Teoria de Galois

Marc Masdeu

2023-02-01

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.

Capítol 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 $\mathrm{char}(A)$.

Fixem-nos que si $\mathrm{char}(A) = n$, 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 $\mathrm{char}(F) = n > 0$, 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 (adjunció d'arrels). Sigui $p(x) \in F[x]$ un polinomi irreductible. Aleshores existeix una extensió K/F tal que K té una arrel de $p(x)$.

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!). De fet, ens dona una base de K com a F-espai vectorial.

Teorema 1.2. Sigui $p(x) \in F[x]$ un polinomi irreductible de grau n, i sigui $K = F[x]/(p(x))$. 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 $F(\alpha_1, \dots, \alpha_n)$. 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 $p(x) \in F[x]$ un polinomi irreductible, i suposem que K/F és una extensió que conté una arrel α de $p(x)$. Aleshores hi ha un isomorfisme

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

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:

Teorema 1.4 (extensió d'isomorfismes). Sigui $\varphi\colon F \to \tilde{F}$ un isomorfisme de cossos. Sigui $p(x) \in F[x]$ un polinomi irreductible, i sigui $\tilde{p}(x)$ el polinomi resultant d'aplicar φ als coeficients de $p(x)$. Sigui α una arrel de $p(x)$ en alguna extensió de K, i sigui β una arrel de $\tilde{p}(x)$ en una extensió de $\tilde{F}$. Aleshores l'aplicació $\alpha \mapsto \beta$ indueix un isomorfisme de cossos

$$\Phi\colon F(\alpha) \cong \tilde{F}(\beta)$$

tal que $\Phi_{|F} = \varphi$:

$$\begin{array}{ccc} F(\alpha) & \xrightarrow[\cong]{\Phi} & \tilde{F}(\beta) \\ \Big| & & \Big| \\ F & \xrightarrow[\cong]{\varphi} & \tilde{F}. \end{array}$$

Capítol 2

Les Torres

Parlarem d'extensions simples, del teorema d'aixecament a anells de polinomis i el teorema de l'extensió. També 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

Capítol 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.

Capítol 4

Descomposició

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). Això ens permetrà (assumint el teorema fonamental de l'àlgebra, que demostrarem més endavant) pensar els elements algebraics sobre $\mathbb{Q}$ dins dels complexos.

Capítol 5

Polinomis Inseparables

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.

Capítol 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.

Capítol 7

Automorfismes

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 $n \geq 5$.

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 8

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.

8.1 La independència (dels caràcters)

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

Definició 8.1. 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 8.1 (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 8.1. Si $\sigma_1, \ldots, \sigma_n$ 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 8.1. Sigui S un subconjunt finit d'automorfismes d'un cos K, i sigui $F = K^G$ el seu cos fix. Aleshores

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

Demostració. TODO □

Teorema 8.2. Sigui G un subgrup finit d'automorfismes d'un cos K, i sigui $F = K^G$ el seu cos fix. Aleshores

$$[K\colon F] = |G|.$$

Demostració. Només ens cal veure que $[K\colon F] \leq |G|$, 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 8.2. 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 9

Cossos Finits

Capítol 10

L'element Primitiu

Capítol 11

Extensions Abelianes i ciclotòmiques

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 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: 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 13

Calculem grups de Galois

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.