MAT^2

MATerials MATemàtics
Volum 2012, treball no. 3, 30 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/matmat

Bicentenari d'un revolucionari: Évariste Galois

Pere Ara, Francesc Bars

1 Introducció

Durant l'any 2011 es va commemorà el bicentenari del naixement d'Évariste Galois (1811-1832), matemàtic francés que, tot i la seva curta vida, va revolucionar el món de l'Àlgebra.

A nivell internacional, tant l'Institut Henri Poincaré com el poble natal de Galois, Bourg-la-Reine, van organitzar diverses activitats per sumar-se a la commemoració. Igualment han anat apareixent diferents publicacions de l'obra i vida de Galois a França aprofitant aquest bicentenari, podeu consultar per exemple [3, 6, 9, 15, 20].

A casa nostra, pel bicentenari, s'ha organitzat una exposició a la Biblioteca de Ciencies i Enginyeries de la Universitat Autònoma de Barcelona, on els signants van col·laborar en la seva vessant més científica[1].

La vida personal i l'obra d'Évariste Galois ha estat icona de moltes generacions de matemàtics arreu del món. A part de molts documents escrits, hi trobem a la xarxa molts documents audiovisuals com per exemple un fragment dins de la pel·lícula "Nada es casualidad 3:19", producció hispanomexicana de l'any 2008, actualment a YouTube, o com es pot veure en la exposició de la Biblioteca de Ciencies i Enginyeries de la UAB esmentada anteriorment.

A Catalunya la figura de Galois també és una icona pels matemàtics catalans. Per exemple, a nivell institucional, la Societat Catalana de Matemàtiques convoca anualment un premi per a monografies en matemàtiques d'estudiants, aquest premi s'anomena *Premi Évariste Galois*. A nivell de

[1] http://www.bib.uab.cat/ciencies/expo/galois/

monografies escrites, hi ha l'excel·lent llibre de l'Antoni Malet "Obra d'Évariste Galois" [13], editat pel IEC l'any 1984. A nivell més lúdic i com a icona estudiantil comentem per exemple que els alumnes de Matemàtiques de la UB durant l'any 1992, sota la direcció de les llavors estudiants de Matemàtiques, Maria Alberich (actualment professora a la UPC) i Maite Naranjo (actualment investigadora al CRM), van organitzar una obra de teatre a la Universitat de Barcelona sobre la vida de Galois, la representació teatral portava per títol "Galouà se muà", i sembla ser que en un futur proper es penjarà al YouTube.

En l'escrit que presentem a continuació volem destacar certs aspectes de la vida i obra de Galois que han fet d'ell una icona mundial. Aquest escrit es basa majoritàriament en els textos que els autors van preparar per la citada exposició en la Biblioteca amb motiu del bicentenari del seu naixement.

En aquest document trobeu primerament una breu bibliografia personal d'Évariste Galois (§2). Després s'entra en una explicació divulgativa sobre diverses conseqüències del resultat clau de l'obra matemàtica d'Évariste Galois: no hi ha una fórmula per les arrels d'un polinomi de grau ≥ 5 per radicals (§3), possibilita o impossibilitat de construccions geomètriques usant regle i compàs (§4) o origami (és a dir plecs de paper) (§5). Tot seguit formulem el resultat principal d'Évariste Galois (§6) i finalment acabem explicant com és d'actual l'obra de Galois (§7).

2 Évariste Galois, el personatge

En aquest apartat ens fonamentem bàsicament en el contingut del llibre de Malet [13] esmentat a dalt.

Com ja s'ha mencionat Évariste Galois va nèixer a Bourg-la-Reine, a 10 kilòmetres de Paris, el 25 d'octubre de 1811, en una família acomodada, culta i liberal. A l'Institut Louis-le-Grand de Paris fou un alumne conflictiu per la seva actitud, però descobrí el seu talent matemàtic a través de la geometria de Legendre i de les memòries originals de Lagrange: *La resolució d'equacions algèbriques, La teoria de funcions analítiques i Lliçons sobre el càlcul de funcions.*

Galois va fer el 1828 un primer intent fallit per entrar a l'École Polytechnique, i aquell mateix any entrà en un curs amb el professor Louis Émile Richard, matemàtic que era recordat amb veneració per Liouville i altres eminències de les matemàtiques d'aquell temps, i qui encoratjà Galois a fer grans avenços. Amb Richard prepararà de nou el concurs d'accés a l'École Polytechnique, la memòria del qual arribà a mans de Cauchy.

El seu segon fracàs, altrament inexplicable, s'ha d'interpretar en funció de les circumstàncies polítiques. El seu pare era un home no identificat amb

el règim ultraconservador de la Restauració, que havia arribat a l'alcaldia de Bourg-la-Reine militant al partit lliberal, cosa que va influir molt en la ideologia del jove Galois. Al 1829 es fa càrrec de la parròquia del seu poble un nou mossèn jove i ple de recel, qui començarà una campanya difamatòria contra aquell alcalde massa lliberal. El pare d'Évariste, en una crisi depressiva, es suicidà el 2 de juliol de 1829 pocs dies després del segon intent fallit en la prova d'accés a l'École Polytechnique del seu fill. Un any més tard, derrocada la Restauració, l'examinador que suspengué a Galois, en Dinet, era acusat per la premsa de "*. . . no fer dels resultats dels exàmens el primer títol per a ésser admès a l'Escola [i de tenir en compte en primer lloc] les bones opinions i els sentiments religiosos i monàrquics de la família*".

Galois fou alumne a l'École Normale des del mes d'octubre de 1829 fins que en fou expulsat al desembre de 1830 després d'haver publicat a la premsa una carta molt ofensiva contra el director. En aquest període Galois publicà cinc articles i presentà a l'Acadèmia de les Ciències una primera monografia sobre les condicions de resolubilitat per radicals de les equacions algèbriques. Al maig de 1830, poc després de morir Fourier, se li comunica la pèrdua d'aquest treball. Reescriu la memòria i, el mes de gener de 1831, la torna a presentar. Llevat de la famosa carta testament, aquest fóra l'últim treball complert de Galois.

A partir de la revolució de juliol de 1830, Galois es va radicalitzar ideològicament, i un cop expulsat de l'École Normale es va dedicar cada vegada amb més intensitat a la lluita política. Fou detingut el mes de maig de 1831 per haver brindat pel rei amb un punyal a la mà al final d'un banquet polític. Tot i això va ser alliberat al cap d'un mes després de ser declarat innocent. La llibertat no li durarà molt, el 14 de juliol és detingut de nou quan anava armat al front d'una manifestació republicana contra la denominada monarquia burgesa de Louis Philippe. Entre les dues estades a la presó s'assabenta que el 4 de juliol, l'Acadèmia, fent seu l'informe de Poisson, havia refusat la memòria presentada el mes de gener.

Galois sortí de la presó el 16 de març de 1832. És llavors quan va iniciar una curta història d'amor que, en circumstàncies no gens clares, va acabar en un desafiament. Conscient que la seva mort podia ser pròxima, va dedicar la nit del 29 de maig a escriure una llarga carta amb les idees matemàtiques *"... que tenia al cap des de fa un any"* i a corregir alguns punts de la memòria que l'Acadèmia no havia acceptat. Després de batre's contra *"dos patriotes republicans"* (així els anomena ell mateix), un pagès el recollí al matí ferit de bala i abandonat. Morí 24 hores més tard.

Els manuscrits que deixà sobre la taula quan va anar al duel foren recollits per el seu germà, qui necessità més de deu anys de grans esforços per aconseguir que un matemàtic important els llegís. Fou Liouville finalment qui va fer arribar el treball de Galois a la sessió de l'Acadèmia d'un 4 de juliol de 1843, i qui permeté la publicació de la seva obra el 1846.

3 No existeix una fórmula per a les arrels d'un polinomi?

Un dels resultats més coneguts de l'obra d'Évariste Galois és la impossibilitat de donar una fórmula per a les arrels d'un polinomi de grau més gran o igual que cinc a partir de radicals. Anem a explicitar i entendre aquest resultat.

La ciència utilitza equacions per a enunciar de forma rigorosa lleis i propietats; aquestes equacions expressen relacions entre diverses variables o estats.

El camp d'aplicació de les equacions és immens, i hi ha una quantitat inabastable d'investigacions dedicades al seu estudi i la seva resolució de forma exacta o aproximada.

El que presentarem a continuació fa referència a la resolució de forma exacta d'equacions algebraiques de grau n.

3.1 La pregunta.

Donat un polinomi $p(x)$ de grau n,

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

amb $a_i \in K$, K un cos, podem expressar les arrels de $p(x)$ de forma exacta?

Per a simplificar l'exposició, pensarem en aquesta secció $a_i \in \mathbb{C}$. Com que sabem pel teorema fonamental de l'Àlgebra que $p(x)$ té en el cos dels complexos n arrels (comptant multiplicitat), la pregunta és: podem trobar una fórmula per a trobar aquestes n arrels complexes de forma exacta a partir del polinomi $p(x)$?

Évariste Galois posa un punt i apart en la qüestió!

Abans d'entrar en la resolució a la pregunta anem a fer un petit aclariment referent al sentit de la frase "calcular" les arrels de forma "exacta". Tot científic sap que donat el polinomi x^2+3x+1 de grau 2 podem trobar-hi les arrels o equivalentment resoldre l'equació algebraica de grau 2 donada per $x^2+3x+1=0$. És ben conegut que hi ha una fórmula per a resoldre de forma exacta aquesta equació de grau 2 i obtenim que $x = \frac{-3+\sqrt{5}}{2}$ i $x = \frac{-3-\sqrt{5}}{2}$. Com que $\sqrt{5}$ és un nombre irracional no podem donar una expressió decimal exacta d'ell, encara que podem aproximar-lo amb tanta precissió com desitgem. Així 2.236067977 és tan sols una aproximació de $\sqrt{5}$, per tant dir que les arrels del polinomi són -2.618033989, -0.3819660113 és incorrecte ja que aquests valors només són una aproximació a la solució. Fixeu-vos que usualment no podem esperar escriure de forma exacta les arrels sense usar "funcions" aplicades als coeficients del polinomi a part de sumes i productes, per exemple en el cas que hem presentat necessitem la funció pendre arrel quadrada.

3.2 Resolució de la pregunta per a $n = 2, 3$ i 4.

Per a un polinomi de grau dos és ben coneguda la resolució afirmativa de la qüestió. Durant el segle XVI, per a un polinomi de grau 3 o 4, es van trobar fórmules similars a la fórmula de grau 2. Recordem que pensem en tot aquest apartat que el polinomi té coeficients en els nombres complexos.

Cardano

Anem primer a fer una mica d'història per la trobada de la fórmula de grau 3 i de grau 4. L'aportació de Galois fa referència a polinomis de grau més gran o igual que 5.

La solució de la cúbica com també de l'equació de quart grau va ser publicada per Gerolamo Cardano (1501-1576) en el seu tractat Ars Magna l'any 1545 (consulteu [2, p. 283]).

Tartaglia

No obstant, sembla ser que Cardano no era el descobridor de cap d'aquests dos resultats. El punt clau per a resoldre la cúbica va ser donat per Niccolò Tartaglia, mentre que la de grau quatre havia estat resolta per Ludovico Ferrari. No obstant, sembla que Tartaglia havia obtingut la idea de la solució d'algú altri. La solució de la cúbica sembla que va ser trobada per un professor de matemàtiques de la Universitat de Bolonya de nom Scipione del Ferro (ca. 1465-1526). Del Ferro no va publicar mai la seva solució (dels documents que es tenen constància en aquests moments), però va revelar-la al seu estudiant Antonio Maria Fior ([2, p. 283]). I és d'aquí d'on aparentment Tartaglia va aprendre la resolució de la cública al voltant de l'any 1541.

Ferrari

Anem finalment a explicitar fórmules per polinomis de grau tres i quatre.

Donat un polinomi arbitrari de grau tres:

$$\ell(X) = X^3 + aX^2 + bX + c$$

la fórmula anomenada actualment de Cardano per a les arrels de $\ell(X)$ és:

$$\sqrt[3]{\sqrt{\Delta} - (q/2)} - \sqrt[3]{\sqrt{\Delta} + (q/2)} - (a/3) \qquad (1)$$

Del Ferro

on $q := (2a^3/27) - (ab/3) + c$, $p := b - (a^2/3)$ i $\Delta := (4p^3 + 27q^2)/108$.

Fixeu-vos que la fórmula (1) no és explícita ja que les arrels cúbiques d'un nombre prenen tres valors!. Per exemple "$\sqrt[3]{i}$" pot significar exactament tres nombres diferents i no està definida de forma única l'expressió "$\sqrt[3]{i}$", realment pot ser qualsevol dels tres nombres complexos diferents següents: $e^{\pi i/6}$, $e^{5\pi i/6}$ i $e^{9\pi i/6}$. Per tant, com apareix $\sqrt[3]{*}$ en la fórmula de Cardano, estem restant en la fórmula tres nombres complexos a tres nombres complexos i per tant hi ha nou resultats!, és a dir, la fórmula de Cardano ens dóna nou possibles

solucions de la cúbica i tant sols tres d'aquestes nou són les solucions del polinomi de grau tres. COM TRIAR AQUESTES TRES SOLUCIONS? Tot i que es pot fer un algoritme per elegir-ho correctament no hi entrem a detallar-ho en aquest apartat. Per a més informació podeu consultar per exemple: http://www.uv.es/ivorra/Libros/Ecuaciones.pdf

Escrivim ara una fórmula per a resoldre un polinomi de grau quatre arbitrari similar a la de grau tres, per al lector interessat consulteu l'adreça http://mathworld.wolfram.com/QuarticEquation.html, o per exemple, el llibre "Galois Theory" de Garling [10, §14.4].

La fórmula, anomenada de Ferrero, per a les arrels d'un polinomi de grau quatre arbitrari

$$X^4 + aX^3 + bX^2 + cX + d$$

és la següent:

$$\frac{Q \pm \sqrt{Q^2 - 4(P-R)}}{2} - \frac{a}{4}; \quad \frac{-Q \pm \sqrt{Q^2 - 4(P+R)}}{2} - \frac{a}{4} \tag{2}$$

on P és una arrel del polinomi $X^3 - \frac{p}{2}X^2 - rX + \frac{4pr-q^2}{8}$ en el que $p := b - 3a^2/8$, $q := c + a^3/8 - ab/2$ i $r := d - 3a^4/256 + a^2b/16 - ac/4$; i Q, R han de verificar les equacions $p = 2P - Q^2$, $q = -2QR$ i $r = P^2 - R^2$.

Igualment com en la fórmula per les arrels de l'equació de grau tres cal fer un petit estudi de quines solucions són les correctes en trobar P, Q i R per aplicar la fórmula (2).

3.3 Resolució de la pregunta per a $n \geq 5$ usant expressions radicals.

Com podeu observar restava la pregunta de si podem trobar una fórmula similar a les que hi ha per a grau 2, 3 o 4.

Abel i Ruffini van afirmar: *en general no és possible trobar una fórmula usant* RADICALS *per a l'equació*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

amb $n \geq 5$ *(on* $a_n \neq 0$*).* Aquí RADICALS indica que podem trobar les solucions aplicant únicament un número finit de sumes, restes, multiplicacions, divisions i extracció d'arrels de qualsevol ordre a partir dels coeficients de l'equació.

Évariste Galois aporta un algoritme per a decidir si per a un polinomi concret de grau més gran o igual que cinc existeix o no una fórmula per a trobar les seves arrels en RADICALS a partir del cos generat pels coeficients de $p(x)$**.** Per fer-ho Galois necessita crear

dues teories, establint una bijecció entre elles, veieu §6 per a una petita explicació d'aquesta bijecció.

Anem primer a fer diverses **aclariments del teorema d'Abel-Ruffini i l'aportació d'Évariste Galois** ja que de vegades s'entenen de forma errònia.

El resultat d'Abel-Ruffini no afirma que les equacions polinòmiques de grau cinc o superior no tenen solucions o que no poden ser resoltes. De fet, pel teorema fonamental de l'Àlgebra qualsevol equació polinomial té solucions. El resultat d'Abel-Ruffini afirma que les solucions no sempre poden ser calculades de forma exacta amb un número finit d'operacions aritmètiques (involucrant suma, producte i prendre arrels m-èssimes "$\sqrt[m]{*}$") a partir del cos generat pels coeficients del polinomi.

Les arrels d'un polinomi de qualsevol grau sobre els complexos poden trobar-se de forma APROXIMADA usant mètodes numèrics tals com el mètode de Newton-Raphson o el mètode de Laguerre.

Per exemple Maple sap calcular arrels de polinomis de forma aproximada als reals i complexos via

```
> fsolve(x^6 + x + x + 2, x);
> fsolve(x^6 + x + 2, x, complex);
```

L'aportació de Galois és donar un criteri per, fixat un polinomi concret de grau ≥ 5, decidir si les seves arrels poden calcular-se de forma EXACTA amb un nombre finit d'operacions aritmètiques, incloent l'extracció d'arrels, a partir dels coeficients del polinomi o no.

Per exemple, les n arrels del polinomi $x^n - R\,e^{i\theta}$ amb R i θ reals són de la forma $\sqrt[n]{R}\,e^{\frac{i\theta}{n}+\frac{2\pi ki}{n}}$ amb $k = 0, ..., n-1$ i, per tant, són les arrels n-èssimes d'un dels coeficients del polinomi. Per tant, aquest és un exemple en què es pot calcular de forma EXACTA les arrels del polinomi per radicals, això provè del fet que l'objecte algebraic associat per Galois al polinomi $x^n - R\,e^{i\theta}$ compleix una propietat específica. Évariste Galois va donar el següent criteri: donat un polinomi $p(x)$ podem associar-li una estructura algebraica, un grup, anomenat el grup de Galois associat a $p(x)$. Llavors, aquest grup satisfà una certa propietat, anomenada propietat de resolubilitat, si i només si les arrels de $p(x)$ es poden resoldre de forma EXACTA amb radicals a partir dels coeficients del polinomi. Per aprofundir aquest resultat podeu consultar qualsevol text de teoria de cossos bàsic o teoria de Galois, per exemple els apunts [1, §5].

Prenem ara els polinomis de grau cinc de la forma $x^5 - n\,p\,x + p$ amb $n \geq 2$ i p primer. El seu grup de Galois associat és el grup de permutacions d'un conjunt de cinc elements, que no compleix la propietat de resolubilitat, per tant, pel criteri que va obtenir Évariste Galois, no podem trobar de forma

EXACTA usant radicals les arrels dels polinomis de grau 5: $x^5 - 15x + 3$, $x^5 - 20x + 2$, $x^5 - 22x + 11$,...

Hi ha paquets informàtics com Magma, Sage o Mathematica que poden aplicar l'aportació de Galois per a polinomis de grau no molt gran. Per exemple, la majoria d'aquests programes poden decidir, per a polinomis de fins a grau set, si és possible calcular de forma exacta les arrels per radicals i en cas afirmatiu donar-ne l'expressió corresponent.

Com a resum sobre resolubilitat per radicals tenim:

Polinomi a $\mathbb{C}[X]$	Les arrels del polinomi són
$X^2 + bX + c$	$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$
$X^3 + aX^2 + bX + c$	$\sqrt[3]{\sqrt{\Delta} - (q/2)} - \sqrt[3]{\sqrt{\Delta} + (q/2)} - (a/3)$ amb $\Delta := (4p^3 + 27q^2)/108$ on $q := (2a^3/27) - (ab/3) + c$, i $p := b - (a^2/3)$.
$X^4 + aX^3 + bX^2 + cX + d$	$\frac{Q \pm \sqrt{Q^2 - 4(P - R)}}{2} - \frac{a}{4}$ $\frac{-Q \pm \sqrt{Q^2 - 4(P + R)}}{2} - \frac{a}{4}$ on P és una arrel del polinomi $X^3 - \frac{p}{2}X^2 - rX + \frac{4pr - q^2}{8}$ en el que $p := b - 3a^2/8$, $q := c + a^3/8 - ab/2$, $r := d - 3a^4/256 + a^2b/16 - ac/4$; i Q, R es determinen per $p = 2P - Q^2$, $q = -2QR$, $r = P^2 - R^2$.
$X^5 + aX^4 + bX^3 + cX^2 + dX + e$ Polinomi arbitrari de grau 5	Abel-Ruffini: No hi ha fórmula per radicals
Polinomi arbitrari de grau ≥ 6	Abel-Ruffini: No hi ha fórmula per radicals
Polinomi concret de grau ≥ 5	Criteri de Galois de resolubilitat.

3.4 La resolució final a la pregunta

Al final del segle XIX o a principis del XX, Hilbert va demostrar que la gran majoria de grups de Galois associats a un polinomi de grau $n \geq 5$ són no resolubles, per tant pel criteri de Galois enunciat en la subsecció anterior, per la gran majoria de polinomis de grau superior o igual a 5 no podem esperar trobar de forma EXACTA amb radicals les seves arrels.

Després del resultat de Galois i de Hilbert podem plantejar-nos: podem trobar les arrels d'un polinomi de grau més gran o igual que 5 de forma EXACTA usant altres expressions que no siguin via RADICALS, per exemple

introduint certes funcions analítiques avaluades en els coeficients del polinomi?

La resposta és: sí.

Mitjançant els Thetanullwerke és pot trobar una fórmula per les arrels d'un polinomi de grau arbitrari de forma EXACTA, observeu que ara permetem que les solucions s'escriguin d'avaluar en certs punts certes funcions analítiques!, enlloc d'expressions en radicals com hem fet anteriorment. J. Thomae troba una fórmula en *Beitrag zur Bestimmung von* $\vartheta(0,0,\dots 0)$ *durch die Klassenmoduln algebraischer Funktionen* [19]. Per a més detalls podeu consultar l'apèndix de H. Umemura en [14] que dóna una fórmula general amb funcions theta per a les equacions algebraiques.

No obstant aquestes fórmules per les arrels usant Thetanullwerke no són massa útils a la pràctica i per a calcular les arrels de forma aproximada per als polinomis on el criteri de Galois ens afirma que no podem esperar trobar-ne una expressió per radicals de les arrels a partir dels coeficients del polinomi s'usa el métode de Newton-Raphson o similars .

4 Construccions amb regle i compàs, problemes clàssics grecs

Una contribució més lúdica de la teoria que va desenvolupar Galois és refereix a problemes de construcció amb regle i compàs i permet resoldre problemes plantejats en temps dels grecs. Aquí intentem explicar una mica aquest contingut que es desenvolupa en un curs típic de teoria de Galois.

Suposem que només tenim un regle sense marques i un compàs, i partim de dos punts fixats del pla, que suposem a distància 1. Direm que un punt del pla és construïble amb regle i compàs si el podem obtenir a partir dels elements mencionats, fent successives interseccions de rectes i/o circumferències obtingudes a partir de quantitats prèviament construïdes (les circumferències tenen centres en punts construïts i radis donats per la distància entre dos punts construïbles). Diem que un nombre real positiu α és construïble si podem construïr un segment de longitud α, és a dir, existeixen dos punts construïbles amb regla i compàs tals que la distància entre ells és α.

Alguns dels problemes relacionats amb construccions amb regle i compàs que varen preocupar als grecs són:

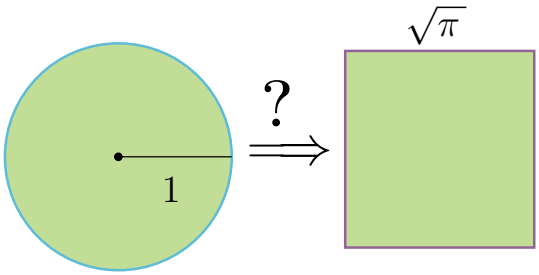
1. És possible duplicar el cub? És a dir, donat un cub de costat 1 (i volum 1), podem construïr (amb regle i compàs) un altre cub de volum 2? Això equival a construïr la longitud real $\sqrt[3]{2}$.

2. És possible la quadratura del cercle? És a dir, donat el cercle unitat, que és construïble amb regle i compàs i té àrea π, podem construïr un quadrat que tingui la mateixa àrea? Això és equivalent a construïr el nombre real $\sqrt{\pi}$.

3. És possible la trisecció de l'angle? És a dir, donat un angle construïble arbitrari θ, podem construïr l'angle $\theta/3$?

Fent servir la teoria d'extensions de cossos —una teoria motivada pels treballs de Galois— es pot veure que cap d'aquestes construccions és possible. De fet la impossibilitat de resoldre el problema 1 es basa en el fet que el polinomi irreductible amb coeficients a $\mathbb{Q}$ que té com arrel $\sqrt[3]{2}$ és un polinomi de grau 3 (és el polinomi x^3-2), mentre que si $\sqrt[3]{2}$ fos construïble, llavors hauria de ser un polinomi de grau una potència de 2. Per la mateixa raó, no podem fer la trisecció de l'angle de $\pi/3$ radiants (60^o). Aquest cop, el polinomi irreductible de $\cos(\pi/9)$ sobre $\mathbb{Q}$ és $x^3-\frac{3}{4}x-\frac{1}{8}$.

Pel que fa a la impossibilitat de la quadratura del cercle (problema 2), la raó d'aquesta és el fet que el nombre π és transcendent, és a dir π no és arrel de cap polinomi no nul a coeficients enters. Aquest fet va ser demostrat a finals del segle XIX per Lindermann i Weierstrass. Com tota quantitat construïble és un nombre algebraic, obtenim la impossibilitat de la quadratura del cercle.



La quadratura del cercle

Els polígons regulars construïbles amb regle i compàs varen atraure l'atenció de matemàtics molt importants, especialment Gauss, que a l'edat de 19 anys va demostrar que el polígon regular de 17 costats és construïble. Gauss va provar al 1796 que si un polígon regular de n costats és construïble, llavors n ha de ser de la forma següent: $n=2^s p_1\cdots p_r$, on r i s són enters no negatius, i p_i són primers de Fermat diferents. El recíproc d'aquest resultat va ser establert per Wenzel al 1836. Els primers de Fermat són els nombres primers de la forma $p=2^r+1$. Es pot veure que si $p=2^r+1$ és un primer de Fermat, llavors l'exponent r ha de ser una potència de 2. Per exemple $2^{2^0}+1=3$, $2^{2^1}+1=5$, $2^{2^2}+1=17$, $2^{2^3}+1=257$ i $2^{2^4}+1=65537$ són primers de Fermat. Fermat va conjecturar que tots els nombres de la forma $2^{2^n}+1$ són primers. Això és erroni, com va demostrar Euler l'any 1732. De fet

$$2^{2^5}+1=2^{32}+1=4294967297=641\cdot 6700417$$

és el nombre més petit de la forma $2^{2^n}+1$ que no és primer. Curiosament, no es coneix cap primer de Fermat apart dels ja mencionats.

5 Construcions amb origami

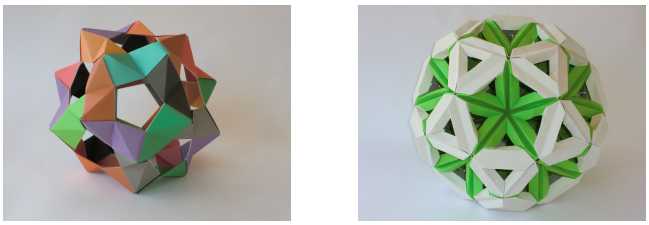
Una altra contribució lúdica dels resultats de Galois ha estat la seva aplicació en origami o plecs de paper.

Una explicació matemàtica més ampliada del que escriurem tot seguit podeu trobar-ho en el llibre [4] o bé [1, B2]. També recomanem la pàgina web sobre origami de'n Robert J. Lang, http://www.langorigami.com/

5.1 El terme origami i aquest escrit

L'origami és l'art d'origen japonès consistent amb el plegat de paper, per a obtenir figures de formes variades. En català també s'anomena papiroflèxia.

En l'origami no es poden utilitzar tisores, cola o grapes, tan sols paper i plegats amb les mans. Es pot observar que amb tan sols unes poques fulles de paper podem construir diferents cossos geomètrics (políedres i tot), a vegades aquestes construccions usant més d'un paper s'anomenen origami modular i no seran tractats aquí.



Políedres construïts amb origami modular

En aquest escrit ens centrarem en construccions que es poden fer amb un sol paper. La teoria iniciada per Évariste Galois ens indica quines línies i punts podem obtenir de forma exacta sobre el paper per tal de després procedir a fer plecs i obtenir amb l'art japonès d'origami figures increïbles com la rosa de Kawasaki, que veieu a continuació.

A la web es troben videos per a construir l'anterior Rosa de Kawasaki. Un que ens agrada especialment, ja que s'inicia amb el paper marcat, és el video que actualment es troba a l'adreça

http://www.youtube.com/watch?v=RmH86VqjGRg&feature=related

Aquest video s'inicia sobre un paper on hi ha línies i punts dibuixats que representen les linies i punts marcades sobre el paper construïbles amb Origami a partir de l'axiomàtica que presentarem tot seguit. Fixeu-vos que un cop marcades les línies aconseguir la rosa de Kawasaki és TOT UN ART! Matemàtiques i art complementant-se!

El full on s'inicia la construcció de la Rosa de Kawasawi, amb diferents pasos fins la seva construcció

Comentem en aquest punt que molt sovint en assignatures de dibuix tècnic s'explica una construcció usant regle i compàs de l'heptàgon regular, no obstant aquesta construcció no és exacta (ja que es pot demostrar usant teoria de Galois que no és factible, llegiu-ho en §3 referent a construcció amb regle i compàs, o veieu també [1, B1]). La pseudoconstrucció de l'heptàgon regular amb regle i compàs en dibuix tècnic fa una petita aproximació per obtenir el punt necessari per la construcció, aquesta aproximació quasi bé no s'observa (similar al fet que qualsevol nombre real s'aproxima per nombres racionals). De manera similar, en construir figures amb origami, a vegades, es poden fer aproximacions i construir figures que necessiten punts que no podem construir-se amb l'axiomatica amb origami i tan sols poden obtenir-se de forma aproximada.

El què explicarem a continuació en aquest escrit és la justificació de la construcció en un full d'origami de punts i línies que són construïbles amb origami de forma exacta via una axiomàtica fixada. També explicarem el motiu perquè les arrels de qualsevol equació de tercer grau a coeficients els nombres racionals són construïbles usant origami, i com en origami podem trisecar un angle!

L'argumentació matemàtica es troba dins la teoria que va iniciar Galois.

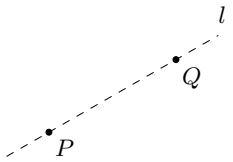
5.2 Punts i nombres reals construïbles usant plecs en un paper

Anem a explicitar certes operacions que podem fer sobre un plà (pensarem també un paper quadrat) que ens permeten construir longituds reals i punts sobre aquest plà, punts i longituds que direm que són construïbles amb origami.

L'axiomàtica per a la construcció és la següent: partim de dos punts $(0,0)$ i $(1,0)$ que marquem de forma arbitrària sobre el paper i construïm

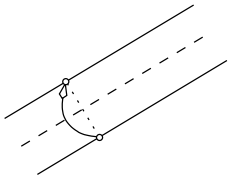
els següents punts i línies (que diem que són construïbles per origami) per iteració a partir dels axiomes següents:

(i) la recta que es forma unint dos punts construïbles direm que és una recta (o línia) construïble (amb origami),

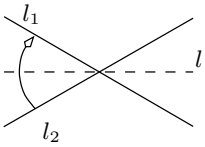


(ii) el punt d'intersecció de dos rectes construïbles (no paral·leles) és un punt construïble,

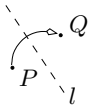
(iii) donades dues rectes paral·leles construïbles, podem construir la recta paral·lela a ambdues i equidistant amb elles,



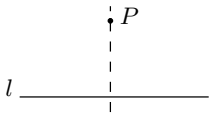
(iv) donades dues rectes construïbles, defineixen un angle, aquest angle es pot biseccionar, és a dir podem construir la recta que bisecciona l'angle,



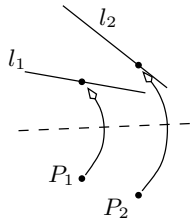
(v) donats dos punts construïbles P i Q diferents, podem construir la recta perpendicular a la recta formada pels dos punts P i Q de manera que el punt de tall d'ambdues rectes és el punt mig del segment PQ,



(vi) donada una recta construïble l i un punt construïble P, podem construir la recta perpendicular a l contenint el punt P,



(vii) donades dues rectes construïbles l_1 i l_2 (no necessàriament diferents) i dos punts construïbles P_1 i P_2 (no necessàriament diferents) un pot construir la recta que simultàniament reflexa P_1 en l_1 i P_2 en l_2,



(es pot veure que aquest axioma afirma que un pot obtenir tangents comuns de les paràboles p_1 i p_2 amb focus P_1, P_2 i directrius l_1 i l_2 respectivament. Per això cal aprofundir una mica sobre les propietats de la paràbola).

(viii) donat un segment entre dos punts construïbles i una recta construïble r amb un punt constuïble P en la recta, podem portar el segment damunt la recta a partir del punt P,

(ix) podem portar un angle construïble (és dir l'angle entre dues línies construïbles) a qualsevol punt construïble P on hi ha una recta construïble r que passa pel punt P.

Els nombres reals construïbles en origami són els punts construïbles en origami en l'eix OX, és a dir de la forma $(\alpha, 0)$.

Denotem per $\mathcal{M}$ el conjunt de tots els nombres reals construïbles amb origami. Es demostra que és un cos (és a dir té operació suma i producte on aquestes operacions tenen les mateixes propietats que tenen la suma i el producte dels nombres reals o racionals). El cos $\mathcal{M}$ conté els nombres racionals i es pot caracteritzar de forma semblant al cas dels nombres reals construïbles amb regle i compàs. És a dir, usant teoria de Galois, Geretschläger e independentment Emert-Meeks-Nelson demostren l'any 1995:

Proposició 5.1 *Es compleix que un punt $x \in \mathbb{R}$ és construïble en origami si i només si existeix una torre de cossos $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ amb $x \in K_n$ i $[K_i : K_{i-1}] \leq 3$ on K_n és un cos dins els nombres reals*[2].

Recordem aquí que per tal que $x \in \mathbb{R}$ sigui construïble amb regle i compàs el resultat és similar al teorema de Geretschläger i Emert-Meeks-Nelson anterior, però per a aquest altre cas la cadena de cossos que cal construir ha de complir $[K_i : K_{i-1}] \leq 2$ i per tant tot punt construïble amb regle i compàs és també construïble amb origami.

Diem que un nombre complex $P + iQ$ amb $P, Q \in \mathbb{R}$ i i el nombre imaginari pur, amb $i^2 = -1$, és construïble amb origami si i només si P i Q són nombres reals construïbles amb origami. Com que podem fer paral·leles i perpendiculars per l'eix OX i OY obtenim que un punt $(P, Q) \in \mathbb{R}^2$

[2] Recordem que si tenim una inclusió de cossos $L \subset K$ es té que K és un L-espai vectorial i $[K : L]$ és la dimensió de K com a L-espai vectorial.

és construïble amb origami si i nomes si $P + iQ$ és un nombre complex construïble amb origami. Obtenim immediatament la versió complexa de la proposició 5.1 següent:

Proposició 5.2 *Un punt $(P, Q) \in \mathbb{R}^2$ (o el nombre complex $P + iQ$) és construïble en origami si, i només si, existeixen una torre de cossos de la forma $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ amb $P + iQ \in K_n$ i $[K_i : K_{i-1}] \leq 3$, on K_n és un cos dins els nombres complexos.*

Finalment, es demostra que $(P, Q) \in \mathbb{R}^2$ és construïble amb regle i compàs si el nombre complex $P + iQ$ té una cadena de cossos com en la proposició 5.2 però exigint $[L_i : L_{i-1}] \leq 2$; per tant tot punt construïble amb regle i compàs és construïble amb plecs de paper.

5.3 Exemples de nombres reals i punts construïbles per origami

Anem primer a fer dos exemples de nombres reals construïbles amb origami.

1. El punt $\sqrt[3]{2+\sqrt{2}}$ és construïble amb origami.

   Efectivament, considerem la torre de cossos

   $$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}\,] \subseteq \mathbb{Q}[\,\sqrt{2}\,,\ \sqrt[3]{2+\sqrt{2}}\,]$$

   dins els nombres reals (on $F[a, b]$ es l'anell de polinomis en a, b i amb coeficients al cos F, es pot demostrar que $F[a, b]$ és un cos si a i b són arrels de polinomis a coeficients en el cos F). Fixeu-vos en què com $\sqrt{2}^{\,2} = 2$ tenim $\mathbb{Q}[\sqrt{2}\,] = \{c + d\sqrt{2} \mid a, b \in \mathbb{Q}\}$ i és un $\mathbb{Q}$-espai vectorial de dimensió 2, és a dir $[\mathbb{Q}(\sqrt{2}\,) : \mathbb{Q}] = 2 \leq 3$, també observem que com $\left(\sqrt[3]{2+\sqrt{2}}\right)^3 = 2+\sqrt{2}$ obtenim $\mathbb{Q}[\,\sqrt[3]{2+\sqrt{2}}\,] = \{e+f(\sqrt[3]{2+\sqrt{2}}\,)+g(\sqrt[3]{2+\sqrt{2}}\,)^2 \mid e, f, g \in \mathbb{Q}[\,\sqrt{2}\,]\}$ i per tant $[\mathbb{Q}[\,\sqrt[3]{2+\sqrt{2}}\,] : \mathbb{Q}[\sqrt{2}\,]] \leq 3$, finalment hem construït una torre de cossos com en l'enunciat de la proposició 5.1, això és $\sqrt[3]{2+\sqrt{2}}$ és construïble amb origami.

2. Les arrels reals d'un polinomi de grau tres a coeficients en els nombres racionals són construïbles amb origami.

   Fem-ho tan sols en un exemple concret. Considerem el polinomi $x^3 + 3x + 1$. Com que és de grau senar sabem que té almenys una arrel real, diem-li α, fixeu-vos que com $\alpha^3 = -3\alpha - 1$ la inclusió de cossos $\mathbb{Q} \subset \mathbb{Q}[\alpha] = \{h + g\,\alpha + m\,\alpha^2 \mid h, g, m \in \mathbb{Q}\}$ satisfà $[\mathbb{Q}[\alpha] : \mathbb{Q}] \leq 3$ i per tant per la proposició 5.1 podem construir α en origami.

   El mateix argument fet pel polinomi $x^3 + 3x + 1$ el podeu fer per a un polinomi arbitrari $x^3 + b\,x^2 + c\,x + a$ amb $b, c, a \in \mathbb{Q}$.

Anem a fer exemples de punts construïbles amb Origami:

1. Usant origami podem trisecar un angle qualsevol que tinguem construït. Recordeu que aquest és un dels problemes que va interessar al pensament grec i que com heu vist en §4 no és factible fer-ho amb Regle i Compàs.

   Anem a justificar perquè podem trisecar un angle en Origami.

   Considereu un angle donat construït amb origami, diem-li θ, tenim doncs construït sobre el paper el punt $(\cos(\theta), \sin(\theta)$, el punt $(0,0)$ i el punt $(1,0)$. Volem construir en origami el punt $(\cos(\theta/3), \sin(\theta/3))$.

   Fixeu-vos que $e^{i\theta/3} = \cos(\theta/3) + i\,\sin(\theta/3)$ és arrel del polinomi de grau 3:

   $$X^3 - e^{i\theta}$$

   com $e^{i\theta}$ és construïble amb origami, tenim una cadena de cossos

   $$\mathbb{Q} \subseteq K_1 \subseteq \ldots \subseteq K_n$$

   on $e^{i\theta} \in K_n$, amb $[K_i : K_{i-1}] \leq 3$. Construïm el cos $K_{n+1} := K_n[e^{i\theta/3}] = \{a + b\,e^{i\theta/3} + c\,e^{i\,2\theta/3} \mid a, b, c \in K_n\}$ on $[K_{n+1} : K_n] \leq 3$ i per la proposició 5.2 obtenim el resultat.

2. En origami podem construir l'heptàgon regular!

   Per a construir el polígon regular de 7 costats és suficient obtenir el punt $(\cos(2\pi/7), \sin(2\pi/7))$ ja que fent el plec de paper sobre el $(0,0)$ entre la línia de l'eix OX amb la línia definida per $(0,0)$ i $(\cos(2\pi/7), \sin(2\pi/7))$ obtenim el punt $(\cos(4\pi/y), \sin(4\pi/7))$ i així successivament fins a trobar tots els vèrtexs del polígon regular de 7 costats.

   Anem a justificar doncs que $(\cos(2\pi/7), \sin(2\pi/7))$ és un punt construïble amb origami.

   Prenem $\alpha := e^{i2\pi/7}$ i observeu que $\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$ per tant tenim

   $$\mathbb{Q} \subset \mathbb{Q}[\alpha] = \{a + b\,\alpha + c\,\alpha^2 + d\,\alpha^3 + e\,\alpha^4 + f\alpha^5 \mid a, b, c, d, e, f \in \mathbb{Q}\}$$

   on $[\mathbb{Q}[\alpha] : \mathbb{Q}] \leq 6$, això no ens és útil per aplicar la proposició 5.2, ja que els graus en la cadena han de ser menors o iguals que tres, per això construïm un cos intermedi que compleixi les propietats per usar el teorema. Considerem el cos $\mathbb{Q}[\alpha + \overline{\alpha}]$ on $\overline{\alpha}$ és el conjugat de α. Fixeu-vos $\mathbb{Q}[\alpha + \overline{\alpha}] \subset \mathbb{Q}[\alpha]$ (en aquest cas una manera fàcil de veure això és tenir en compte que $\overline{\alpha} = \alpha^{-1}$) i $[\mathbb{Q}[\alpha] : \mathbb{Q}[\alpha + \overline{\alpha}]] = 2$, ja que els dos cossos no són iguals (un és dins els reals ja que $\alpha + \overline{\alpha} = 2\cos(2\pi/7) \in \mathbb{R}$ i l'altre no) i α és arrel del polinomi de grau 2 a coeficients en

$\mathbb{Q}[\cos(2\pi/7)] = \mathbb{Q}[\alpha + \bar{\alpha}]$ donat per $X^2 - 2\cos(2\pi/7)\,X + 1$, per tant tenim una cadena de cossos

$$\mathbb{Q} \subseteq \mathbb{Q}[\cos(2\pi/7)] \subseteq \mathbb{Q}[e^{2\pi i/7}]$$

i es pot comprovar que la dimensió de $\mathbb{Q}$-espai vectorial de $\mathbb{Q}[e^{2\pi i/7}]$ (que sabem que és menor o igual a 6) és el producte de la dimensió de $\mathbb{Q}[\cos(2\pi i/7)]$ com $\mathbb{Q}$-espai vectorial i de la dimensió de $\mathbb{Q}[e^{2\pi i/7}]$ com a $\mathbb{Q}[\cos(2\pi i/7)]$-espai vectorial, per tant obtenim que

$$[\mathbb{Q}[e^{2\pi i/7}] : \mathbb{Q}[\cos(2\pi/7)]] = 2 \leq 3, \quad \text{i} \quad [\mathbb{Q}[\cos(2\pi/7)] : \mathbb{Q}] \leq 3$$

Usant la proposició 5.2 obtenim que podem construir el polígon regular de set costats de forma exacta usant origami (i no és construïble amb regle i compàs!).

6 El teorema fonamental d'Évariste Galois

Les conseqüencies i aplicacions dels resultats anteriors en el món de les equacions són de gran utilitat per totes les ciències, així com en les construccions amb regle i compàs, origami i altres en geometria. Tota la teoria es basa en el treball profund i teòric de Galois sobre l'estudi de la teoria de cossos i la creació de la teoria de grups. En aquest apartat no entrem en la definició de cos ni de grup, el lector pot consultar les definicions en [1, 4, 12], tan sols enunciem el resultat clau que va obtenir Évariste Galois (tot i que no va ser fins revisions posteriors de la seva obra que es va donar a conèixer als matemàtics, ja que els seus escrits originals necessitaven revisió i petites rectificacions). El lector interessat en aprofundir en el contingut matemàtic pot consultar qualsevol dels textos citats anteriorment.

Galois va demostrar l'any 1832 la seva famosa *correspondència*: Sigui

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

un polinomi a coeficients enters, i sigui L el mínim subcos de $\mathbb{C}$ que conté les arrels del polinomi $f(x)$. (Recordem que pel teorema fonamental de l'àlgebra $f(x)$ factoritza en factors lineals a $\mathbb{C}$.) Sigui $G = \mathrm{Aut}(L)$ el grup de tots els automorfismes del cos L. Llavors:

Teorema 6.1 (Galois) *Existeix una correspondència bijectiva:*

$$\{\textit{subgrups de } G\} \longleftrightarrow \{\textit{ subcossos de } L\}$$

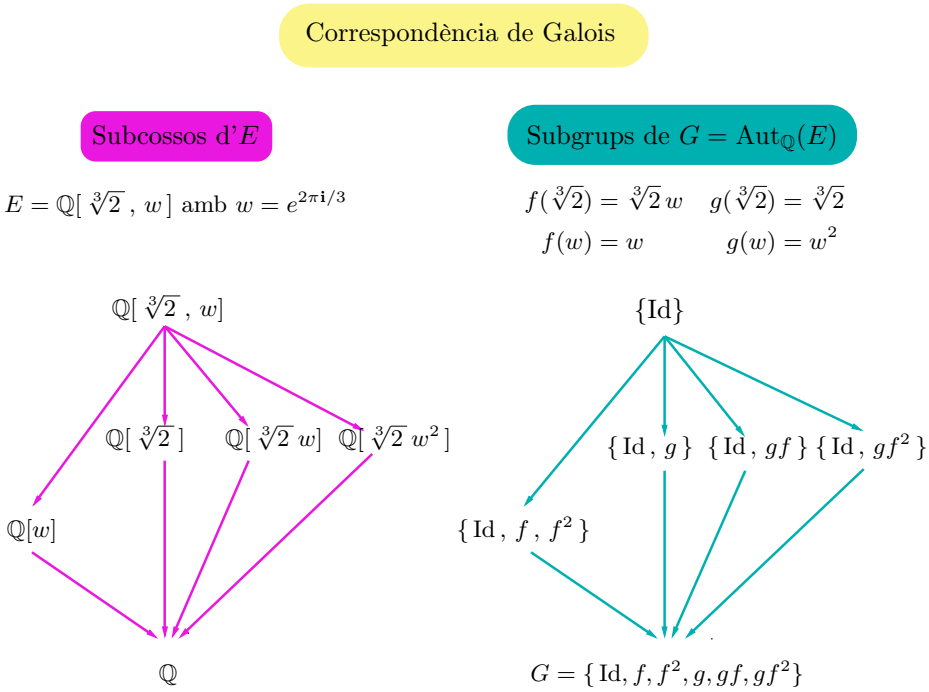
Més concretament, si H és un subgrup de G, llavors:

$$H \mapsto L^H = \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\}\,.$$

L^H s'anomena el cos fix de H. Similarment, si F és un subcos de L, llavors

$$F \mapsto \mathrm{Aut}_F(L) = \{\sigma \in G \mid \sigma(x) = x \quad \forall x \in F\}\,.$$

En el gràfic següent il·lustrem la correspondència de Galois per $f(x) = x^3 - 2$.



7 Galois al segle XXI

La teoria matemática que va desenvolupar Galois s'estudia en molts graus de Matemàtiques com assignatura obligatòria. Tot i que aquesta teoria pot semblar molt abstracta, s'ha aplicat amb molt d'èxit des dels temps de Galois tant per a trobar solucions de problemes com per a provar que d'altres no tenen solucions.

Anem tot seguit a llistar alguns punts actuals de recerca e interrelació amb altres disciplines que ha aportat la teoria que va iniciar Galois. Com observaréu molts d'ells són de gran impacte aplicat! i els que es troben dins la matemàtica fonamental són de tal rellevància qué si algú n'obté la resolució guanyaria amb molta seguretat una medalla Fields (sempre i quant fos menor de 40 anys)[3] (Recordem que la medalla Fields és l'equivalent dels Nobel a la disciplina de les matemàtiques,

http://en.wikipedia.org/wiki/Fields_Medal

i podeu llegir en

http://nobelprizes.com/nobel/why_no_math.html

certs motius per tal que no existeix el premi Nobel de Matemàtiques).

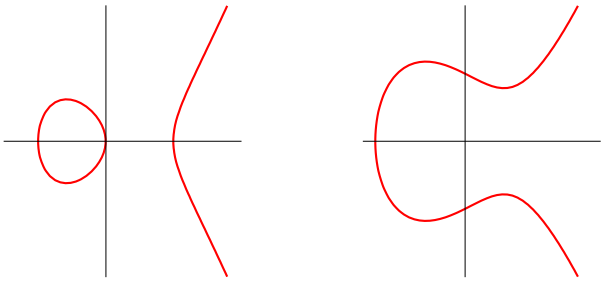
[3] El premi de la Medalles Fields es concedeix actualment cada quatre anys durant el Congrés Internacional de Matemàtics (ICM) i se'n poden concedir fins a quatre.

7.1 Galois i cossos finits.

Évariste Galois, amb els seus treballs,va fer palesa la importància dels cossos finits, per això programes informàtics per a fer càlculs en matemàtiques com Maple o Sage denoten el cos finit per GF "Galois Field" en reconeixement a Galois. Recordem que els cossos finits són la base de la Matemàtica Discreta i que tot això es relaciona amb la Informàtica i l'Enginyeria.

7.2 Galois i Criptografia

La geometria de les corbes el·líptiques sobre cossos finits, és a dir corbes amb equació $y^2 = x^3 + ax + b$, on a, b són elements d'un cos finit, té grans aplicacions a la criptografia de clau pública, per exemple el passaport alemany implementa aquesta aplicació criptogràfica.



Dibuix real de dos corbes el·líptiques sobre els racionals

Per a fer una bona implementació del métode d'encriptació, cal fer una bona elecció dels valors a, b conjuntament amb un punt de la corba. Per això és necessari un estudi dels punts de corbes de la forma $y^2 = x^3 + ax + b$ sobre cossos finits. La teoria construïda per Évariste Galois és de vital importància per a fer aquest estudi. El lector interessat en la implementació i més detalls tècnics pot consultar el llibre d' Steven Galbraith "Mathematics of Public key cryptography" [8] i l'article de Gerhard Frey i Tanja Lange "Mathematical background of public key criptography" [7] (http://www.exp-math.uni-essen.de/zahlentheorie/preprints/preprintfreylange03.pdf).

7.3 Galois i la teoria d'autòmats

La teoria de Galois intenta estudiar si certs números complexos són arrel o no d'algun polinomi a coeficients racionals. Per exemple diem que $\sqrt{3}$ és algebraic sobre els racionals ja que és arrel del polinomi a coeficients racionals $T^2 - 3$, no obstant, com ja hem comentat, π no és algebraic sobre els racionals ja que no existeix cap polinomi a coeficients racionals on π és una arrel. També es diu que π és un nombre *transcendent* sobre els racionals.

Si anem al món de la computació i enginyeria ens interessa decidir quan una sèrie a coeficients en un cos finit

$$\sum_{i=0}^{\infty} a_i\, X^i \qquad \text{amb } a_i \in \mathbb{F}_q$$

és solució o no d'un polinomi en el cos associat a l'anell de polinomis $\mathbb{F}_q[X]$ (on $\mathbb{F}_q$ denota el cos finit de $q = p^n$ elements amb p primer), per exemple la sèrie

$$1 + X + X^2 + X^3 + X^4 + \cdots + X^{2011} + X^{2012} + \ldots \tag{3}$$

Alan Turing
(1912-1954)

és igual a $1/(1-X)$ (prenent la topologia dels entorns del zero donats per la potències de X que seria l'anàleg dels entorns al voltant del 0 per potències enteres de $(1/10)$ quan es considera la topologia del valor absolut usual en els nombres racionals) i per tant la sèrie (3) és solució del polinomi en la variable T següent: $(1-X)\,T-1=0$.

La teoria d'autòmats resol quan és que una sèrie $\sum_{i=0}^{\infty} a_i\, X^i$, amb $a_i \in \mathbb{F}_q$, és solució o no d'un polinomi en T a coeficients en $\mathbb{F}_q[X]$. La teoria d'autòmats s'estudia en el grau d'Informática i està relacionada amb la màquina de Turing.

Fem un exemple de com la teoria d'autòmats permet construir sèries que són arrel d'un polinomi a coeficients en el cos de fraccions de $\mathbb{F}_q[x]$ amb $q = 2$. Abans de concretar l'exemple introduïm alguns conceptes d'aquesta teoria en el cas de $q = 2$.

Un 2-autòmat (S, α, Σ, t) consisteix en:

1. Un conjunt finit S de situacions (els elements de S els anomenem situacions) i una situació inicial fixada α.

2. Una aplicació $t : S \times \Sigma \to S$ (on $\Sigma := \{0, 1\}$ es diu que és *l'alfabet*) anomenada funció transició.

Escrivim $\Sigma^* := \bigcup_{n=0}^{\infty} \Sigma^n$, on Σ^n és el conjunt de les seqüències finites de longitud n d'elements de Σ (en particular, $\Sigma^0 = \{\emptyset\}$ i $\Sigma^1 = \Sigma$), que s'anomena el conjunt de paraules de l'alfabet Σ. Donat $e \in \Sigma^*$ tenim que $e \in \Sigma^n$ pera algun n i escrivim $|e| = n$, a més per a cada $j \geq 0$ denotem per $e(j)$ l'element de Σ que ocupa la posició j en la paraula e (iniciant per la posició zero i d'esquerra a dreta). En Σ^* tenim un producte (té estructura de monoid) que per a $w \in \Sigma^\ell, v \in \Sigma^k$ dóna $w \cdot v \in \Sigma^{\ell+k}$ amb

$$(w \cdot v)(n) = \begin{cases} w(n) & \text{si } \ 0 \leq n < |w| \\ v(n - |w|) & \text{si } \ |w| \leq n < |w| + |v|. \end{cases}$$

(es posa v després de w com a paraula).

Observem que Σ^* com a conjunt es podria pensar com els enters expressats en base 2, no obstant el producte en Σ^* no correspon a la multiplicació de números: donats $(2 =)w := 1.0 \in \Sigma^2$, $(4 =)v := 1.0.0 \in \Sigma^3$, $w \cdot v = (1.0) \cdot (1.0.0) = (1.0.1.0.0)$ que no correspon a 8 en base dos que és 1.0.0.0 .

La funció transició t s'extén a $t : S \times \Sigma^* \to S$ mitjançant la regla inductiva

$$t(a, \emptyset) = a, \quad t(a, \ell\, m) = t(t(a, \ell), m) \quad \text{per a } \ell \in \Sigma,\ m \in \Sigma^*.$$

Es diu que una seqüència $u = (u(k))_{k\geq 0}$ és un "2-automaton" si existeix un 2-autòmat (S, α, Σ, t) i una aplicació $\mathrm{Out} : S \to \mathbb{F}_2$, on $u(0) = \mathrm{Out}(\alpha)$ i $u(k) = \mathrm{Out}(t(\alpha, k_j . \cdots . k_0))$ si $k = \sum_{n=0}^{j} k_n 2^n$ amb $k_n \in \Sigma = \{0, 1\}$.

Anem ara finalment a presentar l'exemple. Considerem el 2-autòmat donat per la següent taula amb estat inicial $\alpha = s_1$ i quatre estats s_1, s_2, s_3, s_4 amb funció de sortida $\mathrm{Out}(s_1) = \mathrm{Out}(s_2) = 1$, $\mathrm{Out}(s_3) = \mathrm{Out}(s_4) = 0$ i amb taula t:

	s_1	s_2	s_3	s_4
0	s_1	s_3	s_2	s_4
1	s_2	s_4	s_2	s_4

Considerem la serie $\sum_{n=0}^{\infty} a_n X^m$ on $a_i \in \{0, 1\}$ del cos finit de dos elements i definides pel 2-autòmat anterior, això és $a_0 = \mathrm{Out}(s_1) = 1$, $a_1 = \mathrm{Out}(t(s_1, 1)) = \mathrm{Out}(s_2) = 1$, $a_2 = \mathrm{Out}(t(s_1, 1.0)) = \mathrm{Out}(t(t(s_1, 1), 0)) = 0$ (1.0 és la representació en base 2 del $2 = 1 \cdot 2^1 + 0 \cdot 2^0$), $a_3 = \mathrm{Out}(t(s_1, 1.1)) = 0$,...

Podem veure que

$$g(X) := \sum_{n=0}^{\infty} a_n X^n = \sum_{m \in M} X^m\,,$$

on M és el subconjunt de $\mathbb{N}$ definit per $M = \bigcup_{n=0}^{\infty} M_n$ essent $M_0 = \{0, 1\}$ i cada un dels M_n s'obté calculant tots els valors $4m, 4m + 1$ per als m de M_{n-1}, per tant $g(X) = (\sum_{m \in M} X^{4m})(1 + X)$ i com que estem treballant a coeficients en un cos de dos elements obtenim

$$g(X) = g(X)^4 (1 + X)$$

per tant $g(X) = (1 + X)^{-1/3}$, és a dir $g(X)$ és algebraic sobre el cos de fraccions de $\mathbb{F}_2[X]$ i és arrel del polinomi en T:

$$(1 + X)\, T^3 - 1.$$

El fet que la sèrie estigui construïda per un automaton fa que la sèrie satisfaci un polinomi en T, i viceversa!

Per aprofundir en aquesta interrelació podeu consultar per exemple el capítol 11 del llibre de D. Thakur "Function Field Arithmetic" [18].

7.4 Galois i les equacions diferencials

La teoria de Galois diferenciable estudia extensions de cossos que tenen una derivació. Bona part de la teoria de Galois diferenciable és paral·lela a la teoria que va desenvolupar Évariste Galois. Una diferència entre ambdues és que els grups que apareixen en la teoria diferenciable tendeixen a ser grups de Lie de matrius. Recordem que els grups de Lie són de gran rellevància en la física i la teoria de Galois diferenciable hi té certa relació. També el problema de trobar quines integrals de funcions elementals poden expressar-se amb altres funcions elementals es l'anàleg del problema que hem plantejar en una altra secció de trobar expressions en radicals per arrels de polinomis. En el cas diferenciable el problema està resolt usant la teoria de Picard-Vessiot. Per exemple amb la teoria de Galois diferenciable es pot demostrar:

a) La integral $\int e^{-t^2} dt$ no es pot resoldre mitjançant funcions elementals.

b) L'equació diferencial $x'' + t\,x = 0$ no es pot resoldre usant funcions elementals e integració.

Treballs com "Differential Galois Theory" de M. Kamensky [11] o millor consulteu llibres com "Introduction to differential Galois theory" de Teresa Crespo i Zbigniew Hajto [5], us permetran aprofundir en aquesta teoria.

7.5 Galois i les topologies de Grothendieck

A. Grothendieck l'any 1970

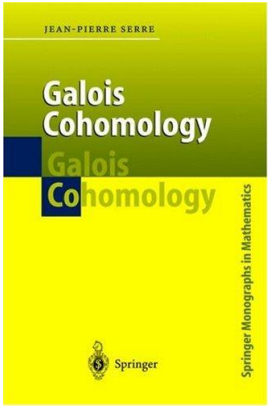
Évariste Galois introdueix la idea següent: enlloc d'estudiar els objectes estudiem els morfismes entre aquests objectes i les propietats d'aquests morfismes ens han de caracteritzar l'objecte. Aquesta idea és va reprendre de forma intensa durant els anys 1950 en el món de la Geometria, més concretament dins la Geometria Algebraica, per Alexander Grothendieck definint el que s'anomena actualment topologies de Grothendieck per a varietats. En l'actualitat gran part de la Geometria Algebraica segueix enfocada dins la direcció desenvolupada per Grothendieck.[4]

Aquesta revolució de Grothendieck es reflexa en la formulació de diverses conjectures que estan en el moment actual entre els problemes més importants en matemàtiques, alguns d'ells es troben a la llista dels problemes del Mil·leni de l'Institut Clay, la seva resolució està recompensada amb un mil·lió de dòlars. Trobareu alguna informació més sobre Grothendieck a http://en.wikipedia.org/wiki/Alexander_Grothendieck

[4] Va rebre la Medalla Fields l'any 1966.

7.6 Galois i Cohomologia i Grup Fonamental

La topologia algebraica associa certs grups a varietats topològiques, un exemple són els grups fonamentals i la cohomologia singular. Aquests objectes permeten estudiar propietats de la varietat topològica i són de gran rellevància. Aquests grups tenen certa relació amb la construcció de cert recubridor de l'objecte topològic. Podem pensar que enlloc d'estudiar directament l'objecte topològic ho trasllada a estudiar-hi certs grups de homotopia o homologia associats a l'objecte i la interrelació d'aquests dos mons (similar a la idea exposada al punt anterior). Per exemple en el grup fonamental de varietats topològiques que són també algebraiques hi apareix de forma natural el grup de Galois del cos base on està definida la varietat, l'estudi d'aquest grup fonamental s'inclou dins el programa anabelià de Grothendieck, de gran importància en la recerca actual sobre aquests temes. Igualment per a representacions de grups sobre un espai vectorial de cohomologia de certa varietat se li assigna la cohomologia de grups.



També, en una varietat algebraica sobre els racionals, el grup de Galois sobre $\mathbb{Q}$ actúa en diverses cohomologies associades a la varietat, en particular actúa en la cohomologia étale de Grothendieck. La cohomologia del grup de Galois a coeficients en les cohomologies de Grothendieck és d'importància vital per entendre l'aritmètica de la varietat àlgebraica, en particular té relació amb la conjectura de Birch i Swinnerton-Dyer. Per un estudi sobre cohomologies en grups de Galois i alguns resultats aritmètics podeu consultar Jean Pierre Serre "Galois Cohomology" [16].

7.7 Galois i Gauss: teoria de nombres

Gauss afirmava: *La reina de les matemàtiques és la Teoria de Nombres.*

Per dir-ho en paraules més planeres la teoria de nombres intenta decidir quan una equació a coeficients en els nombres enters té solució o no, i en cas que tingui solucions trobar-les explícitament. Perquè és la reina de les disciplines matemàtiques? Bé, possiblement per què els problemes són fàcils d'enunciar però la seva resolució necessita usualment técniques molt sofisticades, usant moltes rames fonamentals de la matemàtica: Àlgebra, Anàlisi, Topologia, Geometria,... Podeu trobar més detalls a http://en.wikipedia.org/wiki/Number_theory

Un exemple és l'afirmació següent: *l'equació de Fermat* $x^n + y^n = z^n$ *no té solució als enters amb* $xyz \neq 0$ *i* $n \geq 3$ *natural.*

Recordem que Wiles demostrà el 1995[5] aquesta afirmació, i recordem també que l'equació de Fermat va moure una part important de la recerca de la matemàtica els últims dos segles! Andrew Wiles per demostrar-ho usa: àlgebra, topologia, geometria i anàlisi. Hi ha més detalls al l'apartat següent de la wikipedia: http://en.wikipedia.org/wiki/Wiles'_proof_of_Fermat's_Last_Theorem

A. Wiles

Kinkichi Iwasawa (1917-1998)

La teoria de Galois és clau per a l'estudi de punts en corbes determinades per equacions definides en els enters, com l'equació de Fermat, ja que si una d'aquestes equacions té solució en una extensió dels racionals, per exemple en $\mathbb{Q}(\sqrt{2}\,)$, fent actuar el grup de Galois $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}\,))$, podem construir una altra solució de l'equació, això fa que es poguin associar objectes algebraics amb una acció de grups de Galois i això ens permet obtenir resultats sobre l'aritmètica, aquesta idea d'estudi s'inclou dins l'actual teoria Iwasawa. La teoria Iwasawa és el cor per a l'estudi dels valors enters de la funció L i en particular de la funció zeta de Riemann, funció que també té interés a la Física.

7.8 Galois i representacions de grups

Tant en la física com en la matemàtica donat un objecte on hi actua un grup se li pot associar en moltes situacions una representació de grup, i aquesta representació ha d'aportar informació de l'objecte. En Geometria, on la varietat està definida per equacions algebraiques i per exemple aquestes equacions estan definides en els nombres racionals, sempre podem considerar l'acció de grups de Galois sobre els racionals donant representacions de grup de Galois sobre els racionals. Aquests objectes són claus per a resoldre preguntes en Geometria Aritmètica que inclou preguntes dins el camp de teoria de nombres.

Andrew Wiles per a resoldre el teorema de Fermat construeix tècniques en teoria de representacions de Galois, aquestes técniques són claus per a l'estudi de la geometria algebraica aritmética de diferents varietats i de la teoria de nombres.

En el curs 2010/11 el Centre de Recerca Matemática va desenvolupar un Research Programm anual http://www.crm.cat/arithgeo/, en la direcció de l'estudi de teoria de representacions de grups de Galois. Estem parlant doncs d'un tema d'actualitat puntera mundial en matemàtica fonamental.

[5] Lamentablement A. Wiles tenia més de 40 anys quant va aportar finalment la demostració del resultat de l'equació de Fermat, motiu que va fer que no se li concedís la Medalla Fields

7.9 Hilbert i el problema invers de Galois

Évariste Galois associava a un polinomi sobre els racionals un grup finit. Una pregunta natural és: *donat un grup finit qualsevol, hi ha un polinomi sobre els racionals tal que el grup que Évariste Galois li associava coincideix amb aquest grup?* Aquest problema s'anomena el problema invers de Galois.

David Hilbert va aportar una idea fonamental en el problema invers de Galois a finals del segle XIX amb el que es coneix amb l'actualitat com "el teorema d'irreductibilitat de Hilbert". Aquest teorema sobre els racionals afirma: *Sigui $f(x_1,\dots,x_n,X) \in \mathbb{Q}[x_1,\dots,x_n,X]$ un polinomi sobre $\mathbb{Q}$ en $n+1$ variables $x_1,\dots,x_n,X$. Denotem per $\mathbb{Q}(x_1,\dots,x_n)$ el cos de fraccions de l'anell que polinomis a coeficients a $\mathbb{Q}$ en les variables $x_1,\dots,x_n$. Suposem que l'extensió de Galois sobre $\mathbb{Q}(x_1,\dots,x_n)$ generada per $f(x_1,\dots,x_n,X)$ té grup de Galois finit G. Llavors hi ha infinits $(b_1,\dots,b_n) \in \mathbb{Q}^n$ complint que $f(b_1,\dots,b_n,X)$ genera una extensió de Galois sobre $\mathbb{Q}$ amb grup de Galois G.*

David Hilbert
(1862-1943)

Usant el teorema d'irreductibilitat, Hilbert l'any 1882, va demostrar que els grups de permutacions S_m i alternat A_m es realitzen sobre $\mathbb{Q}$. I per exemple Shih al voltant de l'any 1970 demostrà que el grup $G = \mathrm{PSL}_2(\mathbb{F}_p)$ (el projectiu lineal) també satisfà la pregunta sobre els racionals.

El problema invers de Galois encara no està resolt en l'actualitat tot i que s'han fet molts avenços i hi ha molta literatura. És un dels problemes que ja va moure Hilbert finals del segle XIX i què mou encara la recerca fonamental actual (http://garden.irmacs.sfu.ca/?q=op/inverse_galois_problem).

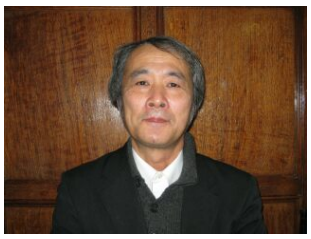
7.10 Galois i Birch amb Swinnerton-Dyer: Funcions L

La Conjectura de Birch i Swinnerton-Dyer és un dels problemes del mil·leni de l'Institut Clay que encara no està resolt (http://www.claymath.org/millennium/Birch_and_Swinnerton_Dyer_Conjecture/)

Donada una corba E, anomenada el·líptica, i definida per $y^2 = x^3 + ax + b$ on a, b racionals podem associar-li una funció de variable complexa anomenada $L(E,s)$ amb $s \in \mathbb{C}$. La conjectura de Birch i Swinnerton-Dyer descriu l'ordre d'anul.lació d'aquesta funció $L(E,s)$ en $s = 1$ i el valor del primer coeficient del desenvolupament de Taylor de $L(E,s)$ en $s = 1$. Per a definir aquesta funció L es pot usar la representació del grup de Galois actuant en els grups de cohomologia associats a una topologia de Grothendieck de la varietat E.

J.Birch i
P. Swinnerton-Dyer

La teoria Iwasawa és clau segons Kazuya Kato (ICM 2006 Madrid) per a entendre els valors enters de les funcions Zeta o L, és a dir $L(E,2)$, $L(E,2011)$,.... Aquests valors enters estan relacionats amb un objecte de geometria aritmética i per tant equipat de l'acció d'un grup de Galois. Es pot demostrar que la conjectura de Birch-Swinnerton-Dyer és un cas particular de conjetures generals de valors enters en funcions L, aquestes conjectures generals, formulades per Bloch i Kato (1990) s'anomenen les conjectures del nombre de Tamagawa, per saber-ne una mica més podeu llegir
http://en.wikipedia.org/wiki/Special_values_of_L_functions.

Fotos de Spencer Bloch and Kazuya Kato autors de la conjectura dels valors especials de funcions L anomenada també conjectura del nombre de Tamagawa

7.11 Galois i sistemes dinàmics: hipòtesi de Riemann

B. Riemann
(1826-1866)

La hipòtesi de Riemann és un altre dels problemes del mil·leni[6] i com ja hem dit interessant tant per a matemàtics com per a físics.

En aquest apartat volem introduir la visió de Deninger en atacar la hipòtesi de Riemann mitjançant sistemes dinàmics. La teoria creada per Deninger (1995-2005) pasa per a introduir aritmètica en els sistemes dinàmics i per tant hi sorgeix de forma natural l'acció del grup de Galois. Podeu consultar sobre l'aritmètica de sistemes dinàmics al llibre de Joseph H. Silverman "The Arithmetic of Dynamical Systems" [17].

7.12 Galois i matemàtics que han rebut medalles Fields

Com ja hem comentat, les medalles Fields són els equivalents en Matemàtiques dels premis Nobel, llevat que es premien tan sols a matemàtics d'edad inferior a 40 anys.

Anem ara a llistar alguns matemàtics que han obtingut medalla Fields i que en la seva recerca hi apareix de forma acusada el llegat d'Évariste Galois: Jean-Pierre Serre, Alexander Grothendieck, Alan Baker, David Mumford, Pierre Deligne, Gerd Faltins, Vladimir Drinfeld i Laurent Lafforgue.

[6] Veieu http://www.claymath.org/millennium/Riemann_Hypothesis/

J.P.Serre, A. Baker, D.Mumford, P.Deligne, G.Faltings, V.Drinfeld, L. Lafforgue.

A tall exemple expliquem l'aportació de Drinfeld i la interelació amb la teoria de Galois. Durant el segle XIX Kronecker i Weber van demostrar que qualsevol cos que conté els racionals i tal que el grup de Galois és un grup commutatiu s'immersiona dins el cos $\mathbb{Q}(\cup_n e^{2\pi i/n})$, cos resultant d'introduir-hi totes les arrels de la unitat. Drinfeld en 1975 donà un anàleg del resultat de Kronecker-Weber però sobre el cos de fraccions de l'anell de polinomis en una variable sobre un cos finit, on s'han d'introduir (enlloc de $e^{2\pi i/n}$) les arrels de certs polinomis que s'obtenen dels mòduls el·líptics anomenats actualment mòduls de Drinfeld en honor al seu descubridor.

7.13 Té futur Galois?

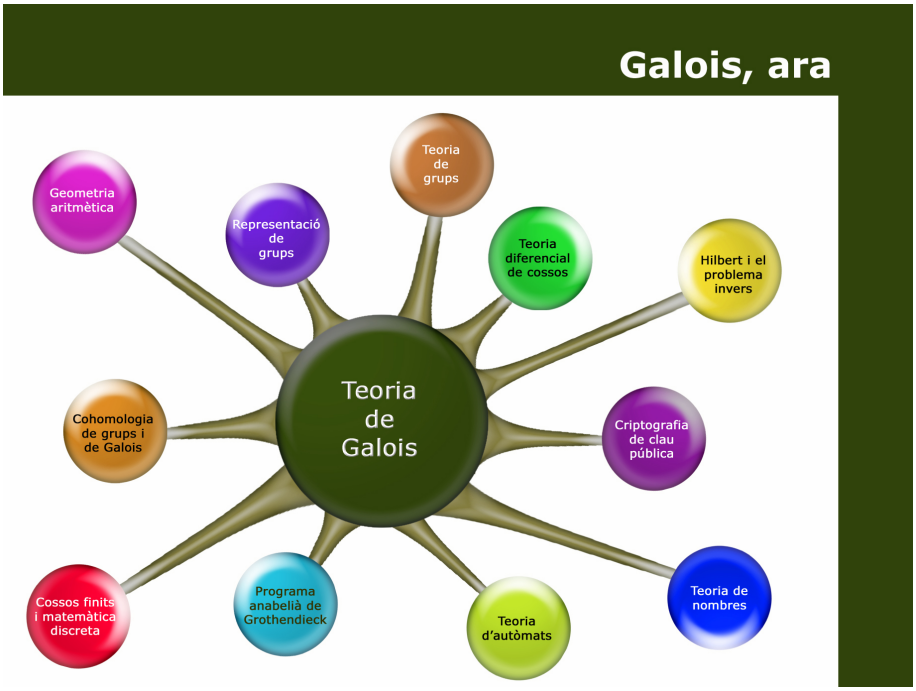
Estem convençuts que noves aplicacions o idees per la matemàtica fonamental sorgiran en els propers anys de l'impacte de la obra que va iniciar Évariste Galois! i potser també d'aplicades: ningú no sap encara si l'anàleg dels motius de Grothendieck traslladats en característica positiva, anomenats t-motius o motius d'Anderson, tindran rellevància en aplicacions computacionals i/o criptogràfiques.

És per això, i molts altres arguments, que creiem que una assignatura de teoria de Galois amb una continuació en una assignatura en teoria de Nombres (teoria que té forta interrelació amb totes les subseccions del capítol 7) haurien d'estar presents en tots els graus de Matemàtiques. En alguns graus alguna d'aquestes assignatures no hi són, potser per una suposada falta d'aplicabilitat, ja que llegint §7.12 s'intueix la seva rellevància pel món matemàtic a nivell fonamental. No obstant, recentment s'han trobat diverses aplicacions, per exemple de la teoria de corbes el·líptiques en criptografia, deixant de ser vàlid l'argument de falta d'aplicabilitat.

Cal justificar els continguts de les matèries dels graus científics per tendències influenciades cap a l'aplicació industrial o bé ha de predominar el contingut humanístic del coneixement sense pressions mercantilistes puntu-

als? Quina Universitat volem construir? Què creieu que afirmaria el "revolucionari" Évariste Galois?

Podem resumir la influència de la teoria de Galois en la matemàtica actual en el gràfic següent:



Referències

[1] F. Bars, *Teoria de Galois explicada en 30 hores*, http://ocw.uab.cat/ciencies-experimentals/teoria-de-galois-explicada-en-30-hores.

[2] C. B. Boyer, *A history of mathematics*, 2nd ed., John Wiley & Sons Inc., New York, 1991. With a foreword by Isaac Asimov; Revised and with a preface by Uta C. Merzbach.

[3] A. Chamber-Loir, *Historie de Galois aux courps finis*, Gazette de mathématiciens, SMF (janvier 2012), 59–70.

[4] D. A. Cox, *Galois theory*, Pure and Applied Mathematics (New York), Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2004.

[5] M. T. Crespo i Z. Hajto, *Introduction to differential Galois theory*, Cracow University Thechnology Press, Cracow, 2007.

[6] C. Ehrhart, *Évariste Galois: La fabrication d'une icône mathématique*, En temps et lieux, Editions de l'Ecole Pratiques de Hautes Etudes en Sciences Sociales, 2011.

[7] G. Frey i T. Lange, *Mathematical background of public key cryptography*, Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 41–73.

[8] S. D. Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, Cambridge, 2012.

[9] *Évariste Galois*, Rev. Histoire Math., SMF **17 (fas. 2)** (2011).

[10] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, Cambridge, 1986.

[11] M. Kamensky, *Differential Galois Theory*, http://www.math.huji.ac.il/~kamensky/lectures/diffgalois.pdf.

[12] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[13] A. Malet, *Obra d'Evariste Galois / introducció, selecció i comentaris per Antoni Malet*, Monografies de la Secció de Ciències, vol. 1, IEC, 1984.

[14] D. Mumford, *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston Inc., Boston, MA, 1984.

[15] P. Pesic, *Abel, Galois et les équations algébriques*, Pour la Science **366** (abril 2008).

[16] J.-P. Serre, *Cohomologie galoisienne*, 5th ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994.

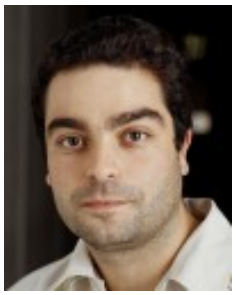
[17] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007.

[18] D. S. Thakur, *Function field arithmetic*, World Scientific Publishing Co. Inc., River Edge, NJ, 2004.

[19] C. J. Thomae, *Beitrag zur Bestimmung von $\vartheta(0,0,\dots 0)$ durch die Klassenmoduln algebraischer Funktionen*, J. Reine Angew. Math. **71** (1870), 201–222.

[20] N. Verdier, *Galois: le mathématicien maudit*, Les Génies de la science, Belin : pour la science, 2011.

Pere Ara
Departament de Matemàtiques
Universitat Autònoma de Barcelona
para@mat.uab.cat



Francesc Bars
Departament de Matemàtiques
Universitat Autònoma de Barcelona
francesc@mat.uab.cat

Publicat el 10 de desembre de 2012