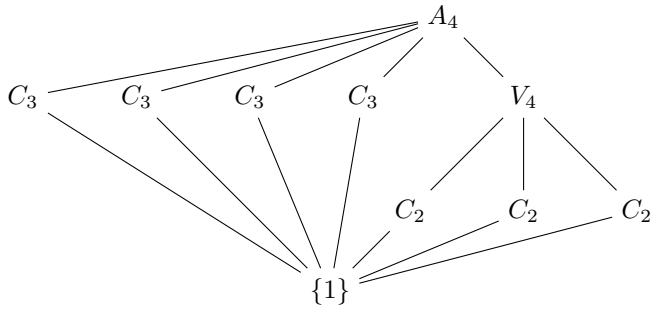
Teoria de Galois

Marc Masdeu

2023-02-13

Índex

Introducció



Aquests són uns apunts de Teoria de Galois, pensats pel curs de 3r del Grau de Matemàtiques de la UAB.

L'assignatura de Teoria de Galois es cursa al primer semestre del tercer curs del Grau de Matemàtiques de la UAB. Consta de 6 crèdits, repartits en:

- Dues hores setmanals de teoria (15 setmanes), que actualment es fan seguides.
- Una hora setmanal de problemes (15 setmanes).
- Tres seminaris pràctics, de 2h cadascun.

El curs es pot dividir de manera natural en 15 sessions de dues hores. El temps efectiu de cadascuna d'aquestes sessions és de 100 minuts, i es pot pensar com una sèrie de 15 capítols. Seguidament detallem cadascun d'aquests capítols i la seva sinopsi.

Episodi 1

Vells coneguts

Començarem recordant les definicions i resultats bàsics que ja s'han vist a altres assignatures, com Fonaments o Estructures algebraiques. Donarem les definicions de cos, característica, cos primer, i veurem que aquest és o bé $\mathbb{F}_p$ per algun primer p, o bé $\mathbb{Q}$. A continuació introduïrem les extensions de cossos i el grau. Construirem el cos $F[x]/(p(x))$ associat a un polinomi irreductible $p(x) \in F[x]$, i veurem alguns exemples.

1.1 Convencions

En aquest curs, tots els anells seran commutatius, i assumirem sempre que tenen unitat. A més, demanarem que un morfisme d'anells enviï l'1 a l'1.

1.2 Característica d'un cos

Lema 1.1. Siguia A un anell qualsevol. Aleshores hi ha un únic morfisme $\mathbb{Z} \to A$.

Demostració. Considerem el morfisme $\iota\colon \mathbb{Z} \to A$ definit com:

$$\iota(n) = \begin{cases} 1_A + 1_A + \cdots + 1_A & n \geq 0, \\ -(1_A + 1_A + \cdots + 1_A) & n < 0, \end{cases}$$

on les sumes tenen n termes. És fàcil comprovar que és un morfisme. La unicitat es demostra per inducció en $|n|$. □

A partir d'ara, qualsevol enter el podem pensar com a element d'un anell donat, i això no ens portarà cap confusió. Com ja sabem, el nucli d'un morfisme d'anells és un ideal. Per tant, el nucli del morfisme $\iota_A\colon \mathbb{Z} \to A$ és un ideal de $\mathbb{Z}$ de la forma (n), amb $n \geq 0$.

Definició 1.1 (Característica). La característica d'un anell A és l'enter no negatiu n tal que $\iota_A = (n)$, i es denota per $\operatorname{char}(A)$.

Fixem-nos que si $\operatorname{char}(A) = n$, aleshores $na = 0$ per a tot $a \in A$.

Proposició 1.1. Sigui F un cos. Aleshores la seva característica és 0 o bé un primer p.

Demostració. Suposem que $\operatorname{char}(F) = n > 0$, i $n = ab$. Aleshores $(a1_A)(b1_A) = (ab)1_A = 0$. Com que F és un cos, això vol dir que $a1_A = 0$ o $b1_A = 0$. Si per exemple $a1_A = 0$, això significa que $n \mid a$.

Com que $n = ab$, necessàriament $a = n$ i $b = 1$. Per tant, els únics divisors de n són trivials, i n és primer. □

Definició 1.2 (cos primer). El cos primer d'un cos F és el cos generat per 1_F. És o bé $\mathbb{Q}$ (si F té característica 0) o bé el cos $\mathbb{F}_p$ (si F té característica p).

1.3 Extensions

Quan K és un cos que conté un altre cos F, direm que K és una extensió de F, i escriurem K/F (no és cap mena de quocient!). Direm també que F és el cos base de l'extensió K/F. També farem servir el diagrama

$$\begin{array}{c} K \\ | \\ F. \end{array}$$

Com que un cos no té ideals propis, un morfisme de cossos $\iota\colon F \to K$ és sempre injectiu i, per tant, la imatge de ι és un subcos de K isomorf a F. A partir d'ara, a vegades identificarem F amb $\iota(F)$, i direm que K és una extensió de F.

Seguidament fem la següent observació clau: quan tenim una extensió K/F aleshores K esdevé automàticament un F-espai vectorial. Això ens permet definir:

Definició 1.3 (grau d'una extensió). El grau de l'extensió K/F és la dimensió de K com a F-espai vectorial, que escrivim com $[K\colon F]$. Direm que K/F és finita si té grau finit, i infinita si no.

Teorema 1.1 (Kronecker). Sigui $f(x) \in F[x]$ un polinomi. Aleshores existeix una extensió K/F tal que K té una arrel de $f(x)$.

Demostració. TODO □

El següent teorema ens diu que l'extensió donada pel teorema anterior té grau igual al grau del polinomi (per això s'ha triat el nom!) quan aquest és irreductible. De fet, ens dona una base de K com a F-espai vectorial.

Teorema 1.2. Sigui $f(x) \in F[x]$ un polinomi irreductible de grau n, i sigui $K = F[x]/(f(x))$. Sigui α la classe de x a K. Aleshores els elements $(1, \alpha, \dots, \alpha^{n-1})$ formen una F-base de K.

Demostració. TODO □

L'aritmètica a $F[x]/(p(x))$ és molt explícita: els seus elements es poden expressar com a polinomis en α de grau menor que $n = \deg(p(x))$. Donats dos polinomis $a(\alpha)$ per $b(\alpha)$, podem considerar el residu $r(x)$ de dividir $a(x)b(x)$ per $p(x)$. Aleshores el producte $a(\alpha)b(\alpha)$ ve donat per l'element $r(\alpha)$. Per divir ens cal utilitzar la identitat de Bézout (exercici).

Exemple 1.1. Mostrem $\mathbb{C}$ com el resultat d'adjuntar una arrel de $x^2 + 1$ a $\mathbb{R}$.

Exemple 1.2. Podem construir de manera semblant $\mathbb{Q}(i)$, o $\mathbb{Q}(\sqrt{2})$, i també $\mathbb{Q}(\sqrt[3]{2})$. Veurem com es poden fer les operacions habituals en algun d'aquests cossos.

Exemple 1.3. Si considerem $\mathbb{F}_p$ el cos finit de p elements i un polinomi $f(x) \in \mathbb{F}_p[x]$ irreductible de grau n (suposant que existeixi!), aleshores obtenim un cos $K/\mathbb{F}_p$ de grau n. Té, per tant, p^n elements.

Exemple 1.4. També podem fer extensions de cossos més "exòtics". Per exemple, podem prendre $k(t)$ com el cos de funcions racionals sobre un cos fixat k, i "afegir" una arrel quadrada de t (mitjançant el polinomi $x^2 - t$).

Sigui K/F una extensió, i considerem un conjunt $S \subseteq K$. Aleshores podem considerar el "mínim" subcos $L \subseteq K$ que conté F i tots els elements de S. S'anomena el cos generat per S sobre F, i escriurem $F(S)$. Si S és un conjunt finit format per $\alpha_1, \dots, \alpha_n$ aleshores escriurem $F(\alpha_1, \dots, \alpha_n)$ i direm que $F(S)$ és finitament generada. Un cas particular és quan S conté un sol element: en aquest cas $F(\alpha)$ s'anomena una extensió simple, i l'element α s'anomena un element primitiu de l'extensió (que no és únic, en general!).

Teorema 1.3 (extensió simple). Sigui $f(x) \in F[x]$ un polinomi irreductible, i suposem que K/F és una extensió que conté una arrel α de $f(x)$. Aleshores hi ha un isomorfisme

$$F[x]/(f(x)) \cong F(\alpha).$$

Aquest isomorfisme és únic si demanem que $[x] \mapsto \alpha$.

Demostració. TODO □

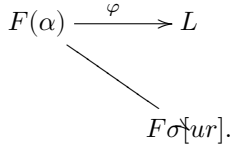
Exemple 1.5. Expliquem l'exemple de $\mathbb{Q}(\sqrt{2})$ i la diferència amb $\mathbb{Q}(\sqrt[3]{2})$. Aquest darrer cos és un subcòs de $\mathbb{R}$, però hi ha un altre subcòs de $\mathbb{C}$ que és isomorf a aquest.

Remarca. En els exemples, hem construit cossos que contenen una de les tres possibles arrels de $x^3 - 2$. Aquests són isomorfs, tal i com hem vist. El fet que un sigui subcos de $\mathbb{R}$ i l'altre de $\mathbb{C}$ té a veure amb anàlisi, no amb àlgebra. Algebraicament, no es poden distingir.

Acabem amb un teorema que ens servirà més endavant. Ens anirà bé fer servir la notació següent. Si $\sigma\colon F \to L$ és un morfisme de cossos i $f(x) \in F[x]$ és un polinomi qualsevol, escrivim $\sigma(f) \in L[x]$ per denotar el polinomi obtingut d'$f(x)$ aplicant σ als seus coeficients.

Teorema 1.4 (extensió de morfismes). Sigui $\sigma\colon F \to L$ un morfisme de cossos. Sigui $f(x) \in F[x]$ un polinomi irreductible. Aleshores l'aplicació $\varphi \mapsto \varphi(\alpha)$ indueix una bijecció

$$\mathrm{Hom}_\sigma(F(\alpha), L) \to \{\beta \in L \mid \sigma(f)(\beta) = 0\}.$$



Demostració.

$$\mathrm{Hom}_\sigma(F(\alpha), L) \cong \mathrm{Hom}_\sigma(F[x]/(f(x)), L) \cong \{\sigma \in \mathrm{Hom}_\sigma(F[x], L) \mid \sigma(f) = 0\},$$

i aquest últim conjunt és precisament $\{\beta \in L \mid \sigma(f)(\beta) = 0\}$. □

Episodi 2

Les Torres

Definirem elements algebraics i transcendents i el polinomi mínim d'un element algebraic, amb exemples. Enunciarem i demostrarem la fórmula de les torres, i com es comporta el grau en composicions de cossos.

2.1 Extensions algebraiques/transcendents

Considerem una extensió K/F.

Definició 2.1 (element algebraic). Diem que un element $\alpha \in K$ és algebraic sobre F si α és l'arrel d'un polinomi $f(x) \in F[x]$.

Diem que α és transcendent sobre F si no és algebraic.

L'extensió K/F és algebraica si tots els elements $\alpha \in K$ són algebraics sobre F.

Fixem-nos que si α és algebraic sobre F aleshores sabem que hi ha algun polinomi $f(x) \in F[x]$ que té α com a arrel. Però n'hi ha molts més, per exemple qualsevol múltiple de $f(x)$. El següent resultat ens permet assignar un polinomi canònic a cada element algebraic.

Proposició 2.1. Si α és algebraic sobre F, aleshores hi ha un únic polinomi mònic i irreductible $\mathrm{Irr}_{\alpha,F}(x)$ que té α com a arrel. A més, $f(x) \in F[x]$ té α com a arrel si i només si és un múltiple de $\mathrm{Irr}_{\alpha,F}(x)$.

Demostració. TODO □

Fixem-nos que, si $K/L/F$ és una torre d'extensions i $\alpha \in K$ és algebraic sobre F, aleshores també ho és sobre L, i a més $\mathrm{Irr}_{\alpha,L}(x)$ divideix $\mathrm{Irr}_{\alpha,F}(x)$ a $L[x]$.

Definició 2.2 (polinomi mínim). El polinomi $\mathrm{Irr}_{\alpha,F}(x)$ s'anomena el polinomi mínim d'α sobre F, i el seu grau s'anomena el grau d'α sobre F.

Posant junt tot el què hem vist fins ara, si prenem $\alpha \in K$ aleshores podem considerar la subextensió $F(\alpha)/F$. En aquest cas, $F(\alpha) \cong F[x]/(\mathrm{Irr}_{\alpha,F}(x))$ i per tant $[F(\alpha) \colon F] = \deg \alpha$.

Exemple 2.1. Revisitem els exemples anteriors, calculant els seus polinomis mínims.

Proposició 2.2. Si $[K \colon F] = n$ i $\alpha \in K$, aleshores $\deg \alpha \leq n$. En particular, K/F és algebraica.

Demostració. TODO □

No és cert que tota extensió algebraica sigui finita (en veurem exemples més endavant).

El següent resultat ens caracteritza com són les extensions quadràtiques d'un cos F de característica $\neq 2$.

Proposició 2.3. Sigui F un cos de característica $\neq 2$, i sigui K/F una extensió de grau 2. Aleshores existeix $\delta \in K \setminus F$ tal que $\delta^2 = D \in F$ i $K = F(\delta)$. Escriurem que $K = F(\sqrt{D})$.

Demostració. TODO □

2.2 Torres de cossos

En aquesta secció considerem torres $L/K/F$. Ens interessa relacionar les dues extensions L/K i K/F amb l'extensió total L/F.

Teorema 2.1 (fórmula de les torres). Si $F \subseteq K \subseteq L$, aleshores

$$[L : F] = [L : K][K : F].$$

Si un costat de l'equació és infinit, aleshores l'altre també.

Demostració. TODO (fàcil, però poc elegant) □

Corol · lary 2.1. Si L/F és una extensió finita i K/F és una subextensió (és a dir, $K \subseteq L$) aleshores $[K : F]$ divideix $[L : F]$.

Per exemple, el corol · lari anterior ens permet deduïr que $\sqrt{2}$ no pertany a cap extensió de grau senar.

Exercici 2.1. Demostreu que el polomi $x^3 - \sqrt{2}$ és irreductible sobre $\mathbb{Q}(\sqrt{2})$, fent servir la torre $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

El següent lema senzill ens permetrà construir qualsevol extensió finitament generada de manera iterativa:

Lema 2.1. Si α i β són elements de K/F, aleshores $F(\alpha, \beta) = (F(\alpha)(\beta))$.

Demostració. TODO □

Exercici 2.2. Calculeu el grau de l'extensió $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, i doneu una base.

Teorema 2.2. L'extensió K/F és finita si i només si $K = F(S)$ on S és un conjunt finit d'elements algebraics.

Corol · lary 2.2. Si α i β són algebraics sobre F, aleshores també ho són $\alpha \pm \beta$, $\alpha\beta$ i α/β (si $\beta \neq 0$).

Corol · lary 2.3. Si L/F és una extensió qualsevol, aleshores el conjunt K d'elements de L que són algebraics sobre F forma un subcos $L/K/F$.

Per exemple, podem considerar $\bar{\mathbb{Q}} \subseteq \mathbb{C}$, el conjunt de tots els complexos algebraics, o també $\bar{\mathbb{Q}} \cap \mathbb{R}$, el conjunt dels reals algebraics. Aquests cossos són enumerables (tenen un conjunt d'elements enumerable) i per tant són més petits que $\mathbb{R}$ i que $\mathbb{C}$. D'aquest fet obtenim que hi ha (molts) elements de $\mathbb{R}$ que no són algebraics. En canvi, sovint és difícil demostrar que un real donat (per exemple π) és transcendent.

Teorema 2.3. Si K/F és una extensió algebraica i L/K també, aleshores L/F és algebraica.

Demostració. TODO □

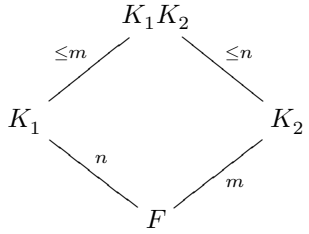
2.3 Compositum de cossos

Recordem que donats dos cossos K_1/F i K_2/F, el seu compost (o compositum) K_1K_2/F és el mínim cos que conté tant a K_1 com a K_2. També es pot pensar com la intersecció de tots els cossos L/F que contenen el conjunt $K_1 \cup K_2$.

Proposició 2.4. Siguin K_1/F i K_2/F dues extensions contingudes a K. Aleshores

$$[K_1K_2 \colon F] \leq [K_1 \colon F][K_2 \colon F].$$

La igualtat es dona si i només si una base de K_1/F segueix essent linealment independent sobre K_2 (o a l'inrevés). A més, tenim:



Demostració. Cal veure que els productes $\alpha\beta$ on α i β recorren bases respectives de K_1/F i de K_2/F generen K_1K_2/F. N'hi ha prou amb veure que les combinacions lineal d'aquests elements formen un cos, que és una observació senzilla. □

Fixem-nos que, si m i n són coprimers, aleshores per la fórmula de les torres tenim $[K_1K2 \colon K_1] = m$ i $[K_1K_2 \colon K_2] = n$. En general, però les desigualtats del diagrama anterior seran estrictes.

Episodi 3

Regle i Compàs

Parlarem de tres problemes de la Grècia clàssica sobre construccions amb regle no marcat i compàs: la quadratura del cercle, la trisecció de l'angle i la duplicació del cub. Caracteritzarem els nombres constructibles, i veurem que aquests problemes no tenen solució. Veurem també que si el regle és marcat aleshores podem trisecar l'angle i també duplicar el cub.

3.1 El problema

Els grecs es van interessar molt per les construccions amb dos instruments molt simples: per una banda, el que habitualment s'anomena regle, i que vol dir simplement un regle sense cap mena de marca. Ens permet, donats dos punts del pla, traçar la recta que els uneix. El segon instrument és el compàs. Donats dos punts podem fixar l'obertura, i donat un tercer punt (que pot coincidir o no amb els anteriors) podem traçar un arc de circumferència amb el radi fixat prèviament, i el centre aquest tercer punt.

Hi ha tres problemes clàssics que ens proposem estudiar:

1. "Duplicació del cub": donat un cub, podem construir-ne un altre de volum exactament el doble?
2. "Trisecció de l'angle": donat un angle θ, podem construir l'angle $\theta/3$?
3. "Quadratura del cercle": donat un cercle, podem construir un quadrat d'àrea igual a la del cercle donat?

Donada una longitud inicial (que definirem com a 1), direm que un nombre real α és constructible si podem construir un segment de longitud α mitjançant una successió finita d'operacions amb regle i compàs. Tenim els quatre tipus d'operacions següents:

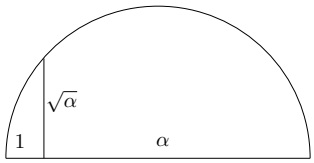
1. Unir dos punts per una recta.
2. Trobar el punt d'intersecció de dues rectes.
3. Dibuixar un cercle amb centre i radi donats.
4. Trobar els punts d'intersecció d'una recta amb un cercle, o de dos cercles.

3.2 La (no) solució

Exercici 3.1. Vegeu que els nombres constructibles formen un subcos de $\mathcal{C} \subseteq \mathbb{R}$. Heu de donar construcions de la suma, resta, producte i divisió de nombres ja construïts.

És fàcil veure que també podem prendre arrels quadrades, com s'indica al següent exercici.

Exercici 3.2. Demostreu que si el diàmetre de la circumferència és $\alpha + 1$, aleshores el segment vertical indicat mesura $\sqrt{\alpha}$.



Fent servir l'equació d'un cercle de radi (x_0, y_0) i radi r

$$(x - x_0)^2 + (y - y_0)^2 ¡ r^2,$$

podem veure que les coordenades de la intersecció amb una recta (posem amb equació $ax + by = c$) pertanyen al cos $\mathbb{Q}(x_0, y_0, r, a, b, c)$. També podem comprovar-ho pel cas de la intersecció de dos cercles. Resumint si α és construcible en n passos a partir de punts en un cos F, aleshores hi ha una successió de cossos

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq F_n,$$

amb $[F_{i+1} \colon F_i] \leq 2$, tals que $\alpha \in F_n$. En particular, α és un nombre algebraic sobre F de grau una potència de 2.

D'aquí en deduïm directament el següent teorema (on haurem d'assumir que π és transcendent, cosa que no demostrem).

Teorema 3.1. Els tres problemes clàssics no són resolubles.

Demostració. Per la duplicació d'un cub de costat 1 ens caldria construir $\sqrt[3]{2}$, que té grau 3 i, per tant, no és constructible.

Si un angle θ és constructible, aleshores fàcilment veiem que $\cos(\theta)$ i $\sin(\theta)$ també són constructibles. Veurem que $\alpha = 2\cos(\pi/9)$ no és constructible. Com que $\cos(\pi/3) = 1/2$, a partir de la fórmula de l'angle triple obtenim

$$\alpha^3 - 3\alpha - 1 = 0.$$

El polinomi $x^3 - 3x - 1$ és irreductible (substituint $x - 2$ obtenim un polinomi 3-Eistenstein) i per tant α té grau 3 i no és constructible.

Finalment, per la quadratura del cercle de radi 1 hauríem de construïr un quadrat de costat $\sqrt{\pi}$. Però aleshores també podríem construir π, que és transcendent (com hem dit, no ho demostrem). □

Més endavant estudiarem quins angles són constructibles. De fet, tenim el següent:

Teorema 3.2. Sigui t un enter. L'angle de t graus (no radians!) és constructible si i només si t és un múltiple de 3.

Demostració. Hi ha construccions molt antigues del pentàgon regular (72°), ja que

$$\cos(72^\circ) = \frac{1}{4}\sqrt{5} - \frac{1}{4},$$

i encara més del triangle equilàter (30°), ja que $\cos(30^\circ) = \sqrt{2}/2$. Com que podem bisectar qualsevol angle, també podem construir 18° i 15°. Finalment, com que $3 = 18 - 15$ també podem construir l'angle de 3°. És clar que no podem construir ni 2° ni 1°, perquè aleshores podríem construir també qualsevol múltiple d'aquests i, per tant, podríem construir 20°, que ja sabem que no és possible. □

3.3 Construccions amb regle marcat i compàs

Aquí veurem que si el regle té dues marques a una distància qualsevol, aleshores podem trisecar l'angle i duplicar el cub.

TODO.

Episodi 4

Normalitat

El cos de descomposició d'un polinomi juga un paper destacat al llarg del curs. Aquí el definirem, i en demostrarem l'existència i unicitat (llevat d'isomorfisme). Aprofitarem per definir extensions normals (aquelles que són cos de descomposició d'un conjunt de polinomis).

Com a aplicació, s'introduiran els polinomis i cossos ciclotòmics, i ho lligarem amb la demostració de l'existència i unicitat de cossos finits de cardinal potència d'un primer.

També veurem les clausures algebraiques, i una construcció (seguint Artin [1] i Jelonek [4]). Això ens permetrà (assumint el teorema fonamental de l'àlgebra, que demostrarem més endavant) pensar els elements algebraics sobre $\mathbb{Q}$ dins dels complexos.

4.1 Cossos de descomposició

Diem que un polinomi $f(x) \in F[x]$ descomposa completament en una extensió K/F si es pot escriure com a producte de polinomis de grau 1.

Definició 4.1 (cos de descomposició). Una extensió K/F és un cos de descomposició del polinomi $f(x) \in F[x]$ si $f(x)$ descomposa completament a K i no ho fa en cap subextensió $K/K'/F$.

Teorema 4.1 (existència del cos de descomposició). Sigui $f(x) \in F[x]$. Aleshores existeix un cos de descomposició K/F de $f(x)$.

Demostració. Fent inducció en el grau d'f, veiem primer que hi ha un cos L/F on $f(x)$ descomposa completament. Després podem prendre per K/F la intersecció de totes les subextensions $L/K'/F$ on $f(x)$ descomposa completament. □

Fixem-nos que cada vegada que adjuntem una arrel d'un polinomi de grau n, aquest polinomi tindrà un cofactor com a molt de grau $n-1$. Així, per obtenir un cos de descomposició en el pitjor dels casos haurem de fer una extensió de grau $n(n-1)(n-2)\cdots 2\cdot 1 = n!$.

Podem fer servir la fórmula de les torres per demostrar una versió més forta d'aixecament de morfismes.

Teorema 4.2 (teorema d'aixecament d'isomorfismes). Sigui K/F una extensió finita, i sigui L/F una extensió. Aleshores:

$$|\operatorname{Hom}_F(K, L)| \leq [K : F].$$

Demostració. Farem inducció en el grau $n = [K\colon F]$. Quan $n = 1$, el resultat és trivial. En general, prenem un element $\alpha \in K \ F$ i fem servir la fórmula de les torres i 1.4. El cardinal de $\mathrm{Hom}_F(F(\alpha), L)$ és igual al nombre d'arrels d'$\mathrm{Irr}_{\alpha,F}(x)$ a L, que com a molt és $[F(\alpha)\colon F]$.

En tot cas, si $\tilde{\sigma}$ és un d'aquests morfismes, com que $[K\colon F(\alpha)] < [K\colon F]$ podem aplicar la hipòtesi d'inducció i $\tilde{\sigma}$ es pot aixecar a com a molt $[K\colon F(\alpha)]$ morfismes a L. □

Revisant la demostració anterior, obtenim els dos següent corol · laris.

Corol · lary 4.1. Siguin K/F i L/F extensions d'un cos F. Si existeix $\alpha \in K$ tal que $\mathrm{Irr}_{\alpha,F}(x)$ no té cap arrel a L, aleshores no existeix cap F-morfisme $K \to L$.

Corol · lary 4.2. Suposem que tot polinomi irreductible a F amb una arrel a K descomposa completament a L. Aleshores

$$|\,\mathrm{Hom}_F(K, L)| = [K\colon F].$$

Proposició 4.1 (unicitat del cos de descomposició). Siguin K/F i K'/F dos cossos de descomposició de $f(x) \in F[x]$. Aleshores $K \cong K'$.

Demostració. Prenem $L = K'$ al Teorema 4.2 i en repetim la demostració. A cada pas, podem prendre com a α una arrel de $f(x)$ i sempre obtindrem arrels a K' perquè $f(x)$ hi trenca completament. □

Exemple 4.1. Calcularem els cossos de descomposició dels exemples que estem fent servir: $x^2 - 2$, $(x^2 - 2)(x^2 - 3)$, $x^3 - 2$ i de $x^4 + 4$, per exemple, ja que en aquest cas el cos de descomposició és simplement $\mathbb{Q}(i)$.

Exemple 4.2 (cossos ciclotòmics). Calculem el cos de descomposició del polinomi $x^n - 1$. Les seves arrels s'anomenen arrels n-èssimes de la unitat. En els complexos les arrels són els nombres $e^{\frac{2\pi i}{n}}$, amb $n = 0, \dots, n - 1$. Per tant $\mathbb{C}$ conté el cos de descomposició de $x^n - 1$. En general, si $K/\mathbb{Q}$ és un cos de descomposició de $x^n - 1$, aleshores podem veure que aquestes formen un grup amb la multiplicació que, de fet, és cíclic. Diem que una arrel de la unitat ζ_n és primitiva si és un generador d'aquest grup. Si en fixem una, les altres primitives són de la forma ζ_n^a, amb a coprimer amb n. Hi ha, doncs, $\varphi(n)$ arrels primitives.

Anomenem *cos ciclotòmic n-èssim$ al cos $\mathbb{Q}(\zeta_n)$, que és el cos de descomposició de $x^n - 1$: si adjuntem ζ_n, automàticament totes les seves potències pertanyen a aquest cos. A l'episodi 6 aprendrem com calcular el grau d'aquest cos, però –a tall d'espòiler– podem veure fàcilment que quan $n = p$ és primer, aleshores

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-1} + \cdots + x + 1),$$

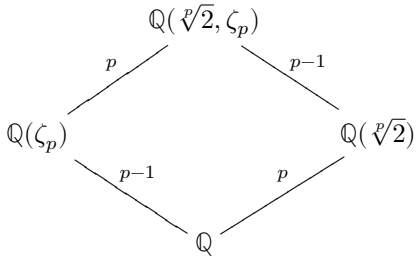
i ja hem vist que el polinomi $\Phi_p(x) = x^{p-1} + x^{p-1} + \cdots + x + 1$ és irreductible. Per tant, tenim

$$[\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = p - 1.$$

Exemple 4.3. Calcularem ara el cos de descomposició de $x^p - 2$, on p és un primer. Si anomenem α una arrel d'aquest polinomi, aleshores les altres arrels són de la forma $\alpha\zeta$, on ζ és una arrel p-èssima de la unitat. Podem veure fàcilment que el cos de descomposició és $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$.

Tenim la torre $L/\mathbb{Q}(\zeta_p)/\mathbb{Q}$ i $L/\mathbb{Q}(\zeta_p)$ té grau com a molt p, ja que està generada per $\sqrt[p]{2}$. Per tant, es té la desigualtat $[L\colon \mathbb{Q}] \leq p(p - 1)$. Com que L té subcossos de grau p i de grau $p - 1$, aquests dos nombres divideixen el grau de l'extensió total i, com que són coprimers, en deduim que el grau és

exactament $p(p-1)$. Ho podem il·lustrar amb el diagrama següent:



4.2 La clausura algebraica

Definició 4.2 (clausura algebraica). Diem que $\bar{F}/F$ és una clausura algebraica d'F si $\bar{F}/F$ és algebraica i tot polinomi $f(x) \in F[x]$ descomposa completament a $\bar{F}$.

Definició 4.3 (algebraicament tancat). Un cos F és algebraicament tancat si és una clausura algebraica sobre si mateix. És a dir, si tot polinomi $f(x) \in F[x]$ té alguna arrel a F.

Aviat veurem que tot cos té alguna clausura algebraica, i que hi ha cossos algebraicament tancats. Veurem primer que les clausures algebraiques són algebraicament tancades.

Proposició 4.2. Sigui $\bar{F}/F$ una clausura algebraica de F. Aleshores $\bar{F}$ és algebricament tancat.

Demostració. Considerem un polinomi $f(x) \in \bar{F}[x]$, i considerem l'extensió $\bar{F}(\alpha)$ obtinguda adjuntant una arrel de $f(x)$ a $\bar{F}$. Aleshores $\bar{F}(\alpha)/\bar{F}/F$ és una torre algebraica, i per tant l'extensió total és algebraica. En particular, α és algebraic sobre F i, per tant, $\alpha \in \bar{F}$, com volíem demostrar. □

El següent resultat ens permet trobar una clausura algebraica de qualsevol subcos d'un cos algebraicament tancat.

Proposició 4.3. Sigui K/F una extensió, i suposem que K és algebraicament tancada. Aleshores la subextensió $\bar{F}/F$ formada pels elements de K que són algebraics sobre F és una clausura algebraica de F .

Demostració. L'extensió $\bar{F}/F$ és algebraica per definició. Donat un polinomi $f(x) \in F[x]$, aquest trencarà completament a K en producte de polinomis de la forma $x - \alpha$. Però cadascun dels α és algebraic sobre F i, per tant, és un element de $\bar{F}$. Per tant $f(x)$ ja trencava completament a $\bar{F}[x]$, i per tant $\bar{F}$ és una clausura algebraica de F. □

Cap al final del curs veurem una demostració del següent teorema, que també es pot demostrar amb mètodes analítics.

Teorema 4.3 (Teorema Fonamental de l'Àlgebra). El cos $\mathbb{C}$ dels nombres complexos és algebraicament tancat

Com a conseqüència, podrem clausures algebraiques de qualsevol extensió subextensió $\mathbb{C}/F/\mathbb{Q}$. En particular, el cos $\bar{\mathbb{Q}}$ format pels complexos algebraics és una clausura algebraica de $\mathbb{Q}$.

Donat un cos qualsevol F, tenim ara l'objectiu de construir una clausura algebraica $\bar{F}/F$. Intuitivament almenys, la idea és de considerar, per cada polinomi $g(x) \in F[x]$, un cos F_g que contingui totes les arrels de g. Aleshores hauríem de prendre el compositum de tots aquests cossos. El problema és que per fer el compositum hem de prendre una intersecció de molts cossos, i no està clar on viuen aquests cossos (la intersecció de conjunts només té sentit quan aquests conjunts són subconjunts d'un conjunt

fixat). Fixem-nos que si només consideréssim un nombre finit de polinomis $g_1(x), \dots, g_n(x)$ aleshores podríem prendre el cos de descomposició del producte $g_1(x) \cdots g_n(x)$.

Teorema 4.4 (existència de clausura algebraica). Sigui F un cos. Aleshores existeix una clausura algebraica $\bar{F}/F$.

Demostració. Considerem un conjunt $\mathcal{U} \supset F$ de cardinal estrictament superior a $\mathcal{N} = \max(\aleph_0, |K|)$.

Sigui

$$X = \{K \subseteq L \subseteq S \mid L/K \text{ és una extensió algebraica de } K\},$$

amb la relació d'ordre

$$K_2 > K_1 \iff K_2/K_1 \text{ és una extensió algebraica.}$$

Com que tota cadena té un element maximal (prenem la unió de totes les extensions), el lema de Zorn ens diu que hi ha un element maximal a X, que anomenarem $\bar{F}$. Només ens cal veure que $\bar{F}/F$ és una clausura algebraica. Sigui $f(x) \in F[x]$ un polinomi no constant, i suposem que no té cap zero a $\bar{F}$. Podem construir una extensió $L/\bar{F}$ on $f(x)$ tingui un zero. Aleshores L/F és algebraica, i per tant

$$|\bar{F}| \leq |L| \leq \mathcal{N}.$$

Per tant, $|S \setminus \bar{K}| = |S| > |L \setminus \bar{K}|$. Això fa que existeixi una aplicació (de conjunts) injectiva $i\colon L \to S$ tal que $i(x) = x$ si $x \in \bar{F}$. Podem doncs transportar l'estructura de cos de L a $i(L)$ i obtenim un nou element maximal $L > \bar{F}$, contradient la maximalitat de $\bar{F}$. □

Una demostració alternativa: ::: {.proof} Presentem una demostració alternativa que amaga una mica més els problemes amb la teoria de conjunts. Gràcies a la Proposició 4.3, n'hi ha prou amb construir una extensió K/F algebraicament tancada.

Per cada polinomi mònic no constant $f = f(x) \in F[x]$, considerem una variable x_f. Tenim l'anell de polinomis en infinites variables $F[\{x_f\}]$, i hi podem considerar l'ideal I generat pels polinomis $f(x_f)$.

Veurem que I no és el total i que, per tant, està contingut en un ideal maximal $\mathcal{M}$. El quocient l'anomenem K_1, que és una extensió de F que conté una arrel de cada polinomi amb coeficients a F. Podem iterar el procés (començant amb K_1 en comptes de amb F) per obtenir K_2/K_1, una extensió on tot polinomi amb coeficients a K_1 té una arrel, i així construim una successió de cossos de la qual en podem prendre la seva "unió" K. Donat un polinomi $f(x) \in K[x]$, tots els seus coeficients viuen necessàriament a K_n i, per tant, $f(x)$ té alguna arrel a K_{n+1} i, per tant a K.

Ens queda per veure que I és un ideal propi. Suposem que no i arribarem a contradicció. Suposem que tenim una relació

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots + g_k f_k(x_{f_k}) = 1, \quad g_i \in F[\{x_f\}].$$

En total, aquesta relació només involucra un nombre finit de variables. Les hi posem nom: denotem $x_1 = x_{f_1}$, i així successivament fins a $x_k = x_{f_k}$. Després anomenem $x_{k+1}, \dots, x_r$ la resta de variables que apareixen en els polinomis g_i, de manera que podem reescriure la relació anterior com

$$g_1(x_1, \dots, x_r) f_1(x_1) + g_2(x_1, \dots, x_r) f_2(x_2) + \cdots + g_k(x_1, \dots x_r) f_k(x_k) = 1.$$

Prenem ara una extensió finita F'/F que contingui una arrel α_i de $f_i(x)$ per cada i. La relació anterior particularitza, si fem $x_i = \alpha_i$ per $i = 1, \dots, k$ i $x_i = 0$ per $i > k$, a $0 = 1$, que és una contradicció. Això acaba la demostració. :::

La clausura algebraica és única llevat d'isomorfisme, fet que es pot deduir fàcilment de la unicitat de cossos de descomposició.

Demostració. TODO □

Remarca. L'existència i unicitat de clausures algebraiques fou demostrada per Steinitz el 1910, i la demostració era molt més llarga i complicada (unes 20 pàgines).

També es pot demostrar (però ens cal teoria que veurem una mica més endavant) que el cos K_1 que apareix a la demostració anterior ja és algebraicament tancat, així que no caldria fer tots els altres infinits passos. La demostració d'aquest fet no és senzilla, fa servir el teorema de l'element primitiu (vegeu 10), i separa els casos de característica 0 i característica p.

4.3 Extensions normals

Definició 4.4 (extensió normal). Una extensió algebraica K/F es diu normal si tot polinomi irreductible $f(x) \in F[x]$ que té una arrel a K trenca completament a K.

Dit d'una altra manera K/F és normal si per tot $\alpha \in K$ el seu polinomi mínim sobre F descomposa completament a K. D'entrada, sembla difícil demostrar que una extensió donada K/F és normal, ja que cal veure una propietat per possiblement infinits polinomis. Veurem ara que les extensions normals tenen una caracterització més senzilla. En particular, el cos de descomposició d'un polinomi és sempre una extensió normal.

Proposició 4.4. Una extensió K/F és normal si i només si K és el cos de descomposició d'un conjunt $S \subset F[x]$ de polinomis de F.

Demostració. Suposem que K/F és normal. Per cada element $\alpha \in K$, denotem per $f_\alpha(x) = \mathrm{Irr}_{\alpha,F}(x)$. Aleshores K és el cos de descomposició del conjunt $S = \{f_\alpha(x) \mid \alpha \in K\}$.

Recíprocament, si K és el cos de descomposició d'un conjunt S i $f(x) \in F[x]$ té una arrel $\alpha \in K$, aleshores sense perdre generalitat podem suposar que $f(x)$ és irreductible. Considerem el conjunt $\Sigma \subset K$ d'elements de K que són arrels de polinomis a S. Podem trobar un subconjunt finit S_0 i el seu corresponent conjunt d'arrels Σ_0 tals que $\alpha \in F(\Sigma_0)$. Però aleshores $F(\Sigma_0)$ és un cos de descomposició d'un polinomi (el que s'obté multiplicant tots els polinomis de S_0 i extraient-ne la part lliure de quadrats). Per tant, $f(x)$ descomposa completament a $F(\Sigma_0)$ i per tant també a K. □

Proposició 4.5. Sigui $L/K/F$ una torre. Si L/F és normal, aleshores L/K també ho és.

Demostració. Trivial: si L/F és el cos de descomposició d'un conjunt de polinomis S, també ho és del mateix conjunt pensat com a conjunt de polinomis amb coeficients a K. □

Episodi 5

Polinomis (In)separables

Definim la noció de separabilitat d'un polinomi, i posem algun exemple. Introduïm el morfisme de Frobenius, que ens permet definir cossos perfectes. Aprofitem per parlar del grau de separabilitat/inseparabilitat d'una extensió, i la factorització d'aquesta.

Finalment, donem l'existència i unicitat dels cossos finits.

5.1 Separabilitat de polinomis i extensions

Sigui F un cos.

Definició 5.1 (separabilitat). Un polinomi $f(x) \in F[x]$ és separable si les seves arrels (en un cos de descomposició) són totes diferents. Si $f(x)$ no és separable diem que $f(x)$ és inseparable.

Fixem-nos que la definició no depèn del cos de descomposició que ens triem, per unicitat llevat d'isomorfisme. De fet, podem caracteritzar la separabilitat de $f(x)$ sense haver de considerar cap cos de descomposició:

Proposició 5.1. Un polinomi $f(x)$ té una arrel múltiple α si i només si α és una arrel de $f'(x)$. En particular, $f(x)$ és separable si i només si $\mathrm{mcd}(f(x), f'(x)) = 1$.

Demostració. TODO (fàcil, fet a fonaments). □

Corol · lary 5.1. Si $f(x) \in F[x]$ és irreductible i F té característica 0, aleshores f és separable. En general, un polinomi $f(x) \in F[x]$ és separable si i només si és producte de diferents polinomis irreductibles.

Demostració. TODO (molt fàcil). □

Exemple 5.1. El polinomi $x^n - 1$ té derivada nx^{n-1} i per tant, si $n \neq 0$ a F aleshores $x^n - 1$ és separable, i en aquest cas hi ha n arrels de la unitat diferents a F. En canvi, si F és de característica $p \mid n$, aleshores cada arrel de $x^n - 1$ és múltiple.

Ja hem estudiat el problema de separabilitat en característica 0, que és molt senzill. Ens centrarem ara en característica p, així que sigui F un cos de característica finita p. Pensem en què pot anar malament per tal que un polinomi irreductible $f(x) \in F[x]$ sigui inseparable. Cal que la seva derivada tingui factors en comú amb $f(x)$, i això només pot passar si la derivada és 0.

Lema 5.1. Sigui $f(x) \in F[x]$ amb $\text{char}(F) = p$. Si $f'(x) = 0$, aleshores hi ha un polinomi $f_1[x] \in F[x]$ tal que $f(x) = f_1(x^p)$.

En particular, observem que si $f(x) \in F[x]$ és inseparable, aleshores el seu grau és un múltiple de p.

Proposició 5.2. Sigui $f(x) \in F[x]$ amb $\text{char}(F) = p$ un polinomi irreductible. Aleshores hi ha un únic $k \geq 0$ i un únic polinomi irreductible i separable $g(x) \in F[x]$ tal que

$$f(x) = g(x^{p^k}).$$

Demostració. Iterem el procediment del lema anterior fins que el polinomi que obtenim és separable. Seguirà essent irreductible, i ja haurem acabat. □

Definició 5.2 (grau de separabilitat). Sigui $f(x) \in F[x]$ amb $\text{char}(F) = p$ un polinomi irreductible. El grau de separabilitat de $f(x)$ és el grau de $g(x)$ en la proposició anterior, i el denotem per $\deg_s f(x)$.

El grau d'inseparabilitat és l'enter p^k que hi apareix, i el denotem per $\deg_i f(x)$.

Observem que $\deg f(x) = \deg_s f(x) \deg_i f(x)$.

Proposició 5.3. Sigui F un cos de característica p. Aleshores l'aplicació $a \mapsto a^p$ és un morfisme de cossos $F \to F$.

Demostració. Només cal veure que $(a+b)^p = a^p + b^p$ i que $(ab)^p = a^p b^p$. La primera igualtat es veu fent servir que p divideix a $\binom{p}{i}$ per a $1 \leq i \leq p-1$, i la segona és trivial. □

El morfisme de la proposició anterior s'anomena el morfisme de Frobenius. Observem que si $\mathbb{F}$ és un cos finit, aleshores el morfisme de Frobenius és un isomorfisme (només cal comptar), però en general no és cert. Per exemple, la imatge de Frobenius a $F = \mathbb{F}_p(t)$ és $\mathbb{F}_p(t^p)$.

Proposició 5.4. Sigui $\mathbb{F}$ és un cos de característica p tal que el morfisme de Frobenius és exhaustiu. Aleshores tot polinomi irreductible sobre $\mathbb{F}$ és separable.

Demostració. Suposem que $f(x)$ fos inseparable. Aleshores $f(x) = f_1(x^p)$ per algun $f_1(x) \in \mathbb{F}[x]$. Els coeficients de f_1 són potències de p, i aleshores podem escriure

$$f_1(x) = a_m^p x^m + a_{m-1}^p x^{m-1} + \cdots a_1^p x + a_0^p.$$

Per tant, tenim

$$f(x) = f_1(x^p) = a_m^p x^{pm} + a_{m-1}^p x^{p(m-1)} + \cdots a_1^p x^p + a_0^p = \left(a_m x^m + a_{m-1} x^{m-1} + \cdots a_1 x + a_0\right)^p,$$

que contradiu el fet que $f(x)$ sigui irreductible. □

Aquesta definició ens servirà per unificar els dos casos on la separabilitat no és problemàtica.

Definició 5.3 (cos perfecte). Un cos F és perfecte si té característica 0 o bé el morfisme de Frobenius és exhaustiu.

Corol · lary 5.2. Si F és perfecte, aleshores tot polinomi irreductible a $F[x]$ és separable.

Finalment, podem introduir el concepte d'extensió separable.

Definició 5.4 (extensió separable). Una extensió K/F és separable si tot element de K és arrel d'un polinomi separable sobre F.

Corol · lary 5.3. Tota extensió finita d'un cos perfecte és separable. En particular, els cossos finits són separables.

Corol · lary 5.4. Sigui F un cos de característica p, i sigui K/F una extensió finita tal que $p \nmid [K : F]$. Aleshores K/F és separable.

Demostració. Sigui $\alpha \in K$, i considerem $\mathrm{Irr}_{\alpha,F}(x)$. Com que el seu grau és un divisor de $[K : F]$, no pot ser divisible per p i, per tant, és separable. □

Més endavant ens serà útil saber que que la separabilitat es comporta bé en torres. ::: {.lemma} Sigui $L/K/F$ una torre. Si L/F és separable, aleshores L/K i K/F també ho són. ::: ::: {.proof} Si L/F aleshores K/F és separable, trivialment. Per veure que L/K també ho és, observem simplement que per tot $\alpha \in L$, el polinomi $\mathrm{Irr}_{\alpha,K}(x)$ és un divisor (a $K[x]$) del polinomi $\mathrm{Irr}_{\alpha,F}(x)$. :::

Més endavant veurem que el recíproc també és cert, però per ara no ens caldrà.

5.2 Applicació : cossos finits

L'objectiu és demostrar l'existència de cossos finits d'ordre qualsevol potència d'un primer, i veure que són únics (llevat d'isomorfisme).

Teorema 5.1 (Existència i unicitat de cossos finits). Per tot primer p i tot $n \geq 1$, hi ha un únic (llevat d'isomorfisme) cos finit d'ordre p^n, que denotarem per $\mathbb{F}_{p^n}$. A més, si $\mathbb{F}$ és un cos finit de característica p, aleshores és isomorf a $\mathbb{F}_{p^n}$ per alguna $n \geq 1$.

Demostració. Sigui $n \geq 1$, i fixem-nos que el polinomi $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ té derivada -1 i, per tant, és separable. Si α i β són dues arrels qualssevol, aleshores $\alpha\beta$ i $\alpha + \beta$ també són arrels. Per tant, el conjunt L format per les p^n arrels forma un subcos del cos de descomposició de $f(x)$ i, per tant, com que L conté totes les arrels, ha de ser el propi cos de descomposició. Com que L té p^n elements, té grau n sobre $\mathbb{F}_p$, i per tant hem vist que hi ha cossos finits de grau n per qualsevol $n \geq 1$.

Sigui ara $\mathbb{F}$ un cos finit qualsevol de característica p. Com que és un espai vectorial sobre el seu cos primer $\mathbb{F}_p$, ha de tenir p^n elements per algun $n \geq 1$. Fixem-nos que $\mathbb{F}^\times$ és un grup d'ordre $p^n - 1$ i, per tant $\alpha^{p^n-1} = 1$ per tot $\alpha \in \mathbb{F}$. Per tant α és una arrel de $x^{p^n} - x$ i $\mathbb{F}$ està contingut al cos de descomposició d'aquest polinomi. Mirant el nombre d'elements, veiem que és igual al cos de descomposició. □

Episodi 6

Polinomis Ciclotòmics

L'objectiu principal és demostrar que l'extensió ciclotòmica $\mathbb{Q}(\zeta_n)$ té grau $\varphi(n)$ (la phi d'Euler). Per això, introduïrem els polinomis ciclotòmics, veurem que són irreductibles i mònics i tenen coeficients enters.

6.1 Definició

Sigui μ_n el grup de les arrels n-èssimes de la unitat, que podem pensar dins de $\mathbb{C}$. Com a grup abstracte, és isomorf a $\mathbb{Z}/n\mathbb{Z}$ (un cop fixem una arrel primitiva ζ_n):

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n, \quad a \mapsto \zeta_n^a.$$

Ja hem observat que les arrels primitives són exactament les de la forma ζ_n^a amb a coprimer amb n i que, per tant, n'hi ha $\varphi(n)$. Fixem-nos també que si $d \mid n$ aleshores $\mu_d \subseteq \mu_n$. Però fixem-nos que si $\zeta \in \mu_n$, aleshores ζ és una arrel primitiva d-èssima per algun $d \mid n$.

Definició 6.1 (polinomi ciclotòmic). El polinomi ciclotòmic n-èssim $\Phi_n(x)$ és el polinomi de grau $\varphi(n)$ que té per arrels les arrels primitives de la unitat:

$$\Phi_n(x) = \prod_{\substack{1 \le a \le n \\ \mathrm{mcd}(a,n)=1}} (x - \zeta_n^a).$$

6.2 Càlcul recursiu

Tenim la factorització

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d \mid n} \Phi_d(x).$$

En particular, comparant graus tenim la identitat

$$n = \sum_{d \mid n} \varphi(d).$$

A més, fixem-nos que la fórmula anterior ens permet calcular els polinomis ciclotòmics de manera recursiva, dividint pels factors coneguts:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)}. \tag{6.1}$$

Els primers valors són, per exemple:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\
\Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1 \\
\Phi_{13}(x) &= x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

Lema 6.1. Els polinomis $\Phi_n(x)$ són mònics de grau $\varphi(n)$ i tenen coeficients enters.

Demostració. L'únic que ens cal veure és que $\Phi_n(x)$ té coeficients enters. Això es veu fàcilment per inducció en n i l'algoritme de divisió, fent servir la fórmula (6.1). □

6.3 Irreductibilitat

Amb una mica més de feina podem veure que també són irreductibles.

Teorema 6.1. Els polinomis $\Phi_n(x)$ són irreductibles.

Demostració. Prenem $n \geq 3$, i escrivim una factorització $\Phi_n(x) = f(x)g(x)$ amb $f(x)$ i $g(x)$ mònics a $\mathbb{Z}[x]$, i amb $f(x)$ irreductible de grau com a mínim 2. L'objectiu és demostrar que $f(x) = \Phi_n(x)$, és a dir, que tota arrel primitiva n-èssima és arrel de $f(x)$. Sigui doncs ζ una arrel n-èssima primitiva que sigui arrel de $f(x)$, i veurem que ζ^a també és arrel de $f(x)$ per a tot a coprimer amb n.

TODO □

Corol · lary 6.1. El cos ciclotòmic $\mathbb{Q}(\zeta_n)$ té grau $\varphi(n)$ sobre $\mathbb{Q}$.

Episodi 7

Automorfismes

Començarem definint els automorfismes d'una extensió. Veurem que formen un grup, i que cada subgrup té associat el cos dels elements fixos per aquest. Veurem també que els automorfismes envien cada element α a una arrel de $\mathrm{Irr}(\alpha, x)$, i demostrarem que en una extensió normal el cardinal del grup d'automorfismes està fitat pel grau de l'extensió. Així, podrem definir una extensió de Galois com aquella on la fita s'assoleix.

7.1 Definició

Sigui K un cos. Un automorfisme de K és simplement un isomorfisme de K a K, i el grup d'automorfismes de K (amb la composició) s'escriu $\mathrm{Aut}(K)$.

Si $\alpha \in K$, diem que $\sigma \in \mathrm{Aut}(K)$ fixa α si $\sigma(\alpha) = \alpha$. Més en general, si S és un subconjunt de K, diem que $\sigma \in \mathrm{Aut}(K)$ fixa S si $\sigma(x) = x$ per a tot $x \in S$.

Fixem-nos també que tot automorfisme fixa el cos primer de K (exercici). En particular, $\mathrm{Aut}(\mathbb{Q}) = \mathrm{Aut}(\mathbb{F}_p) = 1$.

Un cas important de subconjunt S es dona quan tenim una extensió de cossos K/F. En aquest cas, escrivim $\mathrm{Aut}(K/F)$ com el grup d'automorfismes que fixen F (que és un subgrup d'$\mathrm{Aut}(K)$):

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(x) = x \,\forall x \in F\}.$$

Proposició 7.1. Sigui K/F una extensió, i sigui $\alpha \in K$ un element algebraic sobre F. Aleshores per tot $\sigma \in \mathrm{Aut}(K/F)$ envia α a una arrel $\sigma(\alpha)$ de $\mathrm{Irr}(\alpha, F)(x)$.

Demostració. Com que $\mathrm{Irr}(\alpha, F)(x)$ té coeficients a F i σ és un morfisme de cossos, tenim

$$\mathrm{Irr}(\alpha, F)(\sigma(\alpha)) = \sigma(\mathrm{Irr}(\alpha, F)(\alpha)) = \sigma(0) = 0.$$

□

Corol · lary 7.1. Sigui $f(x) \in F[x]$ un polinomi irreductible i K/F és una extensió. Aleshores tot automorfisme $\sigma \in \mathrm{Aut}(K/F)$ permuta les arrels de $f(x)$ a K.

Corol · lary 7.2. Sigui K/F una extensió algebraica. Aleshores $\mathrm{Hom}_F(K, K) = \mathrm{Aut}(K/F)$.

Demostració. Sigui $\sigma\colon K \to K$ un morfisme que fixa F. Ja sabem que és injectiu, però volem veure que és exhaustiu. Si K/F és una extensió finita això ja ho sabem (per àlgebra lineal), però aquí ho volem veure en general. Sigui $\beta \in K$ qualsevol element. Considerem el conjunt

$$B = \{\text{arrels de } \mathrm{Irr}_{\beta,F}(x) \text{ a } K\}.$$

Aleshores σ indueix una aplicació injectiva al conjunt finit B i, per tant, també exhaustiva. Per tant hi ha $\alpha \in B \subseteq K$ tal que $\sigma(\alpha) = \beta$. □

Aquests resultats ens permeten descriure el grup d'automorfismes d'extensions algebraiques considerant com actuen aquests automorfismes en els elements que generen l'extensió, ja que tot automorfisme quedarà únicament determinat per aquesta acció. En particular, quan K/F és finita el nombre d'automorfismes també serà finit.

Exemple 7.1. Calculem $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ i $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/QQ) = 1$.

7.2 Cossos fixos

Fixem K un cos. Hem vist com associar a cada subcos $F \subseteq K$ un subgrup $\mathrm{Aut}(K/F)$ d'$\mathrm{Aut}(K)$. Prenem ara la direcció oposada. Associarem a cada subgrup d'automorfismes una certa extensió. Concretament, si $S \subseteq \mathrm{Aut}(K)$ és un subconjunt, podem considerar aquells elements de K que són fixos per tots els elements de S. És molt fàcil veure que aquest conjunt, que escriurem K^S i anomenarem el cos fix per S, és un subcos de K (exercici). Fixem-nos també que

$$K^S = K^{\langle S \rangle},$$

on $\langle S \rangle$ és el subgrup d'$\mathrm{Aut}(K)$ generat per S (el subgrup més petit que conté S). Per tant, normalment considerarem només cossos fixos per subgrups d'$\mathrm{Aut}(K)$ i no perdrem generalitat.

Lema 7.1. Sigui K un cos. - Si $F1 \subseteq F_2 \subseteq K$, aleshores $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$. - Si $H_1 \leq H_2 \leq \mathrm{Aut}(K)$, aleshores $K^{H_2} \subseteq K^{H_1}$.

Demostració. Trivial. □

Lema 7.2. Sigui F un cos infinit, i sigui V un F-espai vectorial, i siguin $V_1, \dots, V_r$ subespais propis. Aleshores $V \neq \bigcup V_i$.

Demostració. Fem inducció en la dimensió n de V. El cas $n = 1$ és trivial, així que podem assumir-ho cert per tot F-espai vectorial de dimensió $\leq n-1$ i ho demostrarem per V. Triem un subespai $U \subset V$ de dimensió $n-1$ diferent de tots els V_i (aquí utilitzem que F és infinit). Aleshores apliquem inducció als subespais $U \cap V_i$ d'U, i obtenim un element d'U que ja ens serveix. □

Remarca. El lema també és cert quan V és de dimensió infinita (exercici), però no ens caldrà per les aplicacions.

Proposició 7.2. Sigui K/F una extensió finita, i siguin $K_1, \dots, K_r$ subextensions diferents de K. Aleshores hi ha algun element de K que no pertany a cap dels K_i.

Demostració. Si F és infinit, ja estem pel lema anterior. Fem doncs el cas on F és finit. En aquest cas K també és finit, posem que té p^n elements. Aleshores els K_i també són finits, i tenen p^i elements cadascun. Com que tots són diferents i hi ha un únic cos finit de cada cardinal, la unió dels K_i té com a molt

$$\sum_{j=0}^{n-1} p^j = \frac{p^n - 1}{p - 1}$$

elements, que és menor que p^n. □

Teorema 7.1. Sigui K/F una extensió finita. Aleshores

$$|\operatorname{Aut}(K/F)| \leq [K\colon F].$$

En particular, $\operatorname{Aut}(K/F)$ és un grup finit.

Demostració. Suposem que $\operatorname{Aut}(K/F)$ conté $\sigma_1 = 1, \dots, \sigma_n$ automorfismes diferents. Per cada $i \neq j$, considerem el conjunt

$$\operatorname{Eq}_{\sigma_i,\sigma_j} = \{x \in K \mid \sigma_i(x) = \sigma_j(x)\}.$$

És fàcil veure que $\operatorname{Eq}_{\sigma_i,\sigma_j} \subsetneq K$ i que $\operatorname{Eq}_{\sigma_i,\sigma_j}$ és un cos. Aplicant la proposició anterior, hi ha algun $\alpha \in K$ que no està en cap dels $\operatorname{Eq}_{\sigma_i,\sigma_j}$. El polinomi mínim d'$\alpha$ sobre F té arrels $\alpha, \sigma_2(\alpha), \dots, \sigma_{n+1}(\alpha)$, que són totes diferents. Per tant $[F(\alpha)\colon F] \geq n$. Però $F(\alpha)$ és una subextensió de K i, per tant $[K\colon F] \geq n$. □

Donarem un nom doncs a aquelles extensions que tinguin el nombre màxim d'automorfismes que permet aquesta fita.

Definició 7.1 (extensió de Galois). Sigui K/F una extensió finita. Diem que K és Galois sobre F (o que K/F és una extensió de Galois) si $|\operatorname{Aut}(K/F)| = [K\colon F]$. En aquest cas, escriurem $\operatorname{Gal}(K/F) = \operatorname{Aut}(K/F)$.

Corol·lary 7.3. Sigui K/F una extensió finita i Galois. Aleshores $K^{\operatorname{Gal}(K/F)} = F$.

Demostració. Escrivim $G = \operatorname{Gal}(K/F)$, i sigui $M = K^G \supseteq F$. Tenim, per definició, que $G = \operatorname{Aut}(K/M)$. Per tant, $[K\colon F] = |G| \leq [K\colon M]$, del que en deduim $F = M$. □

Corol·lary 7.4. Sigui K/F una extensió finita i Galois. Aleshores hi ha un polinomi irreductible i separable $f(x) \in F[x]$ de grau $[K\colon F]$ que descomposa completament a K.

Demostració. Sigui $n = [K\colon F] = |\operatorname{Gal}(K/F)|$. A la demostració del teorema, prenem tots els n automorfismes, obtenint $\alpha \in K$ tal que $F(\alpha) = F$. El seu polinomi mínim $f(x) \in F[x]$ és irreductible, de grau n i té per arrels $\{\sigma(\alpha) \mid \sigma \in \operatorname{Aut}(K/F)\}$. Per tant té n arrels totes diferents, com volíem. □

Les dues propietats de les extensions de Galois de fet les caracteritzen. Vegem una quarta caracterització d'aquestes extensions:

Teorema 7.2 (Caracterització d'extensions de Galois). Sigui K/F una extensió finita i sigui $G = \operatorname{Aut}(K/F)$. Aleshores els següents enunciats són equivalents: 1. $|G| = [K\colon F]$. 2. $F = K^G$. 3. K/F és normal i separable. 4. Hi ha un polinomi $f(x) \in F[x]$ irreductible i separable de grau $[K\colon F]$ que descomposa completament a K.

Demostració. Ja hem vist $1 \implies 2$ i $1 \implies 4$. Fixem-nos també que $4 \implies 3$ és obvi. - $2 \implies 3$: Suposem que $K = F(\alpha_1, \dots, \alpha_m)$, i considerem el conjunt finit

$$B = \{\sigma(\alpha_i) \mid \sigma \in G, i = 1, \dots, m\}.$$

Fixem-nos que no sabem quants elements exactament conté B. En tot cas, considerem el polinomi separable

$$f(x) = \prod_{\beta \in B} (z - \beta).$$

Observem que $\sigma(f) = f$ per a tot $\sigma \in G$ i, per tant, $f \in K^G[x] = F[x]$. Finalment, α_i és arrel de $f(x)$ per a tot $i = 1, \dots, m$ i concloem que K és el cos de descomposició de $f(x)$.

- $3 \implies 1$: Suposem que K/F és el cos de descomposició d'un polinomi separable $f(x) \in F[x]$. Com s'ha indicat al Corol · lari 4.2, a cada pas podem prendre per α una arrel del polinomi $f(x)$ i per tant tindrem la igualtat.

□

Remarca. Suposem que K/F és de Galois, i sigui $\alpha \in K$ una arrel del polinomi $f(x)$ que apareix a la condició (4). Aleshores $K = F(\alpha)$. Veiem doncs que tota extensió finita de Galois és primitiva. Més endavant veurem que només cal que K/F sigui separable.

Si K/F és una extensió de Galois i $\alpha \in K$, els elements $\sigma(\alpha)$ (on $\sigma \in \mathrm{Gal}(K/F)$) s'anomenen conjugats de Galois d'α sobre F. Si $K/M/F$ és una subextensió, el cos $\sigma(M)$ s'anomena el conjugat de M per σ.

Episodi 8

El Teorema Fonamental

Enunciem i demostrem el teorema fonamental de la teoria de Galois. Acabarem amb diversos exemples concrets d'extensions, il · lustrant la correspondència de Galois.

Proposició 8.1. Sigui K una cos qualsevol. Sigui $G \leq \mathrm{Aut}(K)$ un subgrup finit, i sigui $F = K^G$. Aleshores K és Galois sobre F, i $\mathrm{Gal}(K/F) = G$.

Demostració. Per definició d'F, tenim $G \leq \mathrm{Aut}(K/F)$, i només ens cal veure la igualtat. El teorema ens diu que $|G| = [K : F]$, i ja hem vist $|\mathrm{Aut}(K/F)| \leq [K : F]$. Per tant:

$$[K : F] = |G| \leq |\mathrm{Aut}(K/F)| \leq [K : F].$$

Per tant, totes les desigualtats són igualtats i, en particular $|G| = |\mathrm{Aut}(K/F)|$. □

Corol · lary 8.1. Si G_1 i G_2 són subgrups diferents d'$\mathrm{Aut}(K)$, aleshores $K^{G_1} \neq K^{G_2}$.

Demostració. Trivial. □

Sigui K/F una extensió finita de Galois. A cada subextensió K/M li podem associar el seu grup de Galois, $\mathrm{Gal}(K/M)$. També podem associar a cada subgrup $H \leq \mathrm{Gal}(K/F)$ el cos fix K^H. El següent resultat ens diu que aquestes dues operacions són inverses mútuament.

Teorema 8.1. Sigui K/F finita Galois. Aleshores $M \mapsto \mathrm{Gal}(K/M)$ i $H \mapsto K^H$ estableixen una bijecció

$$\{ \text{ subextensions } K/M/F\} \overset{1:1}{\longleftrightarrow} \{ \text{ subgrups } H \leq \mathrm{Gal}(K/F)\}.$$

A més el grau $[M : F]$ es correspon amb l'ordre d'H.

Demostració. Hem de veure: 1. $K^{\mathrm{Gal}(K/M)} = M$. Això és automàtic a partir de la proposició i del Corol · lari 7.3. 2. $\mathrm{Gal}(K/K^H) = H$. Escrivim $M = K^H$. Ja sabem que K/M és de Galois, i $|\mathrm{Gal}(K/M)| = [K : M]$. A més, per definició tenim $H \leq \mathrm{Gal}(K/M)$. Hem de demostrar la igualtat: donat $\tau \in \mathrm{Gal}(K/M)$, veurem que $K = \bigcup_{\sigma \in H} \mathrm{Eq}(\sigma, \tau)$. Pel Lema 7.2, algun dels $\mathrm{Eq}(\sigma, \tau)$ ha de ser tot K, i això ens diu que $\tau \in H$. Per tant, només ens cal comprovar que per tot $\alpha \in K$, hi ha algun $\sigma \in H$ tal que $\sigma(\alpha) = \tau(\alpha)$. Considerem el polinomi

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \in K[x].$$

Fixem-nos que $\sigma(f) = f$ per tot $\sigma \in H$ i per tant $f(x) \in K^H[x] = M[x]$. Com que τ fixa M, tenim que $\tau(f) = f$. Però aleshores $\tau(\alpha)$ ha de ser una arrel de f, és a dir, $\tau(\alpha) = \sigma(\alpha)$ per algun $\sigma \in H$, com volíem. □

Hem vist que si $K/M/F$ és Galois aleshores K/M també ho és. Què podem dir de l'extensió M/F? ::: {.proposition} Sigui $K/M/F$ una torre amb K/F Galois, posem $G = \mathrm{Gal}(K/F)$. Aleshores són equivalents: 1. M/F és Galois. 2. $H = \mathrm{Gal}(K/M)$ és un subgrup normal de G. 3. $\sigma(M) \subseteq M$ per a tot $\sigma \in G$.

En aquest cas, $\mathrm{Gal}(M/F) \cong G/H$. ::: ::: {.proof} Sigui $H = \mathrm{Gal}(K/M)$. 1 $\implies$ 2: Sigui $\sigma \in G$. Si $\alpha \in M$ té polinomi mínim $f(x) \in F[x]$, aleshores σ en permuta les seves arrels i, en particular, \$ ( ) M. Per tant σ restringeix a un morfisme de M, que ja hem vist que és un automorfisme. Hem construit doncs una aplicació $G \to H$, i és fàcil comprovar que és un morfisme de grups. El seu nucli és doncs un subgrup normal, format per aquells automorfismes $\sigma \in G$ que fixen M, és a dir, és justament $\mathrm{Gal}(K/M)$.

2 $\implies$ 3: Sigui $\sigma \in G$. Per definició, $\sigma(M) \in K^{\tilde{H}}$, on $\tilde{H} = \sigma H \sigma^{-1}$. Com que H és normal $\tilde{H} = H$ i $K^{\tilde{H}} = K^H = M$.

3 $\implies$ 1: escrivim $M = F(\alpha_1, \dots \alpha_n)$, i considerem

$$B = \{\sigma(\alpha_i) \mid \sigma \in G, i = 1, \dots, n\}.$$

Aleshores $f(x) = \prod_{\beta in B}(x - \beta)$ és un polinomi separable amb coeficients a F. La hipòtesi és que $B \subseteq M$ i, per tant, M és el cos de descomposició de f. :::

Per acabar d'entendre bé la correspondència de Galois, relacionem operacions conegudes entre cossos i entre grups. ::: {.proposition name=" "} Sigui K/F Galois amb $G = \mathrm{Gal}(K/F)$. Sigui M_1 i M_2 dues subextensions, amb $H_i = \mathrm{Gal}(K/M_i)$. Aleshores:

1. $\mathrm{Gal}(K/M_1M_2) = H_1 \cap H_2$, i
2. $\mathrm{Gal}(K/(M_1 \cap M_2)) = \langle H_1, H_2 \rangle$. ::: ::: {.proof} Directa, per definició. :::

Podem resumir tot l'episodi en un sol resultat:

Teorema 8.2 (Teorema fonamental de la teoria de Galois). Sigui K/F una extensió de Galois finita amb grup de Galois G. Hi ha una bijecció entre

$$\{\text{subcossos } K/M/F\} \overset{1:1}{\longleftrightarrow} \{subgrups H \leq G\}$$

donada per \$M $H = \mathrm{Gal}(K/M)$ i $H \mapsto M = K^H$ que satisfà:

1. (gira les inclusions) $M_1 \subseteq M_2$ si i només si $H_2 \leq H_1$.
2. (preserva els graus) $[K : M] = |H|$ i $[M : F] = [G : H]$.
3. (preserva normalitat) M/F és Galois si i només si H és normal en G.
4. (gira els reticles) $M_1M_2 \leftrightarrow H_1 \cap H_2$ i $M_1 \cap M_2 \leftrightarrow \langle H_1, H_2 \rangle$.

Exemple 8.1. Calculem alguns exemples, com $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, el cos de descomposició de $\sqrt[3]{2}$, $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, o el cos de descomposició de $\mathbb{Q}(\sqrt[8]{2}, \zeta_8)$ de $\sqrt[8]{2}$. És important adonar-se que no n'hi ha prou en assignar valors als generadors d'una extensió per definir un automorfisme, ja que hi pot haver relacions amagades entre els generadors. Per exemple, si $\theta = \sqrt[8]{2}$, tenim $\theta^4 = \zeta_8 + \zeta_8^{-1}$ i per tant no totes les tries $\theta \mapsto \theta\zeta_8^i$ i $\zeta_8 \mapsto \theta_8^j$ amb j senar donen lloc a automorfismes.

Episodi 9

Cossos Finits

Aplicarem el teorema fonamental de la teoria de Galois a l'estudi complet des cossos finits i les seves extensions. Sabem que per cada potència de primer p^n hi ha un únic cos amb p^n elements, que anomenem $\mathbb{F}_{p^n}$.

9.1 Grup de Galois

Ja vam definir $\mathbb{F}_{p^n}$ com el cos de descomposició del polinomi $x^{p^n} - x \in \mathbb{F}_p[x]$. Per tant, l'extensió $\mathbb{F}_{p^n}/\mathbb{F}_p$ és de Galois.

Lema 9.1. El grup $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ és cíclic d'ordre n, generat per l'automorfisme de Frobenius

$$\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad \alpha \mapsto \sigma(\alpha) = \alpha^p.$$

Demostració. Fixem-nos que σ és un automorfisme, perquè és un endomorfisme injectiu d'un grup finit. També tenim $\sigma^i(x) = x^{p^i}$, i per tant σ té ordre n a $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Com que l'ordre d'aquest grup és $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$, obtenim el resultat. □

9.2 Subcossos

El teorema fonamental ens diu que els subcossos de $\mathbb{F}_{p^n}$ estan en correspondència amb els subgrups de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle$. Sabem de teoria de grups que per cada divisor $d \mid n$ hi ha exactament un subgrup d'índex d, que és el generat per σ^d. A més, tots els subgrups són normals (perquè és un grup abelià). Per tant, tenim:

Proposició 9.1. Si $d \mid n$, aleshores $\mathbb{F}_{p^d}$ és un subcos de $\mathbb{F}_{p^n}$. Recíprocament, si $\mathbb{F} \subseteq \mathbb{F}_{p^n}$ és un subcos, és de Galois, i $\mathbb{F} \cong \mathbb{F}_{p^d}$ amb $d \mid n$.

Vegem una aplicació fàcil d'aquest resultat: ::: {.corollary} El polinomi irreductible $\Phi_8(x) = x^4 + 1 \in \mathbb{Z}[x]$ és reductible mòdul qualsevol primer p. ::: ::: {.proof} Per $p = 2$, tenim $x^4+1 = (x+1)^4$. Suposem ara p senar. Com que $8 \mid p^2-1$ (mirem els quadrats senars mòdul 8), tenim que $x^8-1 = (x^4-1)(x^4+1)$ divideix a $x^{p^2-1} - 1$ a $\mathbb{Z}[x]$. Per tant, $x^4 + 1$ divideix també a $x^{p^2} - x$. Això vol dir que les arrels de $x^4 + 1$ viuen totes a $\mathbb{F}_{p^2}$. Però si fos irreductible, generaria una extensió de grau 4, contradicció. :::

9.3 Polinomis irreductibles

Ja hem vist que tota extensió de Galois és simple. Obtenim, per tant:

Proposició 9.2. L'extensió $\mathbb{F}_{p^n}/\mathbb{F}_p$ és simple. Equivalentment, per cada $n \geq 1$ existeix un polinomi $f(x) \in \mathbb{F}_p[x]$ irreductible de grau n.

Proposició 9.3. El polinomi $x^{p^n} - x$ és el producte de tots els polinomis irreductibles de grau d, per tots els $d \mid n$.

Demostració. Sigui $f(x)$ un polinomi irreductible de grau $d \mid n$. Aleshores l'extensió generada per f és de grau d sobre $\mathbb{F}_p$ i per tant és $\mathbb{F}_{p^d}$. Per tant, $f(x)$ és un divisor de $x^{p^d} - x$, que al seu torn divideix $x^{p^n} - x$.

Recíprocament, suposem que $f(x)$ és un factor irreductible de $x^{p^n} - x$, podem de grau d. Aleshores l'extensió que genera és un subcos de $\mathbb{F}_{p^n}$ i, per tant, té grau $d \mid n$. □

Corol · lary 9.1. El nombre de polinomis irreductibles de grau n a $\mathbb{F}_p[x]$ és:

$$\Psi(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d},$$

on μ és la funció de Möbius.

Demostració. Comptant els graus dels polinomis de la proposició anterior, obtenim

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

El resultat s'obté aplicant la fórmula d'inversió de Möbius. □

La proposició anterior també ens permet de trobar polinomis irreductibles de manera recursiva. D'entrada, podem dividir pels polinomis irreductibles de graus $d \mid n$ amb $d \leq n$ per quedar-nos amb el producte dels polinomis irreductibles de grau n. Ens caldrà factoritzar-los per obtenir els factors irreductibles.

TODO: explicar l'algoritme de factorització de Berlekamp.

9.4 La clausura algebraica d'$\mathbb{F}_p$

Ja hem vist que $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ si i només si $d \mid n$. Per tant, donades dues extensions d'$\mathbb{F}_p$ com ara $\mathbb{F}_{p^n}$ i $\mathbb{F}_{p^m}$, podem pensar-les dins de $\mathbb{F}_{p^{nm}}$. Així, podem prendre la unió de totes elles i obtenir la clausura algebraica de manera explícita:

Proposició 9.4. Tenim

$$\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

Episodi 10

Element Primitiu

El primer objectiu és demostrar el teorema de l'element primitiu. Recordem que una extensió K/F és simple si hi ha algun $\alpha \in K$ tal que $K = F(\alpha)$.

Teorema 10.1 (caracterització d'extensions simples). Una extensió K/F és simple si i només si hi ha finites subextensions $K/M/F$.

Demostració. Suposem que $K = F(\alpha)F$ és simple, i sigui $f(x) = \mathrm{Irr}_{\alpha,F}(x)$. Considerem una subextensió $K/M/F$. Aleshores $g(x) = \mathrm{Irr}_{\alpha,M}(x)$ és un divisor de $f(x)$ pensats a $K[x]$. Sigui $M' \subseteq M$ l'extensió generada sobre F pels coeficients de $g(x)$. Com que $\mathrm{Irr}_{\alpha,M}(x) = \mathrm{Irr}_{\alpha,M'}(x)$, tenim $[K : M] = [K : M']$ i per tant $M = M'$. En conclusió, els subcossos M estan generats per coeficients dels factors irreductibles de $f(x)$ pensat com a polinomi a $K[x]$ i, per tant, n'hi ha un nombre finit.

Recíprocament, suposem que K/F té un nombre finit de subcossos. Gràcies a la Proposicó 7.2, hi ha algun $\alpha \in K$ que no pertany a cap dels subcossos de K. Per tant, $F(\alpha) = K$. □

10.1 El teorema de l'element primitiu

Amb aquesta caracterització i tot el què sabem fins ara podem demostrar fàcilment el teorema de l'element primitiu.

Teorema 10.2 (Element Primitiu). Si una extensió K/F és finita i separable, aleshores existeix $\gamma \in K$ tal que $K = F(\gamma)$.

Demostració. Sigui L/K una extensió tal que L/F sigui Galois. Per exemple, podem prendre el compositum de tots els cossos de descomposició dels polinomis mínims d'un conjunt de generadors de K/F. Aleshores L/F és primitiva i, pel criteri anterior, hi ha un nombre finit de subcossos de L. En particular, hi ha un nombre finit de subcossos de K i, un altre cop pel criteri anterior, l'extensió K/F és primitiva. □

Podem generalitzar una mica aquest teorema:

Teorema 10.3. Suposem que $K = F(\alpha, \beta)$ i β és separable sobre F. Aleshores existeix $\gamma \in K$ tal que $K = F(\gamma)$.

Demostració. Si F és un cos finit, aleshores $F(\alpha, \beta)$ també és un cos finit i per tant sabem que és simple. Suposem doncs que F és infinit, i escrivim $f(x)$ i $g(x)$ pels polinomis mínims d'α i β, respectivament.

Sigui $L/F(\alpha,\beta)$ un cos de descomposició per $f(x)g(x)$, i escrivim $\alpha=\alpha_1,\alpha_2,\dots\alpha_r$ per les arrels de $f(x)$ a L i $\beta=\beta_1,\beta_2,\dots,\beta_s$ per les arrels de $g(x)$ a L. Per cada i i per cada $j\neq 1$, l'equació

$$\alpha_i+X\beta_j=\alpha+X\beta_j$$

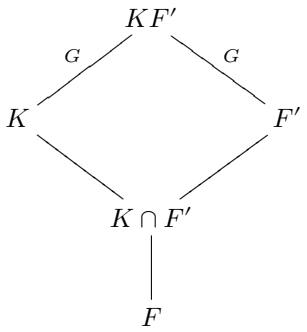
només té la solució $X=\frac{\alpha_i-\alpha}{\beta-\beta_j}$ (el denominador no és zero perquè $g(x)$ és separable). Per tant, com que F és infinit podem prendre $t\in F$ que no sigui cap de les solucions anteriors, i definim $\gamma=\alpha+t\beta$. Veurem que $F(\alpha,\beta)=F(\gamma)$. N'hi ha prou amb veure que $\beta\in F(\gamma)$, perquè aleshores $\alpha=\gamma-t\beta$ també hi serà. Considerem els polinomis a $g(x)$ i $h(x)=f(\gamma-tx)$ a $F(\gamma)$. Observem que $g(\beta)=0$ i $h(\beta)=f(\gamma-t\beta)=f(\alpha)=0$. Però les altres arrels de $g(x)$ són les β_j amb $j>1$, i $h(\beta_j)\neq 0$ en aquest cas. Per tant, $\mathrm{mcd}(g(x),h(x))=(x-\beta)$ i en deduim que $\beta\in F(\gamma)$, com volíem. □

10.2 Galois i compositum d'extensions

Estudiem ara com es comporta la propietat de ser Galois quan prenem compositums.

Suposem que tenim extensions K/F i F'/F.

Proposició 10.1. Si K/F és de Galois, aleshores KF' és de Galois sobre F' i la restricció indueix un isomorfisme $\mathrm{Gal}(KF'/F')\cong\mathrm{Gal}(K/K\cap F')$:



En particular, si F'/F és finita, aleshores

$$[KF':F]=\frac{[K:F][F':F]}{[K\cap F':F]}.$$

Demostració. Sabem que K és el cos de descomposició d'un polinomi separable $f(x)\in F[x]$. Aleshores, KF' és el cos de descomposició del mateix polinomi $f(x)$ ara pensat com a polinomi a $F'[x]$. Considerem ara el morfisme restricció

$$\varphi\colon\ \mathrm{Gal}(KF'/F')\to\mathrm{Gal}(K/F).$$

Està ben definit: donat $\sigma\in\mathrm{Gal}(KF'/F')$, com que F és un subcos de F' també fixa els elements de F, i per tant la seva restricció a K dona lloc a un element de $\mathrm{Gal}(K/F)$. Calcularem el nucli i la imatge de φ.

Si $\sigma\in\mathrm{Gal}(KF'/F')$, i suposem que $\sigma|_K=1$, vol dir que σ fixa K. Com que també fixava F', fixa tot KF' i per tant és la identitat a $\mathrm{Gal}(KF'/F')$. Així doncs, φ és injectiva.

Sigui $H=\mathrm{Im}(\varphi)\leq\mathrm{Gal}(K/F)$ la imatge, i sigui $M=K^H$ el seu subcos fix. Volem veure que $M=K\cap F'$, i això ens donarà el resultat gràcies a la correspondència de Galois. Si $\sigma\in H$, aleshores σ fixa F'. Per tant, $K\cap F'\subseteq M$. D'altra banda, el compositum MF' és fix per tot $\sigma\in\mathrm{Gal}(KF'/F')$, ja que aquest σ fixa els elements de F' i en els elements de K hi actua via la restricció. Pel teorema fonamental, $MF'=F'$ i, per tant $M\subseteq F'$, d'on en traiem $K\cap F'=M$.

La fórmula final s'obté comptant graus d'extensions. □

Remarca. Considerem $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ (el nostre prototipus d'extensió no normal) i $F' = \mathbb{Q}(\zeta_3\sqrt[3]{2})$, on ζ_3 és una arrel cúbica primitiva de la unitat. Tenim $[K\colon F] = [F'\colon F] = 3$, i $KF' = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ té grau 6, per tant la igualtat no és certa si cap de les extensions inicials és de Galois.

Estudiem ara el cas on les dues extensions inicials són de Galois.

Proposició 10.2. Siguin K_1/F i K_2/F dues extensions de Galois amb grups G_1 i G_2. Aleshores K_1K_2/F i $K_1 \cap K_2/F$ són Galois, i la restricció a K_1 i a K_2 indueix un isomorfisme

$$\mathrm{Gal}(K_1K_2/F) \cong H = \{(\sigma, \tau) \in G_1 \times G_2 \mid \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\}.$$

En particular, si $K_1 \cap K_2 = F$, aleshores

$$\mathrm{Gal}(K_1K_2/F) \cong G_1 \times G_2.$$

Demostració. Suposem que K_i és el cos de descomposició del polinomi separable $f_i(x) \in F[x]$. Aleshores K_1K_2 és el cos de descomposició de la part lliure de quadrats de $f_1(x)f_2(x)$ i per tant K_1K_2 és Galois sobre F. Sigui ara $f(x)$ un polinomi irreductible a $F[x]$ amb una arrel a $K_1 \cap K_2$. Aleshores totes les arrels de $f(x)$ són a K_1 i també a K_2 i, per tant, a $K_1 \cap K_2$. Per tant, $K_1 \cap K_2$ és Galois.

Considerem ara l'aplicació

$$\varphi\colon \mathrm{Gal}(K_1K_2/F) \to G_1 \times G_2, \quad \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2}).$$

És clarament injectiva, i per tant només ens cal estudiar la imatge. Clarament està continguda dins d'H, i per tant n'hi ha prou amb calcular els ordres. Pel primer teorema d'isomorfisme,

$$|\operatorname{Im}(\varphi)| = |\mathrm{Gal}(K_1K_2/F)| = [K_1K_2\colon F].$$

D'altra banda, fixem-nos que per cada $\sigma \in \mathrm{Gal}(K_1/F)$ hi ha $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ elements $\tau \in \mathrm{Gal}(K_2/K_1 \cap K_2)$ que satisfan $(\sigma, \tau) \in H$. Per tant:

$$|H| = |G_1||\mathrm{Gal}(K_2/K_1 \cap K_2)| = |G_1|\frac{|G_2|}{\mathrm{Gal}(K_1 \cap K_2/F)}$$

i la fórmula de la proposició anterior ens demostra $|H| = |\operatorname{Im}(\varphi)|$. □

Podem demostrar un cert recíproc: ::: {.proposition} Suposem que K/F és una extensió de Galois, i $G = \mathrm{Gal}(K/F) = G_1 \times G_2$. Aleshores K és el compositum de dues extensions de Galois K_1/F i K_2/F amb $K_1 \cap K_2 = F$ i grups de Galois G_1 i G_2, respectivament. ::: ::: {.proof} Definim $K_1 = K^{G_1}$ i $K_2 = K^{G_2}$. Aleshores $K_1 \cap K_2$ correspon a $\langle G_1, G_2\rangle = G$, per tant $K_1 \cap K_2 = F$. El compositum correspon amb $G_1 \cap G_2 = 1$, i per tant $K_1K_2 = K$. :::

Corol · lary 10.1 (clausura de Galois). Sigui K/F una extensió finita separable. Aleshores hi ha una extensió $E/K/F$ tal que E/F és Galois$, i és mínima en el sentit que si E'/K és una extensió amb E'/F Galois, tenim $E \subseteq E'$. Aquesta extensió s'anomena la clausura de Galois de K/F.

Demostració. Ja sabem que hi ha extensions de K que són Galois (prenem el cos de descomposició dels polinomis mínims d'un conjunt de generadors de K). El cos E buscat és llavors la intersecció de totes les extensions E'/K tals que E'/F és Galois. Hem vist que aquesta intersecció serà Galois. □

Episodi 11

Extensions Abelianes i ciclotòmiques

En aquest apartat estudiem les extensions ciclotòmiques, i veiem que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ és canònicament isomorf a $(\mathbb{Z}/n\mathbb{Z})^\times$. Com a aplicació, veurem com construir polígons regulars amb regle i compàs. Veurem que només és possible per polígons regulars de n costats quan φn és una potència de 2. Això passa si i només si n és producte d'una potència de dos i de primers de Fermat diferents.

11.1 Grup de Galois dels cossos ciclotòmics

Sigui $n \geq 2$ i considerem el cos ciclotòmic $\mathbb{Q}(\zeta_n)$. Volem estudiar $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Per cada $a \in \mathbb{Z}$ coprimer amb n, definim l'aplicació

$$\sigma_a \colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n), \quad \zeta_n \mapsto \zeta_n^a.$$

Teorema 11.1. L'aplicació $a \mapsto \sigma_a$ indueix un isomorfisme

$$\psi \colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Demostració. Ja sabem que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ té exactament $\varphi(n)$ elements. Si σ és un d'aquests automorfismes, sabem que ve determinat per on envia ζ_n, que és una arrel del polinomi ciclotòmic $\Phi_n(x)$. Per tant, $\sigma(\zeta_n)$ és una arrel n-èssima primitiva de la unitat i doncs ha de ser ζ_n^a per alguna a coprimera amb n. Així veiem que $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ i ψ és una aplicació ben definida i a més exhaustiva, per tant bijectiva. A més, ψ és un morfisme de grups, ja que

$$(\sigma_a\sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^b)^a = \zeta_n^{ab} = \sigma_{ab}(\zeta_n).$$

□

Fixem-nos que en particular tenim exemples d'extensions cícliques de grau $p-1$ per qualsevol primer p. També tenim una versió més conceptual del teorema xinès dels residus, que escrivim en el cas de dos factors per estalviar notació.

Proposició 11.1. Si n i m són coprimers, aleshores $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$, $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$, i

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}).$$

Demostració. TODO □

El següent lema ens permet trobar generadors dels subcossos de $\mathbb{Q}(\zeta_p)$.

Lema 11.1. Sigui p un primer, i sigui $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ un subgrup. Aleshores

$$\theta_H = \sum_{\sigma \in H} \sigma(\zeta_p)$$

és un generador del cos fix d'H. L'element θ_H s'anomena un període de ζ_p.

Exemple 11.1. Calcularem el reticle de subcossos de $\mathbb{Q}(\zeta_{13})$, fent servir el lema anterior. TODO

11.2 Extensions abelianes

Podem fer servir el què hem vist per demostrar el següent resultat.

Teorema 11.2 (realització de grups abelians). Sigui G un grup finit abelià. Aleshores hi ha una extensió $K/\mathbb{Q}$ continguda dins d'un cos ciclotòmic tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

Demostració. Tot grup abelià és producte de cíclics:

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}.$$

Existeixen primers diferents p_1, p_2, ...p_k tals que $p_i \equiv 1 \pmod{n_i}$. Aquest fet es dedueix del fet que hi ha infinits primers $\equiv 1 \pmod{m}$ per qualsevol m (TODO).

Considerem $n = p_1 p_2 \cdots p_k$. Aleshores, tenim

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/(p_1-1))^\times \times (\mathbb{Z}/(p_2-1))^\times \times \cdots \times (\mathbb{Z}/(p_k-1))^\times.$$

Com que n_i divideix $p_i - 1$, hi ha un subgrup $H_i \leq C_{p_i-1}$ d'índex n_i per cada i, i el quocient per $H_1 \times H_2 \times \cdots \times H_k$ és isomorf a G. Per la correspondència de Galois, hi ha un subcos de $\mathbb{Q}(\zeta_n)$ que realitza G. □

Els cossos ciclotòmics són exemples d'extensions de Galois amb grup abelià. En general, una extensió K/F es diu que té la propietat P si és de Galois i el seu grup de Galois té la propietat P. Per exemple, tenim la següent definició:

Definició 11.1 (extensió abeliana). Una extensió K/F és abeliana si K/F és de Galois i $\mathrm{Gal}(K/F)$ és un grup abelià.

El resultat anterior té un recíproc que no podem demostrar aquí:

Teorema 11.3 (Kronecker-Weber). Sigui $K/\mathbb{Q}$ una extensió finita abeliana. Aleshores K està contingut en una extensió ciclotòmica.

En general, és avui un problema obert el determinar quins grups apareixen quan com a grups de Galois d'extensions $K/\mathbb{Q}$. Ja hem vist que tots els grups abelians apareixen, però hi ha grups (per exemple $\mathrm{PSL}_2(\mathbb{F}_{125})$) pels quals no s'ha demostrat encara que hi apareguin. Aquest problema s'anomena el problema invers de la teoria de Galois.

11.3 Constructibilitat de polígons regulars

Com a aplicació dels cossos ciclotòmics, estudiarem quins polígons regulars es poden construir amb regle i compàs. Ja hem vist que un nombre real α és construible si i només si $\mathbb{Q}(\alpha)$ està contingut en un cos K obtingut a partir de $\mathbb{Q}$ a partir d'un nombre finit d'extensions quadràtiques.

Construir un polígon de n costats és equivalent a construir les arrels n-èssimes de la unitat ζ_n, que al seu torn és equivalent a construir la seva part real $x = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$. Com que $\zeta_n^2 - 2x\zeta_n + 1 = 0$, el cos $\mathbb{Q}(zeta_n)$ és una extensió de grau 2 sobre $\mathbb{Q}(x)$ (aquesta última és real, mentre que $\mathbb{Q}(\zeta_n)$ no). Per tant, si volem que el cos $\mathbb{Q}(x)$ estigui dins de K ens cal en particular que el seu ordre $\varphi(n)/2$ sigui potència de 2, és a dir, que $\varphi(n)$ sigui potència de 2.

Recíprocament, si $\varphi(n)$ és una potència de 2, aleshores $\mathbb{Q}(x)$ té ordre una potència de 2. Prenent successivament subgrups d'índex 2 i fent servir la correspondència de Galois, obtenim una successió

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m = \mathbb{Q}(x), \quad [K_i \colon K_{i-1}] = 2,$$

i per tant x és constructible. D'aquí tenim la següent caracterització. Recordem que un primer p es diu primer de Fermat si $p - 1$ és una potència de 2.

Teorema 11.4 (construcció de polígons regulars). Sigui n un enter positiu. Aleshores el polígon regular de n costats és constructible amb regle i compàs si i només si n és de la forma

$$n = 2^k p_1 \cdots p_r,$$

on $k \geq 0$ i p_i són primers de Fermat diferents.

Demostració. Escrivim n com a producte de potències de primers diferents

$$n = 2^k q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}, \quad q_i \text{ senar.}$$

Aleshores tenim la fórmula coneguda

$$\varphi(n) = 2^{k-1} \prod_{i=1}^{r} (q_i - 1) q_i^{e_i - 1}.$$

Ja veiem que cal que $e_i = 1$ per tot i si volem que $\varphi(n)$ sigui potència de 2. A més, cal que $q_i - 1$ sigui potència de 2 per a tot i, és a dir que q_i sigui un primer de Fermat. □

Només es coneixen cinc primers de Fermat: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. En general, si p és un primer de Fermat aleshores $p = 2^{2^i} + 1$ per algun $i \geq 0$. Els nombres $F_i = 2^{2^i} + 1$ s'anomenen nombres de Fermat. Sembla poc probable que hi hagi infinits primers de Fermat, però és encara un problema obert.

La següent expressió dona (en principi) una manera de construir un 17-gon regular amb regle i compàs.

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}\right) + \frac{1}{8}\left(\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right).$$

Episodi 12

Arrels i radicals

Definirem què vol dir que un polinomi sigui resoluble per radicals, i veurem que és equivalent a què el seu grup de Galois sigui resoluble. D'aquí en podrem deduir que els polinomis generals de grau ≥ 5 no són resolubles per radicals i, per tant, no existeix una fórmula que expressi les arrels d'un polinomi en termes dels seus coeficients. També es mostrarà un exemple concret d'un polinomi de grau 5 sobre $\mathbb{Q}$ amb grup de Galois S_5.

Proposició 12.1. Sigui $f(x) \in \mathbb{Q}[x]$ un polinomi irreductible de grau p amb exactament $p-2$ arrels reals. Aleshores $\mathrm{Gal}(f) \cong S_p$.

Demostració. TODO □

Podem aplicar el resultat anterior al polinomi $f(x) = x^5 - 4x - 2$. Com que és 2-Eisenstein, és irreductible. A més, la seva derivada és $5x^4 - 4$, que té zeros a $x = \pm\frac{\sqrt{2}}{\sqrt[4]{5}}$. Deduïm que $f(x)$ té exactament tres zeros reals, que de fet podem aproximar: $-1.24359639\ldots, -0.50849948\ldots, 1.51851215\ldots$. Per tant, $\mathrm{Gal}(f) \cong S_5$.

Episodi 13

Calculem grups de Galois

Bibliografia

[1] Michael. Artin. Algebra / Michael Artin. eng. 2nd ed., new international ed. Edinbourgh Gate, Harlow, Essex: Pearson, 2014. ISBN: 978-1-292-02766-1.

[2] David S. Dummit i Richard M. Foote. Abstract algebra. 3rd ed. New York: Wiley, 2004.

[3] Meinolf Geck. "On the characterization of Galois extensions". A: Amer. Math. Monthly 121.7 (2014), pàg. 637 - 639. ISSN: 0002-9890. DOI: 10.4169/amer.math.monthly.121.07.637. URL: https://doi.org/10.4169/amer.math.monthly.121.07.637.

[4] Zbigniew Jelonek. "A simple proof of the existence of the algebraic closure of a field". A: Univ. Iagel. Acta Math. 30 (1993), pàg. 131 - 132. ISSN: 0083-4386.

[5] Joseph J. Rotman. Advanced modern algebra. Part 1. Third. Vol. 165. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2015, pàg. xiv+706. ISBN: 978-1-4704-1554-9. DOI: 10.1090/gsm/165. URL: https://doi.org/10.1090/gsm/165.

[6] Steven H. Weintraub. "The theorem of the primitive element". A: Amer. Math. Monthly 128.8 (2021), pàg. 753 - 754. ISSN: 0002-9890. DOI: 10.1080/00029890.2021.1944757. URL: https://doi.org/10.1080/00029890.2021.1944757.