Université Denis Diderot Paris 7, Semestre septembre 2015-janvier 2016

Master 1, cours d'algèbre

(M. Hindry, J-F. Mestre et R. Mneimné)

Un corrigé de l'examen du 13 janvier 2016.

Exercice 1 (Groupes et théorèmes de Sylow) *Soit G un groupe de cardinal $N = 210 = 2 \cdot 3 \cdot 5 \cdot 7$. On se propose de montrer que G est résoluble. On note $\mathcal{S}(G)$ le groupe symétrique de G (isomorphe à $\mathcal{S}_{210}$).*

1.a) L'action de G sur lui-même par translation induit un homomorphisme

$$\rho : G \to \mathcal{S}(G).$$

Calculer la signature de l'image d'un élément d'ordre 2.

1.b) Montrer que G possède un sous-groupe distingué H de cardinal $M = 105 = 3 \cdot 5 \cdot 7$. [Indication : on pourra montrer que $H := \mathrm{Ker}(\epsilon \circ \rho)$ convient, où $\epsilon : \mathcal{S}(G) \to \{\pm 1\}$ désigne l'homomorphisme signature.]

1.c) Soit H un groupe de cardinal $105 = 3 \cdot 5 \cdot 7$. Montrer que H contient un sous-groupe distingué de cardinal 5 ou 7.

1.d) Conclure, en montrant qu'il existe des sous-groupes

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset G_3 \subset G_4 = G$$

tels que $G_{i-1} \lhd G_i$ et $G_i/G_{i-1} \cong \mathbf{Z}/p\mathbf{Z}$ (avec $p = 2, 3, 5$ ou 7).

Solution.

1.a) Une translation (à gauche, par exemple) par un élément g différent de l'élément neutre n'a aucun point fixe donc la permutation correspondante non plus. Décrivons sa décomposition en produit de cycles à supports disjoints de $\rho(g)$, quand g est un élément d'ordre 2; la permutation $\rho(g)$ est donc un produit de m transpositions à support disjoints, avec $2m = |G|$ et donc $m = 105$. Le signe de la permutation est donc $(-1)^{105} = -1$.

1.b) Un groupe de cardinal pair contient un élément d'ordre 2, disons g. Comme $\epsilon \circ \rho(g) = -1$ d'après la question précédente, on voit que $\epsilon \circ \rho : G \to \{+1, -1\}$ est surjectif, donc $G/\operatorname{Ker} \epsilon \circ \rho \cong Im(\epsilon \circ \rho) \cong \mathbf{Z}/2\mathbf{Z}$. On a donc $|\operatorname{Ker} \epsilon \circ \rho| = |G|/2 = 105$. Le groupe $H := \operatorname{Ker} \epsilon \circ \rho$ est de plus distingué car c'est le noyau d'un homomorphisme (on peut aussi déduire cela du fait que le sous-groupe est d'indice 2).

1.c) Soit n_5 (resp. n_7) le nombre de 5-sous-groupes de Sylow de G (resp. le nombre de 7-sous-groupes de Sylow). Les théorèmes de Sylow indiquent que $n_5 \equiv 1 \bmod 5$ et

n_5 divise $3 \cdot 7$, donc $n_5 \in \{1, 21\}$; de même on conclut que $n_7 \in \{1, 15\}$. Si $n_5 = 1$ (resp. $n_7 = 1$), alors il y a un seul 5-sous-groupe de Sylow et il est distingué (resp. il y a un seul 7-sous-groupe de Sylow et il est distingué. Voyons que $n_5 = 21$ et $n_7 = 15$ est impossible. En effet, le nombre d'éléments d'ordre 5 est égal au nombre d'éléments contenu dans un 5-sous-groupe de Sylow et différent du neutre, donc il y a $n_5(5-1) = 4n_5$ éléments d'ordre 5; de même il y a $n_7(7-1) = 6n_5$ éléments d'ordre 7. Si $n_5 = 21$ et $n_7 = 15$, on aurait $4 \cdot 21 + 6 \cdot 15 = 84 + 90 = 174$ éléments d'ordre 5 ou 7 ce qui est absurde. Il y a donc bien un sous-groupe distingué de cardinal 5 ou 7.

1.d) On peut bien sûr procéder de plusieurs façons. Prenons $G_3 = H$ le sous-groupe de cardinal 105 donné par la question 1.b et prenons comme sous-groupe G_1 le sous-groupe distingué dans $H = G_3$ de cardinal $p = 5$ ou 7. Le quotient G_3/G_1 est de cardinal $105/p$ donc égal à 21 ou 15; il contient donc un sous-groupe distingué U de cardinal respectivement 7 ou 5 [Rappel vu en cours et exercices : dans un groupe de cardinal pq, avec $p < q$ premiers, il y a un unique q-sous-groupe de Sylow qui est donc distingué]. Considérons la surjection canonique $\pi : G_3 \to G_3/G_1$ et posons $G_2 = \pi^{-1}(U)$; on a alors $|G_2| = |U| \cdot |G_1| = 35$. On a alors construit une suite

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset G_3 \subset G_4 = G$$

avec $G_{i-1} \lhd G_i$ et $G/G_3 \cong (\mathbf{Z}/2\mathbf{Z})$, $G_3/G_2 \cong (G_3/G_1)/U \cong \mathbf{Z}/3\mathbf{Z}$, et, ou bien $G_1 \cong \mathbf{Z}/5\mathbf{Z}$ et $G_2/G_1 \cong \mathbf{Z}/7\mathbf{Z}$, ou bien $G_1 \cong \mathbf{Z}/7\mathbf{Z}$ et $G_2/G_1 \cong \mathbf{Z}/5\mathbf{Z}$.

[Variante (esquissée). On prend $G_3 = H$ le sous-groupe de cardinal 105 donné par la question 1.b. On considère alors S_5 (resp. S_7) un 5-sous-groupe de Sylow (resp. un 7-sous-groupe de Sylow), l'ensemble $G_2 := S_5 \cdot S_7 := \{xy \mid x \in S_5,\, y \in S_7\}$ est alors un sous-groupe, car S_5 ou S_7 est distingué dans H, de plus l'indice de G_2 dans G_3 est 3, qui est le plus petit facteur premier de $|H|$ donc G_2 est distingué dans G_3. Enfin, les théorèmes de Sylow donnent que S_7 est distingué dans G_2.]

Exercice 2. (Anneaux)

2.a) Lesquels des anneaux suivants sont intègres, factoriels, principaux ?

$$A_1 = \mathbf{Z}[i],\ A_2 = \mathbf{Z}[X, Y],\ A_3 = \mathbf{Q}[X, Y]/(XY).$$

2.b) Montrer que l'anneau $B = \mathbf{Q}[X, Y]/(XY - 1)$ est principal.
[Indication : on pourra montrer qu'il s'identifie à l'anneau des fractions rationnelles dont les éléments non nuls s'écrivent $f(X) = P(X)X^n$, avec $n \in \mathbf{Z}$ et P polynôme tel que $P(0) \neq 0$, et montrer que la fonction $\delta(f) = \deg P$ permet de définir une division euclidienne dans l'anneau B.]

Solution.

2.a) Donnons d'abord les réponses.
- L'anneau $\mathbf{Z}[i]$ est euclidien, donc principal, factoriel et intègre.

- L'anneau $\mathbf{Z}[X,Y]$ est factoriel et intègre, mais n'est pas principal.
- L'anneau $\mathbf{Q}[X,Y]/(XY)$ n'est pas intègre (donc n'est ni factoriel ni principal).
L'existence d'une division euclidienne dans l'anneau $A_1 = \mathbf{Z}[i]$, par rapport à la norme $N(a+bi) = a^2+b^2$ a été vue en cours; cela entraîne que A_1 est principal et donc factoriel. Comme $\mathbf{Z}$ est principal donc factoriel, l'anneau de polynômes en deux variables à coefficients dans $\mathbf{Z}$ est factoriel. Mais A_2 n'est pas principal : l'idéal I engendré par X et Y n'est pas égal à l'anneau entier, alors que les seuls diviseurs communs de X et Y sont les seules unités. Enfin, si l'on note x (resp. y) la classe de X (resp. de Y) dans $A_3 = \mathbf{Q}[X,Y]/(XY-1)$, on a $x \neq 0$ et $y \neq 0$ mais $xy = 0$, et l'anneau A_3 est donc non intègre.

2.b) Soit $\phi : \mathbf{Q}[X,Y] \to \mathbf{Q}(X)$ l'homomorphisme d'anneaux défini par $\phi(X) = X$ et $\phi(Y) = X^{-1}$; visiblement $XY - 1 \in \operatorname{Ker}\phi$ et ϕ induit ainsi un homomorphisme $\tilde{\phi} : \mathbf{Q}[X,Y]/(XY-1) \to \mathbf{Q}(X)$. On vérifie qu'il est injectif : si un polynôme vérifie $P(X,X^{-1}) = 0$, alors le polynôme $P(X,Y)$ contient $Y - X^{-1}$ en facteur dans $\mathbf{Q}(X)[Y]$ et donc $P(X,Y) = (XY-1)Q(X,Y)$. L'image est précisément l'ensemble des fractions rationnelles en X de la forme $Q(X,X^{-1})$, qu'on peut aussi écrire $P(X)/X^m$, avec $P \in \mathbf{Q}[X]$.

[Variante plus "concrète". Écrivons x (resp. y) pour la classe de X (resp. de Y) dans $B = \mathbf{Q}[X,Y]/(XY-1)$; on a alors $xy = 1$ dans B. Si $f = P(x,y) = \sum_{i=0}^{d} P_i(x)y^i$ est un élément de B, on peut faire le calcul suivant. On a $x^d f = \sum_{i=0}^{d} P_i(x)x^{d-i}(xy)^i = \sum_{i=0}^{d} P_i(x)x^{d-i}$, d'où l'écriture annoncée des éléments de B.]

Identifions donc B à l'anneau des fractions rationnelles dont les éléments non nuls s'écrivent $f(X) = P(X)X^n$, avec $n \in \mathbf{Z}$ et P polynôme tel que $P(0) \neq 0$ et définissons δ comme suggéré. Soit alors $f(X) = P(X)X^n$ et $g(X) = Q(X)X^m$ avec $P(0)$ et $Q(0)$ non nuls. On écrit, dans l'anneau $\mathbf{Q}[X]$, la division euclidienne $P = SQ + R$ avec $\deg(R) < \deg(Q)$ (ou $R = 0$) et on en tire

$$f(X) = S(X)Q(X)X^n + R(X)X^n = S(X)X^{n-m}g(X) + R(X)X^n,$$

avec $R(X)X^n = 0$ ou $\delta(R(X)X^n) \leq \deg(R) < \deg(Q) = \delta(g(X))$, ce qui montre l'existence d'une division euclidienne, et donc que B est principal.

Exercice 3. (Modules sur un anneau principal)

3.a) Soit M un A-module, où A est un anneau principal. Si $a \in A$, on définit le sous-module $M[a] := \{m \in M \mid am = 0\}$. On suppose que $\operatorname{pgcd}(a,b) = 1$*; montrer que $M[ab] = M[a] \oplus M[b]$.*
[Indication : penser au théorème de Bézout.]

3.b) On suppose maintenant que $A = K[X]$ et M est un K-espace vectoriel muni d'une structure de $K[X]$-module par un K-endomorphisme u. On suppose que le

polynôme minimal de u s'écrit $P_1 \cdot P_2$ avec des polynômes P_1 et P_2 premiers entre eux. Montrer que l'on peut écrire $M = M_1 \oplus M_2$ comme somme directe de deux sous-espaces vectoriels stables par u, de sorte que, pour $i = 1, 2$, le polynôme minimal de u_{M_i} (l'endomorphisme de M_i induit par u) soit égal à P_i.

Solution.

3.a) On utilise le théorème de Bézout : il existe $u, v \in A$ tels que $au + bv = 1$. Soit d'abord $m \in M[a] \cap M[b]$, alors $m = (au + bv)m = u(a \cdot m) + v(b \cdot m) = 0$. Ainsi on a bien $M[a] \cap M[b] = \{0\}$. Soit ensuite $m \in M[ab]$; on écrit de nouveau $m = u(a \cdot m) + v(b \cdot m) = m_1 + m_2$ et on observe que $b \cdot m_1 = uba \cdot m = 0$ et $a \cdot m_2 = vba \cdot m = 0$, et donc $m_1 \in M[b]$ et $m_2 \in M[a]$ ainsi $M[ab] \subset M[a] + M[b]$. Enfin il est clair que $M[a] \subset M[ab]$ et $M[b] \subset M[ab]$, donc $M[a] + M[b] \subset M[ab]$. On conclut bien que $M[ab] = M[a] \oplus M[b]$.

3.b) En appliquant la question précédente on voit que, en posant $M_1 := M[P_1]$ et $M_2 := M[P_2]$, on a $M = M[P_1P_2] = M[P_1] \oplus M[P_2] = M_1 \oplus M_2$. Rappelons qu'un $K[X]$-sous-module est un K-sous-espace vectoriel stable par u. Le polynôme minimal Q_1 de u_{M_1} divise P_1 et le polynôme minimal Q_2 de u_{M_2} divise P_2; mais Q_1Q_2 annule M donc est divisible par P_1P_2; on conclut que $P_1P_2 = Q_1Q_2$ et donc $P_1 = Q_1$ et $P_2 = Q_2$.

Problème (Extensions de corps et théorie de Galois)

Soit $\zeta := \exp(2\pi i/5)$ et $\alpha = \sqrt[5]{3}$, et $K = \mathbf{Q}(\zeta, \alpha)$.

4.a) Donner le polynôme minimal sur $\mathbf{Q}$ de ζ et α. En déduire la valeur de $[K : \mathbf{Q}(\zeta)]$ puis $[K : \mathbf{Q}(\alpha)]$ et enfin $[K : \mathbf{Q}]$.

4.b) Montrer que $K/\mathbf{Q}$ est une extension galoisienne. On note G son groupe de Galois; quel est son cardinal ?

4.c) On note H_1 le sous-groupe de G correspondant à $K_1 = \mathbf{Q}(\zeta)$ et H_2 celui correspondant à $K_2 = \mathbf{Q}(\alpha)$. Vérifier que H_1 (resp. H_2) est un 5-sous-groupe de Sylow de G (resp. un 2-sous-groupe de Sylow). Montrer de plus que H_1 est l'unique 5-sous-groupe de Sylow de G, alors qu'il y a cinq 2-sous-groupes de Sylow.

4.d) Montrer que, pour $a \in (\mathbf{Z}/5Z)^\times$ il existe $\tau_a \in G$ tel que $\tau_a(\alpha) = \alpha$ et $\tau_a(\zeta) = \zeta^a$. Montrer de même qu'il existe $\sigma \in G$ tel que $\sigma(\alpha) = \zeta\alpha$ et $\sigma(\zeta) = \zeta$.

4.e) Montrer que σ engendre H_1, que $H_2 = \{\tau_a \mid a \in (\mathbf{Z}/5Z)^\times\}$ et que $\tau_a\sigma\tau_a^{-1} = \sigma^a$.

4.f) En déduire que G est isomorphe au groupe de la droite affine sur $\mathbf{F}_5$ (ou encore au produit semi-direct tautologique de $\mathbf{Z}/5\mathbf{Z}$ par $\mathrm{Aut}(\mathbf{Z}/5\mathbf{Z}) = (\mathbf{Z}/5Z)^\times$).

4.g) Montrer que le groupe G possède cinq sous-groupes d'ordre 4, un seul sous-groupe d'ordre 5, un seul sous-groupe d'ordre 10. Combien de sous-groupes d'ordre 2 existe-t-il dans G ?

4.h) Déterminer la liste des sous-extensions $F \subset K$ (on pourra en particulier observer que $\mathbf{Q}(\zeta + \zeta^{-1}) = \mathbf{Q}(\sqrt{5})$).

Solution.

4.a) L'élément ζ est une racine 5-ième primitive de l'unité, son polynôme minimal est le polynôme cyclotomique $\Phi_5 = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$, qui est irréductible de degré $5 - 1 = 4$, d'après le cours. Le polynôme minimal de α est le $\Phi_5 = X^5 - 3$, qui est de degré 5 et irréductible (par exemple, par le critère d'Eisenstein appliqué avec $p = 3$, puisque 3 divise tous les coefficients sauf le coefficient dominant et, de plus, $9 = 3^2$ ne divise pas le coefficient constant). On a donc $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$ et $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 5$. Le polynôme minimal de ζ sur $\mathbf{Q}(\alpha)$ divise Φ_5, donc est de degré ≤ 4 et donc $\mathbf{Q}(\zeta, \alpha) : \mathbf{Q}(\alpha)] \leq 4$; de même on trouve que $[\mathbf{Q}(\zeta, \alpha) : \mathbf{Q}(\zeta)] \leq 5$. On écrit $[K : \mathbf{Q}] = [K : \mathbf{Q}(\zeta)][\mathbf{Q}(\zeta) : \mathbf{Q}] = [K : \mathbf{Q}(\zeta)]4 \leq 20$ et $[K : \mathbf{Q}] = [K : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = [K : \mathbf{Q}(\alpha)]5 \leq 20$. Comme 4 et 5 sont premiers entre eux on trouve que $[K : \mathbf{Q}]$ est divisible par 20 et inférieur à 20 donc égal à 20. On a donc

$$[K : \mathbf{Q}] = 20, \quad [K : \mathbf{Q}(\zeta)] = 5 \quad \text{et} \quad [K : \mathbf{Q}(\alpha)] = 4.$$

4.b) Les racines de $X^5 - 3$ sont les $\zeta^i \alpha$, pour $0 \leq i \leq 4$, mais on a $\mathbf{Q}(\alpha, \zeta\alpha, \ldots, \zeta^4\alpha) = \mathbf{Q}(\zeta, \alpha) = K$. L'extension K est ainsi le corps de décomposition de $X^5 - 3$ donc est une extension normale, et donc galoisienne, puisque la caractéristique est nulle et toute extension est automatiquement séparable. On a de plus $|G| = [K : \mathbf{Q}] = 20$.

4.c) On a $|H_1| = [K : \mathbf{Q}(\zeta)] = 5$ et $|H_2| = [K : \mathbf{Q}(\alpha)] = 4$. Le cardinal de G est $= 2^2 \cdot 5$, donc H_1 est un 5-sous-groupe de Sylow et H_2 est un 2-sous-groupe de Sylow de G. Comme $\mathbf{Q}(\zeta)/\mathbf{Q}$ est galoisienne, on sait que H_1 est distingué et est donc l'unique 5-sous-groupe de Sylow [On peut aussi déduire cela des théorèmes de Sylow, qui impliquent qu'un groupe de cardinal 20 possède un unique 5-sous-groupe de Sylow]. Comme $\mathbf{Q}(\alpha)/\mathbf{Q}$ n'est pas galoisienne, on sait que H_2 n'est pas distingué. Si n_2 désigne le nombre de 2-sous-groupes de Sylow de G, on a n_2 impair et divise 5; comme $n_2 \neq 1$, on conclut que $n_2 = 5$.

4.d) Soit $\rho \in G$ on sait que $\rho(\alpha)$ est une racine de $X^5 - 3$ donc $\rho(\alpha) \in \{\zeta^i \alpha \mid 0 \leq i \leq 4\}$; de même $\rho(\zeta)$ est une racine de Φ_5 donc $\rho(\alpha) \in \{\zeta^a \alpha \mid 1 \leq a \leq 4\}$. Comme il y a *a priori* vingt possibilités et qu'il y a vingt éléments dans G, on voit que toutes les possibilités sont réalisées, i.e. pour chaque $0 \leq i \leq 4$ et $1 \leq a \leq 4$, il existe $\rho \in G$ tel que $\rho(\alpha) = \zeta^i \alpha$ et $\rho(\zeta) = \zeta^a$. En particulier, il existe donc des éléments σ et τ_a comme annoncé.

[On pouvait aussi raisonner sur les cinq éléments de H_1 qui vérifient $\rho(\zeta) = \zeta$ et $\rho(\alpha)$ est une racine de $X^5 - 3$, et respectivement raisonner sur les quatre éléments de H_2 qui vérifient $\rho(\alpha) = \alpha$ et $\rho(\zeta)$ est une racine de Φ_5.]

4.e) L'élément σ vérifie $\sigma^i(\zeta) = \zeta$ et $\sigma^i(\alpha) = \zeta^i \alpha$ donc est d'ordre 5 et engendre donc l'unique 5-sous-groupe de Sylow, c'est-à-dire H_1. Les éléments τ_a fixent α et appartiennent donc à H_2; comme ils sont 4, ils décrivent tout H_2.

Enfin on vérifie que $\tau_a\sigma\tau_a^{-1}(\alpha) = \zeta^a\alpha$ et $\tau_a\sigma\tau_a^{-1}(\zeta) = \zeta$ alors que $\sigma^a(\alpha) = \zeta^a\alpha$ et $\sigma^a = \zeta$ donc on a bien $\tau_a\sigma\tau_a^{-1} = \sigma^a$.

4.f) On a $H_1 \cap H_2 = \{1\}$, $|H_1| \cdot |H_2| = |G|$ et $H_1 \triangleleft G$, donc on sait que G s'écrit comme produit *semi-direct* $G \cong H_1 \rtimes_\phi H_2$ où l'homomorphisme $\phi : H_2 \to \mathrm{Aut}(H_1)$ est donné par $\phi(\tau)(\sigma) = \tau\sigma\tau^{-1}$.
Si l'on identifie $(\mathbf{Z}/5\mathbf{Z})^\times$ avec H_2 par $a \mapsto \tau_a$ et H_1 avec $\mathbf{Z}/5\mathbf{Z}$ par $\sigma^i \mapsto i$, comme on a vu à la question 4.e) que $\tau_a\sigma\tau_a^{-1} = \sigma^a$, on constate que l'action de H_2 sur H_1 s'identifie à l'action "tautologique" de $(\mathbf{Z}/5\mathbf{Z})^\times = \mathrm{Aut}(\mathbf{Z}/5\mathbf{Z})$ sur $\mathbf{Z}/5\mathbf{Z}$. Mais, $\mathbf{Z}/5\mathbf{Z}$ est aussi la droite affine sur $\mathbf{F}_5$ et donc G s'identifie également au groupe affine de cette droite.

4.g) D'après le théorème de Lagrange, les possibilités pour le cardinal d'un sous-groupe de G sont $1, 2, 4, 5, 10, 20$. Nous avons déjà vu que G contient un unique sous-groupe de cardinal 5 et cinq sous-groupes de cardinal 4. Les sous-groupes de cardinal 4 sont cycliques (isomorphes à $(\mathbf{Z}/5\mathbf{Z})^\times \cong \mathbf{Z}/4\mathbf{Z}$) et contiennent chacun un unique élément d'ordre deux. Il y a donc au plus cinq éléments d'ordre 2. Soit M_1 le sous-groupe de cardinal 2 engendré par $\tau = \tau_{-1}$, le sous-ensemble $J = H_1 \cdot M_1$ a pour cardinal 10 et est un sous-groupe, car $H_1 \triangleleft G$. De plus la relation $\tau \circ \sigma \circ \tau^{-1} = \sigma^{-1}$ montre que J est isomorphe au groupe dièdral D_5 et contient donc cinq éléments d'ordre 2. Il y a donc cinq éléments d'ordre 2 et cinq sous-groupes d'ordre 2. Enfin si L' est un sous-groupe d'ordre 10, il contient H_1 et est engendré par H_1 et un élément d'ordre deux, donc est contenu dans L et donc égal à L.
En résumé, outre les sous-groupes triviaux G et $\{1\}$, il y a cinq sous-groupes de cardinal 2, cinq sous-groupes de cardinal 4, un unique sous-groupe de cardinal 5 et un unique sous-groupe de cardinal 10.

4.h) La correspondance de Galois nous permet de dresser la liste des sous-extensions $\mathbf{Q} \subset F \subset K$ par $F = K^U$ où U parcourt la liste des sous-groupes de la question précédente. De plus si $F = K^U$, on a $[K : F] = |U|$ et $[F : \mathbf{Q}] = |G|/|U|$. Nous savons déjà que le sous-groupe H_1 correspond à l'extension $\mathbf{Q}(\zeta) = K^{H_1}$ et que le sous-groupe H_2 correspond à l'extension $\mathbf{Q}(\alpha)$.
Il y a quatre autres extensions "évidentes" de degré 5 sur $\mathbf{Q}$: les extensions $\mathbf{Q}(\zeta^i\alpha)$; elles correspondent donc aux quatre 2-sous-groupes de Sylow distincts de H_2. [Noter que, si $i \not\equiv j \bmod 5$ alors $\mathbf{Q}(\zeta^i\alpha) \neq \mathbf{Q}(\zeta^j\alpha)$, car sinon ce corps contiendrait ζ^{i-j} et donc ζ et α et donc serait égal à K, ce qui est absurde.]
Le sous-groupe L correspond à la sous-extension qui est fixée par τ_{-1}. Montrons qu'elle engendrée par $\beta := \zeta + \zeta^{-1} = 2\cos(2\pi/5)$, ou encore par $\sqrt{5}$, puisque l'on a $\cos(2\pi/5) = \frac{-1+\sqrt{5}}{2}$. En effet $\beta \in K^L$ et $[\mathbf{Q}(\beta) : \mathbf{Q}] = 2 = [K^L : \mathbf{Q}]$ donc $\mathbf{Q}(\beta) = K^L$.
Les extensions $\mathbf{Q}(\zeta^i\alpha, \sqrt{5})$ sont toutes distinctes de degré 10 sur $\mathbf{Q}$ donc correspondent aux sous-groupes de cardinal 2.

On peut récapituler la liste des sous-extensions avec les inclusions dans le diagramme sur la page suivante.

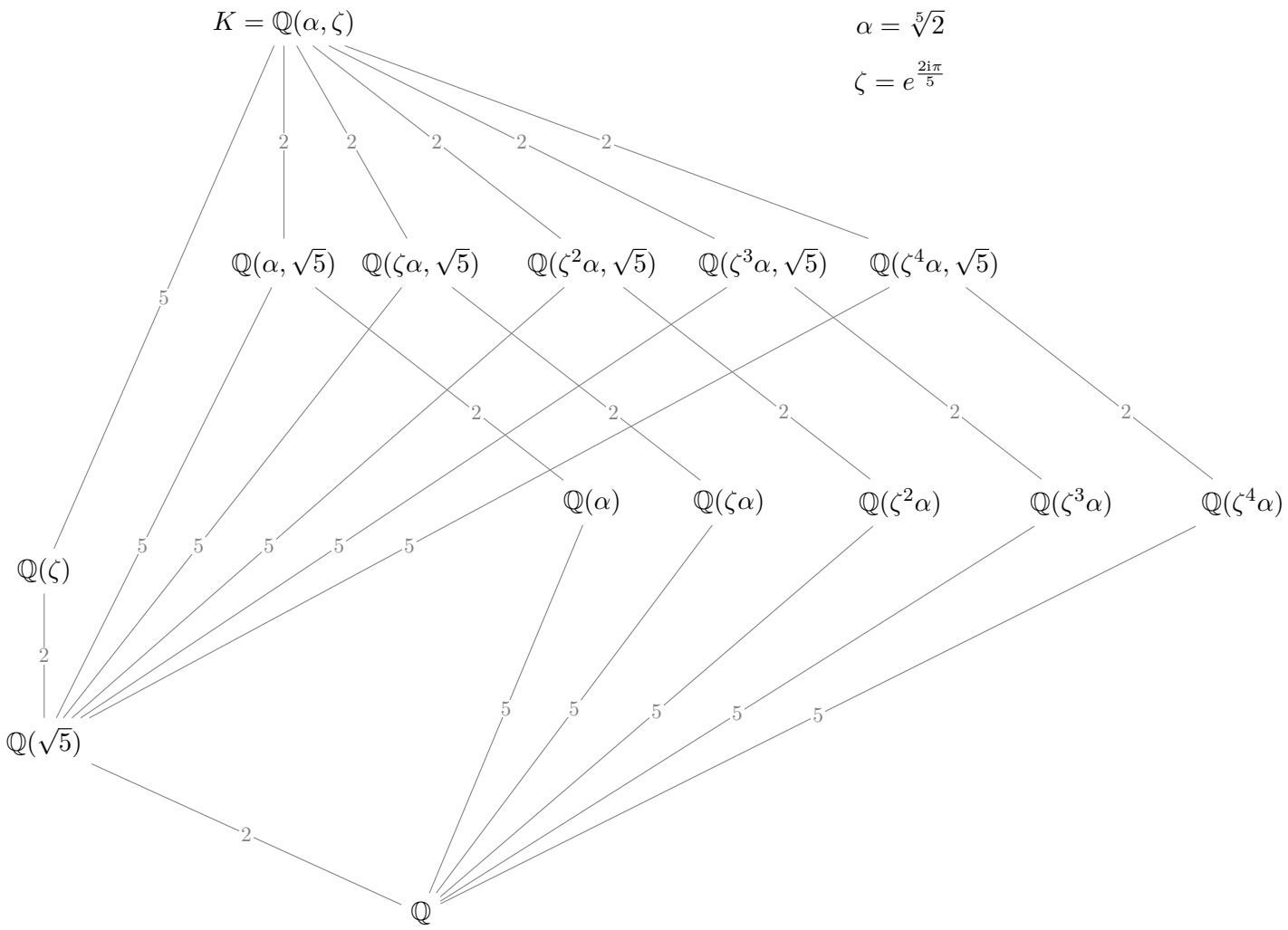

FIGURE 1 – Le corps de décomposition de $X^5 - 2$ sur $\mathbb{Q}$ et ses sous-corps