



TEORIA DE GALOIS

Problemes Curs 1999-2000

Evariste Galois (1811-1832)

Irreductibilitat de polinomis.

1. Comproveu que tota arrel racional d'un polinomi mònic $p(x) \in \mathbb{Z}[x]$ és entera.
2. Proveu que $x^n - m$ on $n \in \mathbb{N}$ i m és un enter lliure de quadrats és irreductible a $\mathbb{Q}[x]$. Si denotem per $\overline{\mathbb{Q}}$ els nombres reals algebraics sobre $\mathbb{Q}$, comproveu que $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$
3. Proveu que el polinomi $x^{p-1} + x^{p-2} + \dots + x + 1$ és irreductible per a tot p primer.
4. Comproveu que si $p(x)$ és un polinomi mònic a $\mathbb{Z}[x]$ i $\overline{p}(x)$ és irreductible a $\mathbb{Z}/(q)\mathbb{Z}[x]$ per algun q primer llavors $p(x)$ és irreductible a $\mathbb{Q}[x]$.
5. Sigui K un cos i f, g dos polinomis coprimers sobre $K[x]$. Proveu que $f - yg$ és irreductible a $K(y)[x]$.
6. Descomposeu els polinomis següents en factors irreductibles al cos indicat:

i) $x^6 - 27$ a $\mathbb{Q}$.

ii) $x^5 - 4x + 2$ a $\mathbb{Q}[i]$.

iii) $x^4 - 4x + 2$ a $\mathbb{Q}[i]$

iv) $x^4 + x^3 + 1$ a $\mathbb{Z}/2\mathbb{Z}$.

7. Digueu quants polinomis de grau menor o igual que 4 hi han a $\mathbb{Z}/2\mathbb{Z}[x]$ i a $\mathbb{Z}/3\mathbb{Z}[x]$
8. Demostreu que el polinomi $X^4 - 386pX^3 + 102030pX^2 + pX + p^2, \forall p$ primer senar, és irreductible a $\mathbb{Q}[X]$.
9. Sigui $\theta = 2\pi/7$. Quin és el polinomi irreductible de $e^{i\theta}$ sobre $\mathbb{Q}$? Quin és el polinomi irreductible de $2 \cos \theta$ sobre $\mathbb{Q}$?

Polinomis simètrics i resolució d'equacions de grau 3 i 4.

10. Expreseu en funció dels polinomis simètrics elementals en tres variables, les expresions següents:

i) $x_1^2 + x_2^2 + x_3^2$

ii) $x_1^3 + x_2^3 + x_3^3$

11. Proveu la següent igualtat

$$\alpha_i^n - s_1 \alpha_i^{n-1} + s_2 \alpha_i^{n-2} + \cdots \pm s_n = 0$$

on $1 \leq i \leq n$ i $s_1, \dots, s_n$ són els polinomis simètrics elementals en les variables $\alpha_1, \dots, \alpha_n$.

12. Donats dos polinomis $f(x) = x^2 + ax + b, g(x) = x^2 + cx + d \in k[x]$ expresa una condició en funció dels parametres a, b, c, d per determinar si tenen alguna arrel en comú.

13. Escriu en funció dels seus coeficients, el discriminant de l'equació genèrica de grau 3.

14. Resol les següents equacions:

i) $x^3 + 6x - 20 = 0$

ii) $x^3 - 5x^2 + x - 5 = 0$

iii) $x^4 - 4x^2 + 4x + 1 = 0$

Extensions de cossos

15. Sigui $K = \mathbb{Z}/p\mathbb{Z}$ un cos (p primer). Supposeu que $f(x) \in K[x]$ és un polinomi irreductible de grau n . Proveu que $K[x]/(f(x)K[x])$ és un cos i dieu quant elements té.

16. Useu els polinomis irreductibles de grau 2 a $\mathbb{Z}/3\mathbb{Z}[x]$ per a construir cossos K de 9 elements. Són isomorfs? Trobeu en cada cas un element $\alpha \in K$ que generi el grup K^* .

17. Construïu un cos de 27 elements. Té el cos anterior un subcos de 9 elements? i de 3?. Existeix algun cos de 6 elements?

18. Demostreu que, si F/k és una extensió finita de cossos de grau primer, aleshores F/k és una extensió simple.

19. Sigui F/k una extensió finita de cossos. Sigui $a \in F$ un element k -algebraic. Demostreu que el grau de a sobre k divideix $[F : k]$.

20. Sigui α un element algebraic de grau senar sobre un cos k . Demostreu que $k(\alpha) = k(\alpha^2)$ i expresseu α com a funció racional de α^2 .

21. Proveu que $\mathbb{Q}[\sqrt{2}]$ i $\mathbb{Q}[\sqrt{-2}]$ no són isomorfs (com a cossos).

22. i) Donats dos elements algebraics α i β sobre un cos K , siguin $f(X) := \text{Irr}(\alpha, K)$ i $g(X) := \text{Irr}(\beta, K)$ els seus polinomis irreductibles sobre K . Demostreu que si el grau de f i el de g són primers entre sí, aleshores f és irreductible en $K(\beta)[X]$.

ii) Siguin K un cos i $L_1|K$ i $L_2|K$ extensions finites contingudes en un cos M . Denotem per L_1L_2 el mínim subcos de M que conté a L_1 i a L_2 , i l'anomenarem el compost de L_1 i L_2 en M . Proveu la desigualtat $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$ i que si els graus $[L_1 : K]$ i $[L_2 : K]$ són primers entre si, aleshores es satisfà la igualtat. És cert el recíproc? Si no doneu-ne un exemple.

23. i) Sigui α un element transcendent sobre un cos k i sigui $F := k(\alpha^{-3} - \alpha^{-2}) \subseteq k(\alpha)$. Demostreu que $k(\alpha)$ és una extensió algebraica finita de F . Calculeu el polinomi $\text{Irr}(t, F)$.

- ii) Considerem l'extensió simple $K(\alpha)/K$ on α és un element transcendent sobre K . Proveu que si $\beta \in K(\alpha)$ i $\beta \notin K$ llavors $[K(\alpha) : K(\beta)]$ és finita i β és transcendent sobre K . Proveu que si $\beta = f(\alpha)/g(\alpha)$, on f, g són coprimers a $K[x]$ llavors $[K(\alpha) : K(\beta)] = \max(\text{grau}(f), \text{grau}(g))$.
24. Siguin α, β dos elements algebraics sobre un cos k . Comproveu que si $\text{irr}(\alpha, K) = \text{irr}(\beta, k)$, llavors els cossos $k(\alpha)$ i $k(\beta)$ són isomorfs però el recíproc no és cert.
25. Sigui $E | k$ una extensió de cossos i siguin α i $\beta \in E$ dos elements algebraics sobre k de grau 3. Estudieu les diferents possibilitats per el grau $[k(\alpha, \beta) : k]$.

Extensions normals i cossos de descomposició.

26. Considerem les extensions de cossos següents

$$E = \mathbb{Q}(\sqrt[3]{2}, \omega \sqrt[3]{2}) \supseteq F = \mathbb{Q}(\sqrt[3]{2}) \supseteq k = \mathbb{Q},$$

on ω és una arrel cúbica de la unitat no trivial. Demostreu que E/k i E/F són normals, però que F/k no ho és.

27. Siguin $E = \mathbb{Q}(\sqrt[4]{2}) \supseteq F = \mathbb{Q}(\sqrt{2}) \supseteq k = \mathbb{Q}$. Demostreu que E/F i F/k són normals i que E/k no ho és.
28. Els nombres $\sqrt{-3}$ i $1 + \sqrt{-3}$ són arrels del polinomi $f(x) = x^4 - 2x^3 + 7x^2 - 6x + 12$. Existeix algun automorfisme del cos de descomposició de f sobre $\mathbb{Q}$, σ , tal que $\sigma(\sqrt{-3}) = (1 + \sqrt{-3})$?
29. Descomponeu cadascun dels polinomis següents en factors lineals en el seu cos de descomposició:

- i) $X^4 + 1 \in \mathbb{Q}[X]$.
- ii) $X^4 + 1 \in \mathbb{Q}(i)[X]$.
- iii) $X^p - t \in \mathbb{F}_p(t)[X]$, t transcendent sobre $\mathbb{F}_p$.

30. Trobeu la clausura normal de $\mathbb{Q}(\sqrt[p]{8})$.
31. Proveu que tota extensió de cossos F/k de grau 2 és una extensió normal.
32. Sigui k un cos, L una extensió de k i D un subconjunt finit de L tal que $L = k(D)$ i tal que per a tot $\alpha \in D$, $[k(\alpha) : k] \leq 2$. Proveu que L/k és normal. És cert si D no és finit?
33. És normal l'extensió $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$?
34. Descriviu els cossos de descomposició dels polinomis següents:
- i) $x^2 + 2$ sobre $\mathbb{Q}, \mathbb{Q}(i)$ i $\mathbb{Q}(\sqrt{2})$.
 - ii) $x^3 - 5$ sobre $\mathbb{Q}$ i sobre $\mathbb{Q}(\sqrt[3]{5})$.
 - iii) $(x^3 - 4)(x^2 + 2)$ sobre $\mathbb{Q}$.
 - iv) $x^6 + x^3 + 1$ sobre $\mathbb{Q}$ i sobre $\mathbb{Q}(i)$.
 - v) $x^{p^6} - 1$, amb p primer sobre $\mathbb{F}_p$.
35. Siguin k un cos, $f \in k[X]$ un polinomi mònic irreductible i L/k una extensió normal.

- i) Demostreu que tots els factors mònics irreductibles de f en $L[X]$ són conjugats respecte k .
 - ii) Demostreu que f descompon en la forma $f = (P_1 \dots P_g)^e$, amb els polinomis $P_i \in L[X]$, mònics, irreductibles, diferents i del mateix grau.
36. Sigui L/k una extensió normal i $f \in k[x]$ un polinomi mònic irreductible de grau primer. Proveu que $f(x)$ o bé és irreductible sobre $L[x]$ o bé descomposa totalment.
37. Proveu que els polinomis següents són irreductibles al cos indicat.
- i) $x^5 - 2$ sobre $\mathbb{Q}(\omega_3, \sqrt[3]{2})$.
 - ii) $x^{31} - 9x^{15} + 6x^{12} + 3$ sobre el cos de descomposició de $x^4 + 2x^2 + x + 7$.

Extensions separables.

38. Siguin $E \supseteq k$ dos cossos, i $p(x)$, $q(x)$ dos polinomis en $k[x]$. Demostreu que el màxim comú divisor no varia si es calcula a $k[x]$ o a $E[x]$.
39. Té el polinomi $X^{37} - 1$ arrels múltiples a alguna extensió de $\mathbb{Q}$? I de $\mathbb{F}_{37}$? I el polinomi $X^4 - 3X^3 + X^2 + 4$ a $\mathbb{Q}$?
40. Donat un cos k de característica $p > 0$, demostreu:
- i) Tota extensió finita de k de grau no divisible per p és separable.
 - ii) Un element α algebraic sobre k és separable si i només si $k(\alpha) = k(\alpha^{p^n})$ per a tot n .
41. Sigui k un cos de característica p primer i L/k una extensió. Suposem que tenim $\alpha, \beta \in L$ separable i purament inseparable respectivament. Proveu que $k(\alpha, \beta) = k(\alpha + \beta)$ i que si $\alpha\beta \neq 0$, $k(\alpha, \beta) = k(\alpha\beta)$.
42. Sigui p un nombre primer i $\mathbb{F}_p$ el cos finit de p elements. Comproveu que $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ és purament inseparable, on t és un element transcendent sobre $\mathbb{F}_p$.
43. Sigui k un cos de característica p primer i L una extensió purament inseparable tal que $[L : k] = p^n$. Prenem d el mínim enter tal que $L^{p^d} \subseteq k$. Proveu que $d = n$ si i només si L/k és simple.
44. Recordem que un cos k de característica $p > 0$ es diu *perfecte* si tot polinomi $f \in k[x]$ és separable sobre $k[x]$. Demostreu que:
- i) Tota extensió algebraica d'un cos perfecte és separable.
 - ii) Tot cos finit és perfecte.
 - iii) Tota extensió algebraica d'un cos perfecte k és perfecte.
 - iv) Una extensió transcendent $k(t)$ d'un cos perfecte k , no és perfecte.
45. Sigui k un cos de característica p primer. Proveu que k és perfecte si i només si el morfisme $\Phi : k \rightarrow k$, $\alpha \mapsto \alpha^p$, és un automorfisme.
46. Sigui k un cos de característica p i $k^p = \{\alpha^p \text{ tals que } \alpha \in k\}$.
- i) Proveu que k^p és un subcos de k i que $k | k^p$ és algebraica. És normal?
 - ii) Proveu que si $k | k^p$ és separable aleshores és una extensió trivial.

iii) Sigui $\bar{k}$ la clausura algebraica de k . Sigui

$$F = \{\alpha \in \bar{k} \text{ tals que } \alpha^{p^n} \in k \text{ per algun } n \in \mathbb{N}\}.$$

Demostreu que F és un subcos de $\bar{k}$, que és perfecte i que és el mínim subcos perfecte de $\bar{k}$ que conté k .

Extensions de Galois.

Nota Biogràfica sobre Evariste Galois.

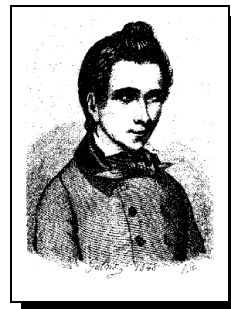
Evariste Galois neix a Bourg-la-Reine a 10km de Paris el 25 d'octubre de 1811 en una família acomodada, culta i lliberal. A l'Institut Louis le Grand de Paris fou un alumne conflictiu per la seva actitud. Allà, Galois descobrí per primer cop els textos de **Legendre** en geometria i les memòries originals de **Lagrange**: Resolució d'Equacions Numèriques, Teoria de Funcions Analítiques i Lliçons sobre el Càlcul de Funcions. Galois va fer al 1828 un primer intent fallit per entrar a l'Ecole Polytechnique, i aquell mateix any entrà en un curs amb el professor **Louis Paul Emile Richard**, matemàtic que era recordat amb veneració per **Liouville** i altres eminències de les matemàtiques d'aquell temps, i qui encoratjà a Galois a fer grans avenços. Amb Richard prepararà el nou concurs d'accés a l'Ecole Polytechnique i la seva primera memòria que presentà a l'Acadèmia de les Ciències i arribà a mans de **Cauchy**. El seu fracàs, d'altra manera 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 alcalde de Bourg-la-Reine militant al partit lliberal, cosa que va influir molt en l'ideologia del jove Galois. Al 1829 es fa càrrec de la parròquia del seu poble un nou pàrroc jove i ple de recel, qui començarà una campanya difamatòria contra aquell alcalde massa lliberal. El pare d'Evariste, en una crisi depressiva, es suïcidà el 2 de Juliol del 1829 pocs dies abans del fracàs de la prova d'accés. Un any més tard, derrocada la Restauració l'examinador que suspengué a Galois, **Dinet** era acusat per la premsa de " ... no fer dels resultats dels exàmens el primer títol per a ser admès a l'escola (...) i de tenir en compte en primer lloc les bones opinions i els bons sentiments religiosos i monàrquics de la família."

Galois fou alumne a l'Ecole Normal desde el mes d'octubre de 1829 fins que en fou expulsat el desembre de 1830 després d'haver publicat a la premsa una carta molt ofensiva contra el director. En aquest període Galois va publicar 5 articles i va presentar a l'Acadèmia de les Ciències, una primera monografia Sobre les Condicions de Resolubilitat per Radicals de les Equacions Algebraiques. Al maig de 1830, poc després de morir **Fourier**, se li comunica la pèrdua d'aquest treball. Rescriu la memòria i al mes de gener de 1831 la tornarà a presentar a l'Acadèmia. Llevat de la famosa carta testament aquest fou l'últim treball complet de Galois.

A partir de la revolució de juliol de 1830, Galois es va radicalitzar ideològicament, i un cop expulsat de l'Ecole Normal 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 ma 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 es 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 de 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 per circumstàncies no gens clares, va acabar amb un duel. Conscient de 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 tinc 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 anomenà ell mateix- un pagès el recull al matí ferit de bala i abandonat. Morí 24 hores més tard.

Els manuscrits que deixà sobre la taula quan se'n 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 fes l'esforç de llegir-los. Fou Liouville finalment qui farà arribar el treball de Galois a la sessió de l'Acadèmia d'un altre 4 de juliol, el de 1843, i qui permetrà la publicació de la seva obra al 1846.



Extret de ANTONI MALET 'Obra d'Evariste Galois'

47. Demostreu que les extensions següents són de Galois i construïu la taula de multiplicació de llurs grups de Galois.

$$(i) \quad \mathbb{Q}(\sqrt{2})/\mathbb{Q} \quad (ii) \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}.$$

48. Sigui F/k una extensió finita i separable. Demostreu que existeix una extensió E/F amb la propietat de ser mínima entre les extensions E/k finites i de Galois. Descriviu E en el cas $k = \mathbb{Q}$ i $F = \mathbb{Q}(\sqrt[4]{2})$.

49. Donat G un grup finit, proveu que existeix L/k una extensió de Galois amb grup de Galois G .

50. Pot ser el grup de Galois d'un polinomi de grau 3 isomorf a $\mathbb{Z}/6\mathbb{Z}$? I el grup de Galois d'un polinomi de grau 4 isomorf a $\mathbb{Z}/8\mathbb{Z}$? Trobeu un polinomi $f \in \mathbb{Q}[x]$ tal que el grup de Galois de f contingui un subgrup isomorf a $\mathbb{Z}/m\mathbb{Z}$ per algun $m > \text{grau}(f)$.

51. Per els polinomis següents sobre $\mathbb{Q}$, doneu el cos de descomposició, el grup de Galois, els seus subgrups i els cossos intermedis.

$$i) \quad X^4 + 9 \text{ sobre } \mathbb{Q}.$$

$$ii) \quad x^7 - 1 \text{ sobre } \mathbb{Q}.$$

$$iii) \quad x^{2n} + 2x^2 + 2 \text{ sobre } \mathbb{R}.$$

- iv) $(x^2 - 3)(x^2 - 5)(x^2 - 7)$ sobre $\mathbb{Q}$.
- v) $x^n - t$ sobre $\mathbb{C}(t)$ on t és transcendent sobre $\mathbb{C}$, i sobre $\mathbb{Q}(t)$.
- vi) $x^2 + 3x + t$ sobre $\mathbb{C}(t)$.
52. Sigui k un cos de característica diferent de 2 i E/k una extensió de Galois de grau 4. Demostreu que $\text{Gal}(E/k) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si i només si $E = k(\alpha, \beta)$ amb $\alpha, \beta \in E \setminus k$ tals que $\alpha^2, \beta^2 \in k$ i $\alpha\beta \notin k$.
53. Donat $k(t)/k$ una extensió simple i transcendent, proveu que hi ha infinits cossos intermitjos.
54. Siguin $\mathbb{Q}(\alpha_i)/\mathbb{Q}$, $i = 1, 2$ $\alpha_i \neq 0$, dues extensions de Galois linealment disjunes ($\mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}$) de graus respectius n_1 i n_2 . Demostreu que si n_1 o n_2 és senar, aleshores el grup de Galois de l'extensió $\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q}(\alpha_1\alpha_2)$ és trivial; és a dir, el producte $\alpha_1\alpha_2$ és un element primitiu de l'extensió $\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q}$.
55. Sigui p un nombre primer i k un cos de característica diferent de p . Sigui $x^p - a$ un polinomi irreductible a $k[x]$. Donada ω una arrel primitiva p -èssima de la unitat suposem que $[k(\omega) : k] = j$. Proveu que el grup de Galois de $x^p - a$, es pot generar per elements σ, τ subjectes a les relacions:
- $$\sigma^p = \tau^j = 1, \quad \sigma^l \tau = \tau \sigma$$
- on $\bar{l}$ és un element d'ordre j del grup multiplicatiu $(\mathbb{Z}/p\mathbb{Z})^*$.
56. (Teorema fonamental de l'àlgebra) Suposem que L/k és una extensió de cossos amb $[L : k] = 2$, que tot element de L té una arrel quadrada, que tot polinomi $f \in k[x]$ de grau senar té una arrel i que k té característica diferent de 2. Sigui M el cos de descomposició sobre L d'un polinomi $f \in k[x]$ irreductible i $G = \text{Gal}(M/K)$. Demostreu que:
- i) G té ordre 2^n per algun $n \in \mathbb{N}$ (Considereu un 2-subgrup de Sylow de G).
 - ii) Si $n > 1$ llavors hi ha un polinomi $g \in L[x]$ de grau dos irreductible.
 - iii) L és algebraicament tancat.
 - iv) Els nombres complexos $\mathbb{C}$ són algebraicament tancats.
57. Observeu que la condició de que k ha de tenir característica diferent de 2 a l'exercici 56 és necessària (Considereu l'extensió de descomposició de tots els polinomis irreductibles de grau senar sobre $\mathbb{Z}/2\mathbb{Z}$).

Cossos finits.

58. Proveu que un cos F és finit si i només si F^* és cíclic.
59. Sigui k un cos finit de característica diferent de 2. Proveu que la suma de tots els elements és 0.
60. Calculeu $\text{Gal}(X^3 + X^2 + 1 \mid \mathbb{F}_5)$.
61. Sigui k un cos de característica p i sigui $f(x) = x^p - x - a$ per algun $a \in k$. Proveu que $f(x)$ és irreductible o bé descompon totalment.
62. Sigui $\mathbb{F}_q$ on $q = p^n$ un cos finit i m un enter positiu. Llavors $(x^{q^m} - x) = \prod f(x)$, on f varia sobre tots els polinomis mòncics irreductibles a $\mathbb{F}_q[x]$ de grau $d \mid m$.

63. Sigui $f(x) \in k[x]$ un polinomi irreductible amb k un cos finit i E una extensió finita de k . Proveu que:

- i) Si $f(x)$ té una arrel a E aleshores les té totes.
- ii) E/k és una extensió de Galois.
- iii) Si $f(x)$ és de grau primer senar aleshores $\Delta(f) \in K^{*2}$.

64. Sigui L un cos algebraicament tancat de característica p .

- i) Proveu que la clausura algebraica de $\mathbb{F}_p$ és:

$$\bar{\mathbb{F}}_p = \{\alpha \in L \mid \alpha^{p^n} = \alpha \text{ per algun } n\}.$$

- ii) Proveu que el morfisme de Frobenius Φ és un automorfisme de $\bar{\mathbb{F}}_p$ i dieu quin ordre té.

- iii) Per a cada $n \geq 1$ denotem per $\mathbb{F}_{p^n}$ el subcos de L amb p^n elements. Proveu que

$$K = \bigcup_{p \nmid n} \mathbb{F}_{p^n},$$

és un subcos de $\bar{\mathbb{F}}_p$. És algebraicament tancat?

Grups.

Repàs de grups

65. Donat G un grup i H un subgrup amb $(G : H) = 2$, proveu que $H \trianglelefteq G$.

66. Sigui G un grup i H, K subgrups de G , proveu:

- i) $HK = \{hk \mid h \in H, k \in K\}$ és un subgrup de $G \Leftrightarrow HK = KH$.
- ii) Si H i K són normals en G aleshores $HK \trianglelefteq G$ i $H \cap K \trianglelefteq G$.
- iii) $K \trianglelefteq G \Rightarrow H \cap K \trianglelefteq H$ i $H/H \cap K \cong HK/K$.
- iv) Si $K \subseteq H$ són subgrups normals de G . Aleshores $K \trianglelefteq H$ i $(G/K)/(H/K) \cong G/H$.
- v) $H_1 \trianglelefteq H_2, H_2 \trianglelefteq H_3 \not\Rightarrow H_1 \trianglelefteq H_3$.

67. Demostreu que si G és un grup abelià finit i p és un nombre primer tal que p divideix $|G|$, aleshores G té algun element d'ordre p .

68. (*Teorema de Cayley*) Sigui G un grup finit. Proveu que existeix un enter positiu n tal que G és un subgrup de S_n .

Grups resolubles

69. Sigui S_4 el grup simètric d'ordre 4.

- i) Demostreu que el subconjunt $V_4 := \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ de S_4 és un subgrup normal d' S_4 . S'anomena grup de Klein.
- ii) Demostreu que els únics subgrups transitius d' S_4 són $S_4, A_4, V_4, C_4 := \langle (1, 2, 3, 4) \rangle, D_4 := V_4 \cup \{(1, 4, 2, 3), (1, 3, 2, 4), (1, 2), (3, 4)\}$ i els seus conjugats.

70. Demostreu que tot grup G d'ordre $2n$ on n és un nombre senar, té un subgrup H amb $(G : H) = 2$. Proveu que no existeix cap grup simple d'ordre 29046.
71. Sigui p, q dos primers diferents. Suposem que G és un grup d'ordre $p^n q$ per algun enter n i G té un únic subgrup H amb q elements. Proveu que G és resoluble.
72. Sigui G un grup. El *subgrup derivat* de G , que denotarem per G' , es defineix com el subgrup generat per $\{x^{-1}y^{-1}xy \mid x, y \in G\}$.
- i) Demostreu que per a tot endomorfisme φ de G , $\varphi(G') \subseteq G'$.
 - ii) Deduïu d'aquí que G' és normal en G .
 - iii) Demostreu que G/G' és un grup abelià (s'anomena l'*abelianitzat* de G , G^{ab}).
 - iv) Demostreu que si $N \trianglelefteq G$ i G/N és abelià, aleshores $G' \subseteq N$.
- Anomenarem $G^{(0)} := G$, $G^{(n)} := (G^{(n-1)})' \forall n \geq 1$ la *sèrie derivada* de G .
73. Donat G un grup, demostreu que $G^{(n)} = 1$ per algun n si i només si G és resoluble.
74. Calculeu la sèrie derivada de S_n per a tot $n \geq 1$.
75. Proveu que si $n \geq 5$, A_n és generat per m -cicles per qualsevol $m \geq 3$ senar.

Resolució d'equacions.

76. Sigui k un cos de característica 0 i p un nombre primer. Proveu que si $a \in k$ i a no té cap arrel p -èsima a k , llavors $x^p - a$ és irreductible a $k[x]$ (és a dir, si és reductible, té algun factor lineal). Descriviu la torre radical per a les solucions de $x^p - a$ i la cadena de grups corresponent.
77. Sigui $f \in \mathbb{Q}[x]$ de grau 3 amb discriminant Δ . Demostreu que f té tres arrels reals si i només si $\Delta \geq 0$. (Indicació: f té una o tres arrels reals).
78. Sigui k un subcos de $\mathbb{R}$ i $f \in k[x]$ un polinomi cúbic irreductible amb tres arrels reals.
- i) Sigui $L = k(r)$, on $r \in \mathbb{R}$ i $r^p \in k$ per algun primer p . Proveu que f és irreductible sobre L .
 - ii) Sigui k un subcos de $\mathbb{R}$ i $f \in k[x]$ com a l'apartat anterior. Si L/k és una extensió amb una torre radical tal que $L \subseteq \mathbb{R}$ llavors f és irreductible a $L[x]$.
79. Doneu un exemple d'un polinomi $f \in \mathbb{Q}[x]$ resoluble per radicals i tal que el seu cos de descomposició no té una torre radical.
80. Sigui k un cos de característica 0 amb totes les arrels de la unitat necessàries. Sigui $K = k(s_1, \dots, s_n)$ on s_i són transcendents. Prenem $f(x) = x^n + a_1 x^{n-1} + \dots + a_n = (x - t_1) \dots (x - t_n)$ de tal manera que $L = k(t_1, \dots, t_n)$ és el cos de descomposició de $f(x)$ sobre K .
- i) Proveu que si $K = K_0 \subset K_1 \subset \dots \subset K_n = L$ és una torre radical, llavors $K_1 = K(\sqrt[n]{\Delta})$.
 - ii) Proveu que si $n \geq 5$ llavors K_1 no té cap extensió radical dins de L . Dedueu d'aquí que L/K no pot ser una torre radical.
81. Sigui $f(x) \in k[x]$ un polinomi irreductible de grau primer p resoluble per radicals i k un cos de característica 0.

- i)* Proveu que les arrels de f es poden ordenar $a_1, \dots, a_p$ de tal manera que els automorfismes del grup de galois siguin de la forma $\sigma(a_i) = a_{ri+s}$, per enters r, s amb $(r, p) = 1$, i prenent els indexos i mòdul p .
- ii)* Deduïu d'aquí que l'equació genèrica de grau 5 no és resoluble per radicals.
82. (*Teorema de Galois*) Sigui k un cos de característica 0, i $f \in k[x]$ irreductible de grau primer. Proveu que $f(x)$ és resoluble per radicals si i només si tota arrel es pot expressar racionalment en funció de dues altres arrels qualsevol.
83. Definim els grups dièdrics com $D_{2n} = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle$.
- i)* Proveu que D_{2n} és resoluble.
- ii)* Suposem que n és una potència de 2. Sigui $f(x) \in \mathbb{Q}[x]$ amb grup de galois D_{2n} . Trobeu una cadena de subgrups

$$D_{2n} = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright \{Id\}$$

complint $(G_i : G_{i+1}) = 2$ per a tot i . Utilitzeu-la per demostrar que el cos de descomposició del polinomi f sobre $\mathbb{Q}$ és una extensió radical sobre $\mathbb{Q}$.

Construccions amb regla i compàs.

84. Demostreu que la duplicació del cub és impossible.
85. Demostreu que la trisecció de l'angle és impossible.
86. Sigui ξ una arrel primitiva n -èsima de la unitat sobre $\mathbb{Q}$ i sigui $\eta = \xi + \xi^{-1}$. Calculeu $\text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}(\eta))$.
87. Doneu expressions radicals úniques per a $e^{2\pi i/5}$ i $e^{2\pi i/7}$ i descriviu la construcció del pentàgon regular.
88. Demostreu que si tenim dibuixada la cúbica $Y^2 = X^3$, aleshores el problema de la duplicació del cub té solució amb regla i compàs.