Entrega 2

Arnau Mas

9 de gener de 2019

Problema 1

Sigui F el cos $\mathbb{Q}(\sqrt[4]{2}, i)$. Hem de veure que F és una extensió de Galois de $\mathbb{Q}$. F és una extensió separable perquè $\mathbb{Q}$ té característica 0 i F és una extensió algebraica —tant i com $\sqrt[4]{2}$ són algebraics sobre $\mathbb{Q}$. Només hem de veure, doncs, que F és una extensió normal. I com que es tracta d'una extensió finita, és equivalent a comprovar que és el cos de descomposició d'algun polinomi. Considerem el polinomi $x^4 - 2$. Les seves arrels a $\mathbb{C}$ són $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ i $-i\sqrt[4]{2}$, per tant el seu cos de descomposició sobre $\mathbb{Q}$ és

$$\mathbb{Q}(x^2 - 4) = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}).$$

I de fet $\mathbb{Q}(x^2 - 4) = F$. D'una banda, és car que F conté $\mathbb{Q}(x^2 - 4)$, i com que

$$i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}}$$

F està contingut dins de $\mathbb{Q}(x^2 - 4)$. Per tant F és un cos de descomposició sobre $\mathbb{Q}$ i per tant n'és una extensió normal.

— ∗ —

Com que F és una extensió de Galois tenim la igualtat

$$|\mathrm{Gal}_{\mathbb{Q}} F| = [F : \mathbb{Q}].$$

Per a calcular el grau $[F : \mathbb{Q}]$ observem que F no pot ser igual a $\mathbb{Q}(\sqrt[4]{2})$ donat que $\mathbb{Q}(\sqrt[4]{2})$ està contingut dins de $\mathbb{R}$ però F no. Això implica que $[F : \mathbb{Q}(\sqrt[4]{2}] = 2$. Efectivament, l'irreductible de i a qualsevol extensió de $\mathbb{Q}$ ha de dividir $x^2 + 1$. I si

fos de grau 1 sobre $\mathbb{Q}(\sqrt[4]{2})$ voldria dir que $i \in \mathbb{Q}(\sqrt[4]{2})$, que no és el cas. Pel lema de les torres, i fent servir que l'irreductible de $\sqrt[4]{2}$ sobre $\mathbb{Q}$ és $x^4 - 2$ es té

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

Això és suficient per a concloure que $\mathrm{Gal}_{\mathbb{Q}} F$ és isomorf al grup dihedral del quadrat, $D_{2\times 4}$, ja que és l'únic subgrup d'ordre 8 de $\mathfrak{S}_4$, i $\mathrm{Gal}_{\mathbb{Q}} F$ és isomorf a un subgrup de $\mathfrak{S}_4$.

— ∗ —

Per a trobar el reticle de cossos intermitjos de l'extensió $F/\mathbb{Q}$ fem servir la correspondència de Galois. Abans, però, determinem l'estructura de $\mathrm{Gal}_{\mathbb{Q}} F$ amb una mica més de detall. Com que F és el cos de descomposició de $x^2 - 4$, tenim que $\mathrm{Gal}_{\mathbb{Q}} F = \mathrm{Gal}_{\mathbb{Q}} x^2 - 4$, per tant els elements de $\mathrm{Gal}_{\mathbb{Q}} F$ permuten les arrels de $x^2 - 4$, que són $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$. Denotem-les, en aquest ordre, per $1, 2, 3$ i 4. D'altra banda, un element de $\mathrm{Gal}_{\mathbb{Q}} F$ queda determinat per on envia $\sqrt[4]{2}$ i i. Les opcions per a $\sqrt[4]{2}$ són les quatre arrels del seu irreductible sobre $\mathbb{Q}$, $x^4 - 2$. I les possibilitats per a i són les dues arrels de $x^2 + 1$, i i $-i$. Així, hi ha quatre elements de $\mathrm{Gal}_{\mathbb{Q}} F$ que fixen i i quatre que no. Això correspon al fet de que de les 8 simetries d'un quadrat, és a dir, elements de $D_{2\times 4}$, n'hi ha 4 que no involucren una reflexió i 4 que si.

Els quatre automorfismes que fixen i són les quatre potències del morfisme que envia $\sqrt[4]{2}$ a $i\sqrt[4]{2}$, és a dir, de la permutació $(1\,2\,3\,4)$. Els quatre morfismes restants són la composició d'un d'aquests pel morfisme conjugació, és a dir, el que envia i a $-i$, i que per tant queda representat per a $(2\,4)$. Els elements de $D_{2\times 4}$ són, doncs

Rotacions	Reflexions
id	(2 4)
(1 2 3 4)	(1 2)(3 4)
(1 3)(2 4)	(1 3)
(1 4 3 2)	(1 4)(2 3)

Anem a determinar el reticle de subgrups de $D_{2\times 4}$. El únics ordres possibles per a subgrups no trivials de $D_{2\times 4}$ són 2 i 4. Els subgrups d'ordre 2 estan generats per elements d'ordre 2. Els elements d'ordre 2 de $D_{2\times 4}$ són tots tret dels dos 4-cicles i la identitat, per tant hi ha 5 subgrups d'ordre 2. Els dos 4-cicles generen el

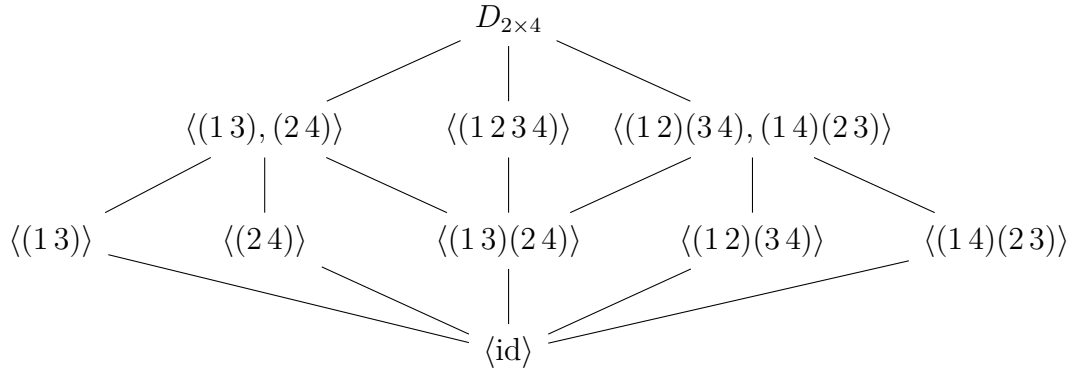
mateix subgrup d'ordre 4, que és isomorf a $\mathbb{Z}/4\mathbb{Z}$. Dos elements d'ordre 2 diferents poden generar un subgrup d'ordre 4 isomorf al grup de Klein V_4 —equivalentment $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$—. A priori tenim $\binom{5}{2} = 10$ possibilitats. Tenim el subgrup

$$\langle (1\,3)(2\,4) \rangle = \langle (1\,3), (1\,3)(2\,4) \rangle = \langle (2\,4), (1\,3)(2\,4) \rangle = \{\mathrm{id}, (1\,3), (2\,4), (1\,3)(2\,4)\}.$$

Un altre subgrup és

$$\begin{aligned}\langle (1\,2)(3\,4), (1\,4)(2\,3) \rangle &= \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle = \langle (1\,4)(2\,3), (1\,3)(2\,4) \rangle \\ &= \{\mathrm{id}, (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(2\,4)\}.\end{aligned}$$

AMb tot això hem exhaurit 6 possibilitats. Les altres 4 generen tot el grup. Efectivament, com que $(1\,3)(1\,2)(3\,4) = (1\,2\,3\,4)$, el subgrup $\langle (1\,3), (1\,2)(3\,4) \rangle$ té ordre superior a 4, i per tant és el total. Conjugant per les potències de $(1\,2\,3\,4)$ arribem a la conclusió de que passa el mateix per a les altres tres possibilitats. El reticle de subgrups és



Un cop coneixem l'estructura de $\mathrm{Gal}_{\mathbb{Q}} F \cong D_{2\times 4}$ podem determinar el reticles de cossos intermitjos de $F/\mathbb{Q}$, fent servir la correspondència de Galois, $H \mapsto F^H$ per a $H \leq \mathrm{Gal}_{\mathbb{Q}} F$. Com que l'extensió és de Galois, la correspondència és bijectiva. En particular es dedueix que hi ha tres cossos intermitjos de grau 2 sobre $\mathbb{Q}$ i cinc cossos intermitjos de grau 4 sobre $\mathbb{Q}$, fent servir que $[F^H : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}} F| \,/\, |H|$.

Comencem pel subgrup $H_1 = \langle (1\,3), (2\,4) \rangle$. Com que H_1 té ordre 4 F^{H_1} ha de tenir ordre 2 sobre $\mathbb{Q}$. Recordem que $(2\,4)$ representa el morfisme conjugació, pel que tots els elements de F^{H_1} han de ser reals. A més

$$(1\,3)(\sqrt{2}) = \left((1\,3)(\sqrt[4]{2})\right)^2 = (-\sqrt[4]{2})^2 = \sqrt{2}$$

per tant $\mathbb{Q}(\sqrt{2}) \subseteq F_1^H$. Però de fet es té igualtat perquè $\mathbb{Q}(\sqrt{2})$ té grau 2 sobre $\mathbb{Q}$.

Considerem el subgrup $H_2 = \langle (1\,2\,3\,4) \rangle$. Com abans, té ordre 2 per tant el corresponent cos F^{H_2} ha de tenir ordre 2 sobre $\mathbb{Q}$. Recordem que $(1\,2\,3\,4)$ permuta

les arrels de x^4-2 cíclicament però fixa i, per tant $\mathbb{Q}(i)\subseteq F^{H_2}$, però de fet es té igualtat perquè $\mathbb{Q}(i)$ té grau 2 sobre $\mathbb{Q}$.

L'últim dels subgrups d'ordre 4 és $H_3=\langle(1\,2)(3\,4),(1\,4)(2\,3)\rangle$. Tenim

$$(1\,2)(3\,4)(i\sqrt{2})=\left((1\,2)(3\,4)(\sqrt[4]{2})\right)\left((1\,2)(3\,4)(i\sqrt[4]{2})\right)=(i\sqrt[4]{2})(\sqrt[4]{2})=i\sqrt{2}$$
$$(1\,4)(2\,3)(i\sqrt{2})=\left((1\,4)(2\,3)(\sqrt[4]{2})\right)\left((1\,4)(2\,3)(i\sqrt[4]{2})\right)=(-i\sqrt[4]{2})(-\sqrt[4]{2})=i\sqrt{2}$$

per tant $\mathbb{Q}(i\sqrt{2})=F^{H_3}$ perquè $\mathbb{Q}(i\sqrt{2})$ té grau 2 sobre $\mathbb{Q}$.

Fem el mateix per als cincs subgrups d'ordre 2, que donen lloc a extensions de grau 4. Ràpidament, com que $(1\,3)(i\sqrt[4]{2})=i\sqrt[4]{2}$ i $(2\,4)(\sqrt[4]{2})=\sqrt[4]{2}$ concloem

$$F^{\langle(1\,3)\rangle}=\mathbb{Q}(i\sqrt[4]{2})\text{ i }F^{\langle(2\,4)\rangle}=\mathbb{Q}(\sqrt[4]{2})$$

perquè tant $\sqrt[4]{2}$ com $i\sqrt[4]{2}$ tenen grau sobre $\mathbb{Q}$, perquè són arrels de x^4-2.

Considerem ara el subgrup $\langle(1\,3)(2\,4)\rangle$. Ja hem vist que $\sqrt{2}$ és fix tant per $(1\,3)$ com per $(2\,4)$, per tant també ho és per la seva composició. També ho és i:

$$(1\,3)(2\,4)(i)=\frac{(1\,3)(2\,4)(i\sqrt[4]{2})}{(1\,3)(2\,4)(\sqrt[4]{2})}=\frac{-i\sqrt[4]{2}}{-\sqrt[4]{2}}=i.$$

Aleshores, com que $\mathbb{Q}(i,\sqrt{2})$ té grau 2 sobre $\mathbb{Q}$, és $F^{\langle(1\,3)(2\,4)\rangle}$. Mirem de trobar un element primitiu d'aquesta extensió. Considerem $\gamma=i+\sqrt{2}$. Aleshores $\gamma^3=7i+\sqrt{2}$, per tant

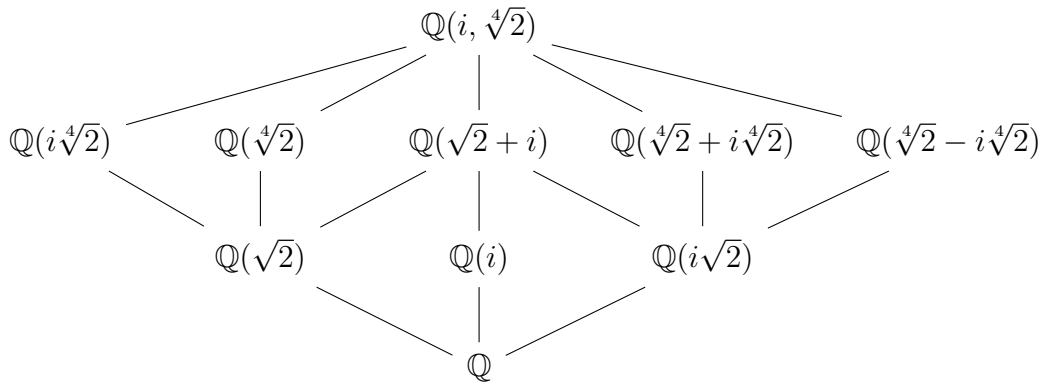
$$i=\frac{\gamma^3-\gamma}{6}$$

és a dir, $i\in\mathbb{Q}(\gamma)$, i per tant $\sqrt{2}=\gamma-i\in\mathbb{Q}(\gamma)$. Això ens dona $\mathbb{Q}(\gamma)=\mathbb{Q}(i,\sqrt{2})$.

Queden dos extensions de grau 4. Per a la que correspon a $\langle(1\,2)(3\,4)\rangle$, com que $(1\,2)(3\,4)$ intercanvia $\sqrt[4]{2}$ amb $i\sqrt[4]{2}$, $\beta=\sqrt[4]{2}+i\sqrt[4]{2}$ és fix per la seva acció, per tant $\mathbb{Q}(\beta)\subseteq F^{\langle(1\,2)(3\,4)\rangle}$. Tenim que $\beta^2=2(i\sqrt{2})$, per tant $\mathbb{Q}(i\sqrt{2})\subseteq\mathbb{Q}(\beta)$. Però la inclusió és estricta perquè β no és fix per $(1\,4)(2\,3)$, a diferència de tots els elements de $\mathbb{Q}(i\sqrt{2})$. Per tant $\mathbb{Q}(\beta)$ té grau almenys 4 sobre $\mathbb{Q}$. I de fet exactament 4 perquè $\beta^4=-8$.

Per un argument molt similar, $\mathbb{Q}(\alpha)=F^{\langle(1\,4)(2\,3)\rangle}$ amb $\alpha=\sqrt[4]{2}-i\sqrt[4]{2}$. Així

doncs, el reticle de cossos intermitjos queda



Problema 2

El conjunt d'automorfismes d'un grup G, $\mathrm{Aut}(G)$ és un grup amb la composició. Tenim que la composició d'automorfismes és automorfisme: en efecte, la composició de morfismes és morfisme, i si $\phi, \psi \in \mathrm{Aut}(G)$ aleshores

$$(\phi \circ \psi)^{-1} = \psi^{-1} \circ \phi^{-1}$$

per tant $\phi \circ \psi$ és un automorfisme i no només un morfisme. A més la composició d'aplicacions és sempre associativa. El morfisme identitat fa el paper d'element neutre. També hi ha inversos perquè la inversa d'un automorfisme també és un morfisme. Així doncs $(\mathrm{Aut}(G), \circ)$ és un grup.

— * —

Considerem una acció d'un grup H sobre un grup G, $\phi\colon H \to \mathrm{Aut}(G)$. Es defineix el producte semidirecte $G \rtimes_\phi H$ o simplement $G \rtimes H$ com $G \times H$ amb l'operació

$$(g_1, h_1)(g_2, h_2) = (g_1\phi(h_1)(g_2), h_1h_2).$$

Aquesta operació dóna a $G \rtimes H$ estructura de grup. Efectivament, és clar que defineix una operació a $G \rtimes H$, és a dir, $(g_1, h_1)(g_2, h_2) \in G \rtimes H$. L'element neutre és (e_G, e_H):

$$(g, h)(e_G, e_H) = (g\phi(h)(e_G), he_H) = (ge_G, h) = (g, h)$$
$$(e_G, e_H)(g, h) = (e_G\phi(e_H)(g), e_Hh) = (\mathrm{id}_G(g), h) = (g, h).$$

L'invers de (g,h) és $(\phi(h^{-1})(g^{-1}),h^{-1})$:

$$(g,h)(\phi(h^{-1})(g^{-1}),h^{-1}) = \Big(g\left(\phi(h)\circ\phi(h^{-1})\right)(g^{-1}),hh^{-1}\Big) = (gg^{-1},e_H) = (e_G,e_H)$$

$$\begin{aligned}(\phi(h^{-1})(g^{-1}),h^{-1})(g,h) &= (\phi(h^{-1})(g^{-1})\phi(h^{-1})(g),h^{-1}h)\\ &= \Big(\big(\phi(h^{-1})(g)\big)^{-1}\phi(h^{-1})(g),e_H\Big) = (e_G,e_H).\end{aligned}$$

Per últim cal comprovar l'associativitat:

$$\begin{aligned}(g_1,h_1)\Big((g_2,h_2)(g_3,h_3)\Big) &= (g_1,h_1)\Big(g_2\phi(h_2)(g_3),h_2h_3)\Big)\\ &= \Big(g_1\phi(h_1)\Big(g_2\phi(h_2)(g_3)\Big),h_1(h_2h_3)\Big)\\ &= \Big(g_1\phi(h_1)(g_2)\Big(\phi(h_1h_2)(g_3)\Big),(h_1h_2)h_3\Big)\\ &= \Big(g_1\phi(h_1)(g_2),h_1h_2\Big)(g_3,h_3)\\ &= \Big((g_1,h_1)(g_2,h_2)\Big)(g_3,h_3).\end{aligned}$$

Observem que amb l'acció trivial $e\colon H\to \mathrm{Aut}(G)$ on $e(h)=\mathrm{id}_G$ per tot $g\in G$ recuperem el producte directe de grups estàndard.

— ∗ —

Considerem un producte directe $G = G_1 \rtimes G_2$. Considerem el subconjunt

$$K = \{(g,h)\in G \mid g = e_{G_1}\}.$$

K és un subgrup. Si (e_{G_1},h_1) i (e_{G_1},h_2) són a K aleshores

$$\begin{aligned}(e_{G_1},h_1)(e_{G_1},h_2)^{-1} &= (e_{G_1},h_1)(\phi(h_2^{-1})(e_{G_1}),h_2^{-1})\\ &= (e_{G_1},h_1)(e_{G_1},h_2^{-1}) = (e_{G_1}\phi(h_1)(e_{G_1}),h_1h_2^{-1})\\ &= (e_{G_1},h_1h_2^{-1})\in K.\end{aligned}$$

Similarment tenim el subgrup $H=\{(g,h)\in G\mid h=e_{G_2}\}$. Si (g_1,e_{G_2}) i (g_2,e_{G_2}) són a H aleshores

$$\begin{aligned}(g_1,e_{G_2})(g_2,e_{G_2})^{-1} &= (g_1,e_{G_2})(\phi(e_{G_2})(g_2^{-1}),e_{G_2})\\ &= (g_1,e_{G_2})(g_2^{-1},e_{G_2}) = (g_1\phi(e_{G_2})(g_2^{-1}),e_{G_2})\\ &= (g_1g_2^{-1},e_{G_2})\in H.\end{aligned}$$

A més H és normal a G: per tot $(x,y)\in G$ i $g\in G_1$ aleshores

$$\begin{aligned}(x,y)(g,e_{G_2})(x,y)^{-1} &= (x\phi(y)(g),y)\left(\phi(y^{-1})(x^{-1}),y^{-1}\right)\\ &= \left(x\phi(y)(g)\left(\phi(y)\circ\phi(y^{-1})(x^{-1})\right),yy^{-1}\right)\\ &= (x\phi(y)(g)x^{-1},e_{G_2})\in H.\end{aligned}$$

És clar que $H \cap K = \langle (e_1, e_2) \rangle$ i que $H \cong G_1$ i $K \cong G_2$ mitjançant les projeccions sobre el primer factor i el segon, respectivament. I per tot $(g, h) \in G$ es té

$$(g, e_{G_2})(e_{G_1}, h) = (g\phi(e_{G_2})(e_{G_1}), e_{G_2}h) = (g, h),$$

és a dir, $HK = G$.

A continuació veiem el recíproc del que acabem de provar: si un grup G té dos subgrups H i K tals que $HK = G$, $H \cap K = \langle e \rangle$ i H és normal a G aleshores G és isomorf a $H \rtimes K$.

En general, la conjugació per un element fix $y \in G$ és un automorfisme. Efectivament, si la denotem per ϕ_y es té

$$\phi_y(x_1x_2) = yx_1x_2y^{-1} = yx_1y^{-1}yx_2y^{-1} = \phi_y(x_1)\phi_y(x_2),$$

i la conjugació per y^{-1} n'és l'invers. Com que H és normal a G, $\phi_y(h) \in H$ si $h \in H$, per qualsevol $y \in G$. Així, ϕ_y es pot restringir a un automorfisme d'H. Això ens permet definir una acció de K sobre H mitjançant $k \mapsto \phi_k$. Això funciona perquè

$$(k_1k_2)h(k_1k_2)^{-1} = k_1(k_2hk_2^{-1})k_1^{-1},$$

és a dir, $\phi_{k_1k_2} = \phi_{k_1} \circ \phi_{k_2}$. Tenim, doncs, el producte semidirecte $H \rtimes K$ mitjançant aquesta acció.

Definim $\Phi \colon H \rtimes K \to G$ com $\Phi(h, k) = hk$. A continuació veiem que Φ és un isomorfisme. Tenim

$$\begin{aligned}\Phi\Big((h_1, k_1)(h_2, k_2)\Big) &= \Phi(h_1\phi_{k_1}(h_2), k_1k_2) \\ &= \Phi(h_1k_1h_2k_1^{-1}, k_1k_2) \\ &= h_1k_1h_2k_2 = \Phi(h_1, k_1)\Phi(h_2, k_2).\end{aligned}$$

Que Φ és exhaustiva és perquè $HK = G$. I que és injectiva és conseqüència de que $H \cap K = \langle e \rangle$. En efecte, si $(h, k) \in \ker \Phi$ aleshores $hk = e$, per tant $h = k^{-1} \in H \cap K$, és a dir $h = k = e$. Així Φ té nucli trivial i per tant és injectiva. Tenim que Φ és un morfisme bijectiu, és a dir un isomorfisme.

Problema 3

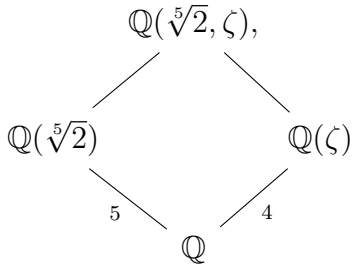
Considerem el polinomi $p(x) = x^5 - 2 \in \mathbb{Q}[x]$. Hem de veure que el seu cos de descomposició sobre $\mathbb{Q}$ és $F = \mathbb{Q}(\sqrt[5]{2}, \zeta)$ on $\zeta = e^{\frac{2\pi i}{5}}$. És clar que $\zeta^k \sqrt[5]{2}$ amb

$0 \leq k \leq 4$ són cinc arrels de $p(x)$ diferents a $\mathbb{C}$. Pel Teorema Fonamental de l'Àlgebra, de fet són totes les arrels. Per tant el cos de descomposició de $p(x)$ és

$$\mathbb{Q}(\sqrt[5]{2}, \zeta\sqrt[5]{2}, \zeta^2\sqrt[5]{2}, \zeta^3\sqrt[5]{2}, \zeta^4\sqrt[5]{2}).$$

Certament aquest cos està contingut a F, i també el conté perquè $\zeta = \frac{\zeta\sqrt[5]{2}}{\sqrt[5]{2}}$. Per tant són iguals.

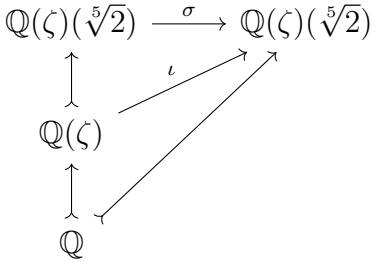
L'extensió $\mathbb{Q}(\sqrt[5]{2})$ és de grau 5 sobre $\mathbb{Q}$ perquè $\sqrt[5]{2}$ és arrel de $x^5 - 2$, que és irreductible per Eisenstein. D'altra banda, $\mathbb{Q}(\zeta)$ és una extensió de grau 4 sobre $\mathbb{Q}$ perquè ζ és arrel de $x^4 + x^3 + x^2 + x + 1$, que és irreductible perquè és un polinomi ciclotòmic. Tenim el següent diagrama d'inclusions



ζ continua sent arrel de $x^4 + x^3 + x^2 + x + 1$ a F, així com $\sqrt[2]{4}$ ho és de $x^5 - 2$, el que vol dir que $[F : \mathbb{Q}(\sqrt[5]{2})]$ no pot ser més gran que 4 i $[F : \mathbb{Q}(\zeta)]$ no pot ser més gran que 5. Això, combinat amb el lema de les torres i amb el fet que 4 i 5 són coprimers ens permet concloure que $[F : \mathbb{Q}] = 4 \times 5 = 20$.

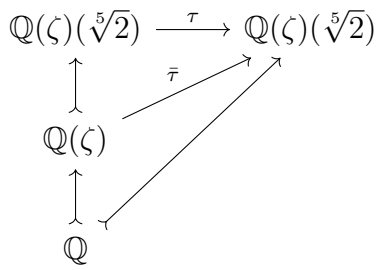
— ∗ —

Sigui $G = \mathrm{Gal}_{\mathbb{Q}}(F)$. Per a determinar els elements de G considerem el següent diagrama



El morfisme ι és la inclusió que ve determinada per $\iota(\zeta) = \zeta$, que existeix perquè ζ és arrel de $x^4 + x^3 + x^2 + x + 1$ a F. Pel lema d'extensió de morfismes, ι es pot extendre a σ tal que $\sigma(\sqrt[5]{2}) = \zeta\sqrt[5]{2}$ perquè $\zeta\sqrt[5]{2}$ és una arrel de $x^5 - 2$ a F. Aleshores $\sigma \in G$.

Similarment considerem



on $\bar{\tau}(\zeta) = \zeta^2$, que és un morfisme perquè ζ^2 és arrel de $x^4 + x^3 + x^3 + x + 1$ a F, i $\tau(\sqrt[5]{2}) = \sqrt[5]{2}$. Pel lema d'extensió de morfismes, τ és un element de G.

— ∗ —

Com que F és un cos de descomposició, pel matiex argument que al problema 1, és una extensió e Galois de $\mathbb{Q}$ i per tant $|G| = [F : \mathbb{Q}] = 20$.

σ té ordre 5 perquè $\sigma^5(\sqrt[5]{2}) = \zeta^5\sqrt[5]{2} = \sqrt[5]{2}$ i τ té ordre 4:

$$\zeta \overset{\tau}{\mapsto} \zeta^2 \overset{\tau}{\mapsto} \zeta^4 \overset{\tau}{\mapsto} \zeta^8 = \zeta^3 \overset{\tau}{\mapsto} \zeta^6 = \zeta.$$

Aleshores $\langle\sigma\rangle$ és un subgrup de G d'ordre 5 i $\langle\tau\rangle$ és un subgrup de G d'ordre 4. Per qüestions de grau, $\langle\sigma\rangle \cap \langle\tau\rangle = \langle\mathrm{id}\rangle$, ja que l'ordre d'un element de la intersecció ha de dividir 5 i 4, per tant només pot ser 1. En particular, si $\sigma^n\tau^m = \sigma^k\tau^l$ aleshores $\sigma^n\sigma^{-k} = \tau^l\tau^{-m} = \mathrm{id}$, pel que $\sigma^n = \sigma^k$ i $\tau^m = \tau^l$. Això vol dir, en particular, que $\langle\sigma\rangle\langle\tau\rangle$ conté almenys 20 elements diferents, els 20 possibles productes d'elements de $\langle\sigma\rangle$ amb elements de $\langle\tau\rangle$. Però $|G| = 20$, el que vol dir $\langle\sigma\rangle\langle\tau\rangle = G$.

Observem que $\langle\sigma\rangle$ és un 5-subgrup de Sylow de G. El nombre de 5-subgrups de Sylow de G, pel tercer teorema de Sylow, divideix 4 i és congruent a 1 mòdul 5, per tant només pot ser 1. Això vol dir que $\langle\sigma\rangle$ és l'únic 5-subgrup de Sylow de G, i per tant és normal, pel segon teorema de Sylow. Estem en totes les hipòtesis per a concloure, fent servir el problema anterior, que

$$G \cong \langle\sigma\rangle \rtimes \langle\tau\rangle$$

i com que $\langle\sigma\rangle$ i $\langle\tau\rangle$ són grups cíclics de 5 i 4 elements respectivament

$$G \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}.$$