterminer la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

3) Donner le treillis des sous-corps cyclotomiques de $\mathrm{K}/\mathbb{Q}$.

4) Déterminer toutess les extensions quadratiques $\mathrm{L}/\mathbb{Q}$ contenues dans $\mathrm{K}/\mathbb{Q}$.

Indication : si $p > 2$ *est un nombre premier alors* $\mathbb{Q}(\exp(2i\pi/p))$ *contient l'élément* $\sqrt{(-1)^{(p-1)/2}p}$.

5) Pour $a \in (\mathbb{Z}/63)^\times$, soit l'élément σ_a de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ défini par $\sigma_a := \zeta \mapsto \zeta^a$.

a) Déterminer l'ordre de σ_{10} et de σ_{29}.

b) Montrer que σ_{10} laisse invariant ζ^7, et que σ_{29} laisse invariant ζ^9.

c) En déduire que $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \langle \sigma_{10}, \sigma_{29} \rangle$.

Exercice 4.
Les extensions considérées sont dans $\mathbb{C}$.

Soit $a, b, c \geq 1$ trois entiers naturels non nuls *avec c impair*, tels que

$$a^2 = 2(b^2 + c^2).$$

1) Donner un exemple d'un tel triplet (a, b, c) quand $c = 1$ et quand $c = 3$.

Soit le polynôme $P = X^4 - 2aX^2 + 2c^2 \ \in \mathbb{Q}[X]$.

2) Montrer que le polynôme P est irréductible.

Posons $\alpha = \sqrt{a + b\sqrt{2}} \in \mathbb{C}$.

Soient $\mathrm{k} = \mathbb{Q}(\sqrt{2})$ et $\mathrm{K} = \mathbb{Q}(\alpha)$.

3) Déterminer $[\mathrm{k} : \mathbb{Q}]$, puis montrer que $\mathrm{k} \subset \mathrm{K}$.

4) Calculer $P(\alpha)$. En déduire $[\mathrm{K} : \mathbb{Q}]$.

5) Soient σ_0 et σ_1 les deux automorphismes de $\mathrm{k}/\mathbb{Q}$ définis par $\sigma_0(\sqrt{2}) = \sqrt{2}$ et $\sigma_1(\sqrt{2}) = -\sqrt{2}$.

a) Déterminer les $\mathbb{Q}$-plongements $\sigma_{i,j}$ de K dans $\mathbb{C}$ prolongeant σ_i (ici $i = 0, 1$, $j = 0, 1$).

b) Calculer le produit $\sigma_{0,0}(\alpha)\sigma_{1,0}(\alpha)$. En déduire que $\mathrm{K}/\mathbb{Q}$ est une extension galoisienne.

c) Déterminer la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

d) Déterminer tous les sous-corps de $\mathrm{K}/\mathbb{Q}$.

Année
2020-2021

Centre de Télé-enseignement Universitaire

UNIVERSITÉ DE FRANCHE-COMTÉ

SESSION 2 D'EXAMEN
(août)

MASTER de MATHÉMATIQUES **VVM7ECOR - CORPS** Durée : 3 heures	**Ce sujet comporte 2 pages** **Documents et/ou matériel autorisés** **Aucun**

Cours de Christian MAIRE

Exercice 1.
Soit $\mathbb{F}_2$ le corps à deux éléments, et soit $P = X^5 + X^3 + X + 1 \in \mathbb{F}_2[X]$.

1) Donner la factorisation de P dans $\mathbb{F}_2[X]$.

2) Soit K le corps des racines de P. Déterminer l'entier t tel que $\mathrm{K} = \mathbb{F}_{2^t}$.

Exercice 2. Soit $\mathbb{F}_5$ le corps à cinq éléments, et soit $P = X^2 + X + 2 \in \mathbb{F}_5[X]$.

1) Montrer que P est irréductible.

2) Est-ce que le polynôme P est primitif ? Justifier.

Exercice 3. Soit le polynôme $P(X) = X^5 + 2X + 6 \in \mathbb{Q}[X]$, et soit K le corps des racines de P sur $\mathbb{Q}$.

1) Montrer que P est irréductible.

2) Donner la factorisation de $\overline{P} = X^5 - X$ dans $\mathbb{F}_3[X]$.

3) En déduire la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

Exercice 4.
Les extensions considérées sont dans $\mathbb{C}$.

Soit ℓ un nombre premier, et soient $a, b, c \geq 1$ trois entiers naturels non nuls *avec ℓ ne divisant pas c*, tels que

$$a^2 = \ell(b^2 + c^2).$$

1) On suppose ℓ impair.
Montrer que si un tel triplet (a, b, c) existe alors $\ell \equiv 1 \pmod 4$.
Donner un exemple d'un tel triplet (a, b, c) pour $\ell = 5$ et $c = 1$; pour $\ell = 5$ et $c = 3$.

Soit le polynôme $P = X^4 - 2aX^2 + \ell c^2 \ \in \mathbb{Q}[X]$.

2) Montrer que le polynôme P est irréductible.

Posons $\alpha = \sqrt{a + b\sqrt{\ell}} \in \mathbb{C}$.

Soient $\mathrm{k} = \mathbb{Q}(\sqrt{\ell})$ et $\mathrm{K} = \mathbb{Q}(\alpha)$.

3) Déterminer $[\mathrm{k} : \mathbb{Q}]$, puis montrer que $\mathrm{k} \subset \mathrm{K}$.

4) Calculer $P(\alpha)$. En déduire $[\mathrm{K} : \mathbb{Q}]$.

5) Soient σ_0 et σ_1 les deux automorphismes de $\mathrm{k}/\mathbb{Q}$ définis par $\sigma_0(\sqrt{\ell}) = \sqrt{\ell}$ et $\sigma_1(\sqrt{\ell}) = -\sqrt{\ell}$.

a) Déterminer les $\mathbb{Q}$-plongements $\sigma_{i,j}$ de K dans $\mathbb{C}$ prolongeant σ_i (ici $i = 0, 1$, $j = 0, 1$).

b) Calculer le produit $\sigma_{0,0}(\alpha)\sigma_{1,0}(\alpha)$. En déduire que $\mathrm{K}/\mathbb{Q}$ est une extension galoisienne.

6) Déterminer la structure de $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

7) Déterminer tous les sous-corps de $\mathrm{K}/\mathbb{Q}$.
