Teoria de Galois

Marc Masdeu

2023-01-28

Índex

Capítol 1

Pilot: Galois entre els radicals

Parlem de les equacions polinomials en una variable, la famosa fórmula quadràtica i els monstres de grau tres i quatre.

En aquests casos, les solucions es poden expressar en termes de les quatre operacions bàsiques a més de l'extracció d'arrels.

Seguidament, estudiem el polinomi $x^3 - 2$, que té una arrel real i dues de complexes. Les podem dibuixar al pla, formen un triangle equilàter. Aquest triangle té un grup de simetries, que és el grup diedral $D_{2\times 3}$ que ja s'ha estudiat a l'assignatura Estructures Algebraiques. D'altra banda, podem introduir el subcòs de $\mathbb{C}$ anomenat $\mathbb{Q}(\alpha, \omega)$ on $\alpha = \sqrt[3]{2}$ i $\omega = e^{2\pi i/3}$ és una arrel cúbica primitiva de la unitat. Aquest és el mínim cos que conté totes les arrels del nostre polinomi (exercici). Ara podem definir les "simetries" d'aquest cos com el grup dels automorfismes (morfismes de cossos que són invertibles, encara que aquesta segona condició serà bastant supèrflua).

Seguidament, canviem el polinomi d'estudi a $x^5 - 2$. Aquí hi ha 10 simetries geomètriques, però en canvi hi ha moltes més "simetries" com a cos de les arrels. En aquest cas, en tenim 20 (en general, si p és un primer, $x^p - 2$ té $p(p-1)$ simetries en les arrels, però només $2p$ simetries geomètriques.

L'objectiu de la Teoria de Galois és estudiar aquest nou grup de simetries, que ens dona molta informació sobre les arrels. En particular, aquest grup ens determina la resolubilitat per radicals del polinomi en qüestió.

Capítol 2

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.

Capítol 3

Les Torres

L'objectiu és estudiar torres d'extensions, i com es comporta el grau en torres finits. Veurem aplicacions que té aquesta fórmula, com ara el càlcul del grau de la composició d'extensions.

Capítol 4

Extensions algebraiques

Parlarem d'elements algebraics i el seu polinomi mínim. Veurem que el cos generat per un element algebraic és isomorf al quocient de l'anell de polinomis pel seu polinomi mínim. Veurem la relació entre extensions algebraiques i extensions finites.

Capítol 5

Regle i compàs

Definirem els nombres construibles amb regla i compàs, i els caracteritzarem.

Aleshores veurem la impossibilitat de la duplicació del cub, la trisecció de l'angle i la quadratura del cercle (aquest últim, assumint la transcendència de π, que no demostrarem).

Capítol 6

La clausura algebraica d'un cos

Definirem la noció de cos algebraicament tancat. Direm que $\mathbb{C}$ ho és, encara que deixarem la demostració més endavant (com a aplicació del teorema fonamental de la TG). Definirem la clausura algebraica d'un cos, i en demostrarem l'existència (si acceptem l'axioma de l'elecció) i unicitat.

Així, podrem pensar les extensions algebraiques com a contingudes a una clausura fixada (si cal).

Capítol 7

Cossos de descomposició

El cos de descomposició d'un polinomi juga un paper destacat al llarg del curs. Aquí els definirem, i en demostrarem l'existència i unicitat (llevat d'isomorfisme). També enunciarem i demostrarem el teorema de l'extensió, que ens permet estendre isomorfismes de cossos a extensions que siguin clausura de Galois d'un polinomi. 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.

Capítol 8

Grups simples, grups resolubles

Aquesta sessió no parla de teoria de cossos, sinó de grups. Això ens cal ja que el teorema fonamental ens relaciona les dues teories. Introduïrem la noció de resolubilitat d'un grup, parlarem dels grups simples i veurem que el grup alternat A_n no és simple per a tot $n \geq 5$. Això implica que S_n no és resoluble per $n \geq 5$.

Capítol 9

Simetries

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.

Capítol 10

La independència (dels caràcters)

En aquesta secció demostrarem un resultat d'àlgebra lineal necessari per la demostració del teorema fonamental de la TG.

Definició 10.1. Un *caràcter* χ d'un grup G amb valors en un cos L és un morfisme de grups

$$\chi\colon G \to L^\times.$$

Podem pensar un caràcter χ com una funció $G \to L$. Les funcions de G a L formen un L-espai vectorial, de manera òbvia.

Teorema 10.1 (Independència lineal dels caràcters)**.** *Siguin $\chi_1, \dots, \chi_n$ caràcters de G diferents. Aleshores són linealment independents, és a dir, no hi ha cap combinació lineal no trivial $a_1\chi_1 + \cdots + a_n\chi_n$ que doni lloc a la funció idènticament zero.*

Demostració. Suposem (reordenant, si cal) que podem escriure

$$a_1\chi_1 + \cdots a_m\chi_m = 0,$$

amb tots els $a_i \neq 0$ (observem $m \leq n$) i amb m mínim. Obtindrem una relació de dependència amb menys termes, arribant així a contradicció.

Prenem $g_0 \in G$ tal que $\chi_1(g_0) \neq \chi_m(g_0)$. Aleshores tenim

$$a_1\chi_1(g) + \cdots a_m\chi_m(g) = 0,$$

i

$$a_1\chi_1(g_0g) + \cdots a_m\chi_m(g_0g) = 0.$$

Multiplicant la primera equació per $\chi_m(g_0)$ i restant-li la segona obtenim, per a tot g,

$$a_1(\chi_m(g_0) - \chi_1(g_0))\chi_1(g) + \cdots a_{m-1}(\chi_m(g_0) - \chi_{m-1}(g_0))\chi_{m-1}(g) = 0.$$

Com que el primer coeficient és diferent de zero, tenim una relació no trivial amb $m-1$ termes, contradicció. □

Un cas particular que ens interessa aquí prové de consirar un morfisme no trivial de cossos $\sigma\colon K \to L$, que indueix un morfisme de grups entre les unitats $\sigma\colon K^\times \to L^\times$ (aquesta restricció ja conté tota la informació que ens cal de σ, perquè ja sabem que $\sigma(0) = 0$). Aleshores σ esdevé un caràcter del grup $G = K^\times$, i per tant tenim el següent:

Corol · lary 10.1. *Si $\sigma_1, \dots, \sigma_n$ són morfismes diferents de K a L, aleshores són linealment independents com a funcions de K.*

Un cas encara més particular d'aquest corol · lari ens permet demostrar una relació numèrica bàsica entre automorfismes d'un cos i els cossos que deixen fixes.

Proposició 10.1. *Sigui S un subconjunt finit d'automorfismes d'un cos K, i sigui $F = K^G$ el seu cos fix. Aleshores*

$$[K : F] \geq |S|.$$

Demostració. TODO □

Teorema 10.2. *Sigui G un subgrup finit d'automorfismes d'un cos K, i sigui $F = K^G$ el seu cos fix. Aleshores*

$$[K : F] = |G|.$$

Demostració. Només ens cal veure que $[K : F] \leq |G|$, ja que l'altra desigualtat ja l'hem demostrat independentment del fet que G sigui un grup.

TODO (llarga) □

D'aquest resultat se'n desprenen fàcilment conseqüències molt importants que val la pena destacar.

Corol · lary 10.2. *Si K/F és una extensió finita, aleshores*

$$|\operatorname{Aut}(K/F)| \leq [K : F],$$

amb igualtat si i només si F és el cos fix d'$\operatorname{Aut}(K/F)$.

Dit d'altra manera, l'extensió K/F és Galois si i només si $F = K^{\operatorname{Aut}(K/F)}$.

Demostració. TODO. □

Capítol 11

El Teorema Fonamental

Enunciem i demostrem el teorema fonamental de la teoria de Galois. Farem servir la independència lineal dels caràcters (que tmabé demostrarem). Després veurem que si L/F és una extensió finita i H un subgrup de $\mathrm{Aut}(L/F)$, aleshores $[L\colon FH] = |H|$. Aquest fet, fonamental, ens permet també caracteritzar les extensions de Galois com aquelles que són normals i separables.

Aleshores ja estarem en posició d'enunciar i demostrar el teorema fonamental. Acabarem amb diversos exemples concrets d'extensions, il · lustrant la correspondència de Galois.

Capítol 12

És més fàcil dibuixar un 17-gon que un heptàgon?

En aquest apartat estudiem les extensions ciclotòmiques, i veiem que $\mathrm{Gal}(\mathbb{Q}(\zeta_n))$ 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.

Capítol 13

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: si f és irreductible amb exactament 3 arrels reals, aleshores la conjugació complexa dona un automorfisme d'ordre 2. Com que $\mathrm{Gal}(f)$ té ordre divisible per 5, hi ha algun element σ d'ordre 5 (Teorema de Cauchy). Però a S_5 els elements d'ordre 5 són necessàriament 5-cicles. Com que $\mathrm{Gal}(f)$ té un 5-cicle i una transposició, és necessàriament tot S_5.

Capítol 14

Teoria de Galois infinita

Farem un esbós de com cal modificar els enunciats per adaptar el teorema fonamental de la Teoria de Galois a extensions infinites.

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.

Pensem que en un curs com aquest hi ha idees molt importants que cal transmetre el més efectivament possible. També hi ha idees menys importants que poden obfuscar aquestes idees fonamentals, de manera que optaré per fer la teoria amb algunes hipòtesis simplificadores. Les classes de problemes introduiran exercicis amb més generalitat.

Així, assumirem que tots els anells que apareixen són unitaris i commutatius, que tots els anells són dominis d'ideals principals (bàsicament tractarem amb els anells de polinomis sobre un cos). Encara que parlarem d'(in)separabilitat, la majoria d'exemples estaran basats o bé en extensions dels racionals o de cossos finits.

Bibliografia

Artin, M. (2014). *Algebra / Michael Artin.* Pearson, Edinbourgh Gate, Harlow, Essex, 2nd ed., new international ed. edition.

Dummit, D. S. and Foote, R. M. (2004). *Abstract algebra.* Wiley, New York, 3rd ed edition.