PROBLEMES D'ÀLGEBRA ABSTRACTA
I. TEORIA DE GRUPS
Curs 09–10

1. Sigui G un grup. Comproveu que l'element neutre de G és únic, que cada element de G té un únic invers i que $(xy)^{-1} = y^{-1}x^{-1}$.

2. Demostreu que en un grup G, per a qualsevol parell d'elements $x, y \in G$, l'ordre de xy coincideix amb l'ordre de yx .

3. Sigui G un grup i $x \in G$ un element d'ordre n. Demostreu que $\operatorname{ord}(x^{-1}) = n$ i que si $k \in \mathbb{N}$, llavors $\operatorname{ord}(x^k) = n/\operatorname{mcd}(n, k)$.

4. Demostreu que si H és un subgrup de G i $g \in G$, aleshores $g^{-1}Hg$ també és subgrup de G.

5. Demostreu que la funció exponencial estableix un isomorfisme entre el grup additiu $(\mathbb{R}, +)$ i el grup multiplicatiu $(\mathbb{R}^*, \cdot)$.

6. Sigui $\omega \in \mathbb{C}$ una arrel cúbica primitiva de la unitat. Demostreu que les matrius

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}$$

formen un grup amb la multiplicació. Estabiu un isomorfisme entre aquest grup i el grup simètric $\mathfrak{S}_3$.

7. Demostreu que el grup additiu $(\mathbb{Q}, +)$ i el grup multiplicatiu $(\mathbb{Q}^*, \cdot)$ no són isomorfs.

8. Sigui $f : G_1 \to G_2$ un homomorfisme de grups. Comproveu que si H_1 és subgrup de G_1, $f(H_1)$ ho és de G_2 i que si H_2 és subgrup de G_2, $f^{-1}(H_2)$ ho és de G_1. Comproveu, a més, que si H_2 és normal a G_2, $f^{-1}(H_2)$ ho és a G_1 però que, en canvi, si H_1 és normal a G_1 llavors $f(H_1)$ no té perquè ser-ho a G_2 i l'únic que es pot assegurar és que és normal a $\operatorname{Im} f$.

9. Comproveu que $\operatorname{Inn} G = \{ \gamma_a : x \mapsto axa^{-1} \mid a \in G\}$ és un subgrup normal de $\operatorname{Aut} G$.

10. Demostreu que si un grup G té un subgrup propi d'índex finit, també té un subgrup normal propi d'índex finit.

11. Sigui H un subgrup de $Z(G)$. Proveu que si G/H és cíclic, G és abelià.

12. Sigui A un grup abelià finit. Demostreu que si l'ordre de A es divideix per un primer p, aleshores existeixen elements a A d'ordre p.

13. Siguin G un grup cíclic amb generador x i H un subgrup de G. Demostreu que H és cíclic amb generador x^k on k és el mínim del conjunt $\{m \in \mathbb{N} : x^m \in H\}$. Quin és l'ordre de H?

14. Demostreu que

a) Els subconjunts $n\mathbb{Z}$ són tots els subgrups de $\mathbb{Z}$.

b) Tot grup cíclic és isomorf a $\mathbb{Z}$ o a $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ per a algun $n > 0$.

c) Tot subgrup i tot quocient d'un grup cíclic és cíclic.

d) Per a cada enter $d \mid n$, el grup $\mathbb{Z}_n$ (i, per tant, tot grup cíclic d'ordre n) té exactament un subgrup d'ordre d.

e) $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ si, i només si, $\mathrm{mcd}(n, m) = 1$.

e) El grup $\mathbb{Z}$ té dos generadors, 1 i -1. El grup $\mathbb{Z}_n$ té $\varphi(n)$ generadors.

f) El grup $\mathrm{Aut}\,\mathbb{Z}$ és isomorf a $\mathbb{Z}/2\mathbb{Z}$ i $\mathrm{Aut}\,\mathbb{Z}_n$ és isomorf a $\mathbb{Z}_n^*$.

15. Doneu un exemple de grup no cíclic tal que tots els seus subgrups propis siguin cíclics.

16. Identifiqueu el grup diedral D_{2n} com a subgrup de $\mathfrak{S}_n$.

17. Siguin a, b elements d'ordre 2 a un grup G tals que ab te ordre $n \geq 3$. Demostreu que $\langle a, b\rangle$ és isomorf al grup diedral D_{2n}.

18. Trobeu el reticle de subgrups de D_8. Observeu que encara que el grup no és abelià tots els seus subgrups propis són abelians.

19. Calculeu l'ordre de tots els elements del grup diedral D_{2n}. Si n és un nombre primer, calculeu-ne els subgrups i digueu quins són normals.

20. Siguin H i K subgrups d'un grup G. El conjunt HK no sempre és un grup, però, com que és una reunió de classes laterals per l'esquerra de K, podem definir $[HK : K]$ com el cardinal d'aquest conjunt de classes laterals. Comproveu les fórmules següents:

a) $|HK||H \cap K| = |H| \cdot |K|$.

b) $[HK : K] = [H : H \cap K]$.

21. Siguin H i K subgrups d'un grup G. Demostreu que:

a) El conjunt HK és un subgrup de G si, i només si, $HK = KH$.

b) Si H és normal a G aleshores HK és un subgrup de G.

c) Si H i K són normals a G, HK també ho és.

22. Siguin G_1 i G_2 dos grups i $\phi : G_2 \to \operatorname{Aut} G_1$ un homomorfisme de grups. Fem servir la notació ${}^b a$ per indicar $\phi(b)(a)$. Sobre el producte cartesià $G_1 \times G_2$ definim l'operació

$$(a_1, b_1)(a_2, b_2) = (a_1 \, {}^{b_1}a_2, b_1 b_2).$$

a) Demostreu que $G_1 \times G_2$ amb l'operació definida té estructura de grup. Aquest grup s'anomena *producte semidirecte* de G_1 i G_2 (respecte ϕ) i s'escriu $G_1 \rtimes_\phi G_2$.

b) Considereu el cas $G_1 = \mathbb{Z}_n$, $G_2 = \mathbb{Z}_2$ i ϕ l'homomorfisme que envia el generador de $\mathbb{Z}_2$ a l'automorfisme de $\mathbb{Z}_n$ donat per $a \mapsto -a$. Demostreu que el producte semidirecte $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ és isomorf al grup diedral D_{2n}.

c) Considereu el cas $G_1 = A$ un grup abelià, $G_2 = \mathbb{Z}_2$ i ϕ l'homomorfisme que envia el generador de $\mathbb{Z}_2$ a l'automorfisme de A donat per $a \mapsto -a$. Calculeu explícitament la cadena de derivats del grup $A \rtimes_\phi \mathbb{Z}_2$ i demostreu que aquest grup és resoluble.

23. Siguin a i b elements d'un grup G. El *commutador* de a i b és

$$[a, b] = aba^{-1}b^{-1} .$$

S'anomena així perquè $ab = [a, b]\, ba$. Si $S, T \subseteq G$ són subconjunts, posem

$$[S, T] = \langle [a, b] \mid a \in S, b \in T \rangle .$$

El subgrup $G' = [G, G]$ es diu el *grup derivat* de G. Comproveu que:

a) G' és un subgrup normal de G amb quocient G/G' abelià.

b) Tot homomorfisme $G \to A$ en un grup abelià factoritza a través de G/G'.

c) G' és el més petit subgrup normal de G amb quocient abelià.

24. Trobeu el subgrup derivat d'un grup diedral D_{2n}. Identifiqueu el grup D_{2n}/D'_{2n}.

25. Considerem la cadena de grups derivats

$$G^{(0)} = G,\ G^{(1)} = G', \ldots,\ G^{(i+1)} = G^{(i)'}, \ldots$$

Demostreu que G és resoluble si, i només si, $G^{(n)} = 1$ per a algun n.

26. *Lema de Burnside.* Sigui G un grup finit operant a un conjunt finit X. Per a cada $a \in G$ diguem n_a al nombre de punts fixos per a; és a dir, $n_a = \#\{x \in X \mid ax = x\}$. Demostreu que

$$|G\backslash X| = \frac{1}{|G|} \sum_{a \in G} n_a.$$

Indicació: compteu el nombre de parells $(a, x) \in G \times X$ tals que $ax = x$.

27. Sigui G un grup operant a un conjunt X. Una relació d'equivalència $\sim$ a X es diu *compatible* amb l'acció de G si $x \sim y \ \Rightarrow\ ax \sim ay$. En tal cas, tenim una acció natural de G sobre el conjunt de classes d'equivalència $X/\sim$. L'acció de G sobre X es diu *primitiva* si les úniques relacions d'equivalència compatibles amb l'acció són la trivial (dos elements sempre estan relacionats) i la d'igualtat.

Demostreu que una acció transitiva és primitiva si, i només si, l'estabilitzador G_x d'un element qualsevol és un subgrup propi maximal de G.

28. Una acció es diu *k-transitiva* si donats $x_1, \ldots, x_k$ i $y_1, \ldots, y_k$, dos conjunts de k elements diferents de X, existeix un element $a \in G$ tal que $ax_1 = y_1, \ldots, ax_k = y_k$.

a) És clar que $\mathfrak{S}_n$ opera n-transitivament sobre el conjunt $\{1, \ldots, n\}$. Quin és el grau de transitivitat de $\mathfrak{A}_n$?

b) Demostreu que tota acció 2-transitiva és primitiva.

29. Sigui G un grup.

a) Proveu que si H és un subgrup normal de G, aleshores $G/Z_G(H)$ és isomorf a un subgrup de $\mathrm{Aut}(H)$. Per a quins H és el subgrup trivial?

b) Proveu que si G és finit i H n'és un subgrup normal de cardinal el més petit primer que divideix $|G|$, aleshores $H \subseteq Z(G)$.

c) Suposeu que $|G| = pq$ amb p, q primers tals que $p < q$ i $p \nmid q - 1$. Demostreu que G és cíclic.

30. Considerem el grup dels quaternions

$$H_8 =< a, b \mid a^4 = e, a^2 = b^2, ba = a^{-1}b > .$$

a) Escriu tots els elements de H_8. Demostra que en té 8.

b) Calcula l'ordre de tots els elements de H_8. Demostra que H_8

c) Fes la partició del grup H_8 en classes de conjugació.

d) Troba tots els subgrups de H_8. Dibuixa el reticle de subgrups. Digues quins són normals.

e) Troba el derivat de H_8.

f) Troba el centre de H_8. Prova que $H_8/Z(H_8)$ és abelià, digues quina és la seva estructura i quants subgrups té.

g) Demostra que H_8 és resoluble.

h) Demostra que no hi ha cap acció transitiva de H_8 que doni lloc a un monomorfisme $H_8 \hookrightarrow S_4$.

31. Sigui p el més petit nombre primer que divideix l'ordre d'un grup G. Demostreu que tot subgrup d'índex p a G és normal.

32. Sigui G un grup d'ordre p^2, p primer. Demostreu que G és abelià.

33. Sigui G un grup finit. Demostreu que G és un p-grup si, i només si, tots els seus elements tenen ordre una potència de p. Proveu també que G és un p-grup si, i només si, tots els seus subgrups propis són p-grups.

34. Demostreu que un grup és producte directe dels seus subgrups de Sylow si, i només si, tots aquests subgrups són normals.

35. Sigui G un grup d'ordre pq, amb p i q primers diferents. Demostreu que G és resoluble.

36. Sigui G un grup d'ordre pqr, amb p, q i r primers diferents. Demostreu que G és resoluble.

37. Demostra que si p i q són nombres primers, tot grup de cardinal p^2q és resoluble.

38. Siguin A un anell (commutatiu) i $G = GL_2(A)$ el grup de les matrius 2×2 amb coeficients a A i determinant invertible. Sigui H el subconjunt de G format per les matrius triangulars superiors. Demostreu que H és un subgrup de G, que en general no és abelià però que sempre és resoluble.

39. Trobeu tots els 3−subgrups de Sylow de $S_4 \times \mathbb{Z}/3\mathbb{Z}$. Demostreu que no hi ha cap grup simple d'ordre 72.

40. Sigui $A = \{1, 2, 4\} \subset \mathbb{Z}/7\mathbb{Z}$. Definim

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in A,\ b \in \mathbb{Z}/7\mathbb{Z} \right\}.$$

a) Demostreu que A és un subgrup del grup multiplicatiu $(\mathbb{Z}/7\mathbb{Z})^*$ i que G és un subgrup del grup lineal $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$.

b) És G abelià? És simple? És resoluble?

c) Trobeu explícitament un p-subgrup de Sylow de G per a cada p.

d) Doneu una sèrie de composició de G.

41. Siguin G un grup finit simple, i H un subgrup de G. Demostreu que $|G|$ divideix $[G : H]!$. Concloeu que tots els grups d'ordre $4p$ o $4p^2$ (amb p primer) són resolubles.

PROBLEMES D'ÀLGEBRA ABSTRACTA
II. Anells
Curs 09–10

1. Proveu que $A = \left\{ \frac{n}{2^k} \mid n, k \in \mathbb{Z} \right\}$ és un anell i trobeu les seves unitats.

2. Sigui p un nombre primer. Considereu el conjunt

$$E_p = \left\{ \frac{n}{m} \mid n, m \in \mathbb{Z},\ p \nmid m \right\}.$$

Proveu que E_p és un anell i trobeu les seves unitats. Demostreu que el conjunt $I_p = \left\{ \frac{n}{m} \in E_p \text{ tals que } p \mid n \right\}$ és un ideal de E_p. Descriviu el quocient E_p/I_p.

3. Siguin A i B anells.

i) Proveu que el grup d'unitats de $A \times B$ és isomorf al producte directe dels grups d'unitats A^* i B^*.

ii) Proveu que $I = A \times 0$ és un ideal de $A \times B$ i que $(A \times B)/I$ és isomorf a B.

4. Sigui $\mathfrak{a}$ un ideal de l'anell A. Proveu que

$$\mathrm{Ann}(\mathfrak{a}) = \{x \in A : xa = 0\ \forall a \in \mathfrak{a}\}$$

és també un ideal de l'anell A. S'anomena *anul·lador* de $\mathfrak{a}$.

5. Siguin G un grup abelià i $A = \mathrm{End}(G)$. Demostreu que A és un anell unitari. Doneu un exemple de grup G per al qual A sigui commutatiu i proveu que $\mathrm{End}(\mathbb{Z} \times \mathbb{Z})$ és no commutatiu.

6. Siguin A un anell i $a \in A^*$. Demostreu que l'aplicació de A en A definida per $x \mapsto axa^{-1}$ és un automorfisme de A

7. Caracteritzeu els divisors de zero de l'anell de matrius $M_2(\mathbb{R})$.

8. Donats $m \in \mathbb{Z}_n$, definim

$$A_{m,n} = \left\{ \begin{pmatrix} a & mb \\ b & a \end{pmatrix} \in M_2(\mathbb{Z}_n) | a, b \in \mathbb{Z}_n \right\}$$

i) Demostreu que $A_{m,n}$ és un subanell commutatiu de $M_2(\mathbb{Z}_n)$.

ii) Proveu que $A_{3,7}$ és un cos.

iii) Proveu que l'aplicació

$$\begin{array}{ccc} \phi : A_{3,7} & \longrightarrow & A_{5,7} \\ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} & \longrightarrow & \begin{pmatrix} a & 5(3b) \\ 3b & a \end{pmatrix} \end{array}$$

és un isomorfisme d'anells.

iv) Proveu que $A_{2,7}$ no és un cos.

9. Dos ideals $\mathfrak{a}$ i $\mathfrak{b}$ d'un anell A són *coprimers* si $\mathfrak{a} + \mathfrak{b} = A$. Anàlogament es defineix el concepte de coprimers per a una família finita d'ideals i el de coprimers dos a dos. Si $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ són coprimers dos a dos, demostreu que:

1. $\mathfrak{a}_1$ i $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ són coprimers,
2. $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$.

10. *Teorema xinès del residu.* Siguin $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals coprimers dos a dos. Demostreu que donats elements $x_i \in A$ existeix un element $x \in A$ tal que $x \equiv x_i \pmod{\mathfrak{a}_i}$ per a tot i.

11. Siguin $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals d'un anell A i $\phi : A \to (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$ l'homomorfisme que és la projecció canònica sobre cada coordenada. Comproveu que $\ker \phi = \bigcap \mathfrak{a}_i$ i que ϕ és exhaustiva si, i només si, els $\mathfrak{a}_i$ són coprimers dos a dos.

12. Siguin A un anell i $\mathfrak{a}$ un ideal de A. Demostreu que hi ha una correspondència bijectiva entre el conjunt d'ideals primers de A que contenen $\mathfrak{a}$ i el conjunt d'ideals primers de l'anell quocient $A/\mathfrak{a}$.

13. Sigui A un anell. Un element $a \in A$ s'anomena *nilpotent* si existeix un $n \geq 1$ tal que $a^n = 0$. Demostreu que la suma d'un nilpotent i una unitat és una unitat.

14. Sigui $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ *l'anell dels enters de Gauss*. Demostreu que les seves unitats són $\{\pm 1, \pm i\}$ i que $N : \mathbb{Z}[i] \to \mathbb{Z}$ definida per $N(z) = z\bar{z} = |z|^2$ és una norma euclidiana.

15. Demostreu que $I = \{f \in \mathbb{Z}[x] : f(0) \text{ és parell }\}$ és un ideal de $\mathbb{Z}[x]$, que és maximal i que no és principal.

16. Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomi amb coeficients en l'anell A. Demostreu que:

a) f és una unitat si, i només si, a_0 és una unitat i els a_i són nilpotents per a $i > 0$.

b) f és nilpotent si, i només si, tots els a_i ho són.

c) f és un divisor de zero si, i només si, existeix una constant no nul·la $a \in A$ tal que $af = 0$.

17. Sigui A un anell en el qual 2 no és un divisor de zero. Un polinomi $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ (amb $n \geq 2$) és *alternat* si, per cada permutació $\sigma \in \mathfrak{S}_n$, $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = (\operatorname{sgn}\sigma) f(X_1, \ldots, X_n)$. Comproveu que $\Delta = \prod_{i<j}(X_i - X_j)$ és un polinomi alternat. Demostreu que els polinomis alternats són els de la forma Δf, amb f un polinomi simètric.

18. Siguin $f, g \in K[X]$ dos polinomis amb coeficients en un cos K. Demostreu que $\operatorname{disc}(fg) = \operatorname{disc} f \operatorname{disc} g \operatorname{Res}(f, g)^2$.

19. Sigui p un nombre primer. Calculeu el discriminant del polinomi ciclotòmic $\phi_p(X) = (X^p - 1)/(X - 1) \in \mathbb{Z}[X]$.

20. *Matriu de Sylvester*. Siguin $f(X) = A_0X^n + \cdots + A_n$ i $g(X) = B_0X^m + \cdots + B_m$ dos polinomis amb coeficients en un cos K. Considereu la matriu quadrada de dimensió $n + m$

$$M = \begin{pmatrix} A_0 & & A_n & & \\ & A_0 & & A_n & \\ & & \cdots & \cdots & \\ & & A_0 & & A_n \\ B_0 & & B_m & & \\ & B_0 & & B_m & \\ & & \cdots & \cdots & \\ & & B_0 & & B_m \end{pmatrix}$$

Demostreu que $\operatorname{Res}(f, g) = \det M$. Indicació: multipliqueu M per la matriu de Vandermonde que té a les columnes les arrels de $f(X)$ i les de $g(X)$.

21. Siguin $f, g \in K[X]$ polinomis de graus n i m, respectivament amb coeficients en un cos K. Demostreu que existeixen polinomis r i s, de graus menors que m i n, respectivament, tals que $\operatorname{Res}(f,g) = f(X)r(X) + g(X)s(X)$.

Indicació: considereu el sistema lineal sobre $A[X]$ que té per matriu la matriu de Sylvester d'aquests polinomis, per solució el vector

$$(X^{n+m-1}, X^{n+m-2}, \ldots, X, 1),$$

i plantejeu-vos la seva resolució per Cramer.

22. Si $A[X]$ és factorial, demostreu que per a qualssevol $f, g \in A[x]$ és

$$\operatorname{Res}(f,g) = 0 \iff (f,g) \neq 1.$$

23. Demostreu que els elements nilpotents són un ideal de l'anell A. Se l'anomena *radical* de A i es denota $\mathfrak{Rad}\, A$.

24. Demostreu que el radical d'un anell és la intersecció de tots els seus ideals primers. Indicació: si $a \in A$ no és nilpotent, apliqueu el lema de Zorn al conjunt dels ideals que no contenen cap potència de a i comproveu que un element maximal d'aquest conjunt és un ideal primer.

25. Definiu el radical d'un ideal $\mathfrak{a} \in A$ (de dues maneres diferents, corresponents als dos exercicis anteriors). Comproveu que $\mathfrak{Rad}(\mathfrak{Rad}\, \mathfrak{a}) = \mathfrak{Rad}\, \mathfrak{a}$. Definiu el radical d'un element en un domini d'ideals principals. Què és el radical d'un nombre enter?

26. Un anell *local* és un anell que té un únic ideal maximal.

a) Siguin A un anell i $\mathfrak{m}$ un ideal tal que tot element de $A \setminus \mathfrak{m}$ és una unitat. Demostreu que A és local i que $\mathfrak{m}$ és el seu ideal maximal.

b) Siguin A un anell i $\mathfrak{m}$ un ideal maximal tal que tot element de la forma $1 + x$, $x \in \mathfrak{m}$, és una unitat. Demostreu que A és local.

27. Demostreu que si I, J són ideals d'un anell A i $\wp$ és un ideal primer de A que conté $I \cap J$, aleshores o bé $I \subseteq \wp$ o bé $J \subseteq \wp$.

28. Demostreu que si $x^3 + Ax + B \in \mathbb{Z}[x]$ és irreductible, aleshores el seu discriminant és un enter diferent de $0, \pm 1$.

29. Demostreu que si A és un anell (unitari commutatiu) finit, tot ideal primer de A és maximal.

30. Considereu el morfisme $\mathbb{Z}[X] \to \mathbb{Z}_2[X] \to \mathbb{Z}_2[X]/(X^3 + X + 1)$ obtingut per composició del morfisme de reducció dels coeficients mòdul 2 amb la

projecció al quocient. Proveu que és exhaustiu i que el seu nucli és $\mathfrak{m} = (2, X^3 + X + 1)$. És $\mathfrak{m}$ un ideal principal?

31. Demostreu que si un anell A té algun ideal primer sense divisors de zero, aleshores A és íntegre.

32. Sigui A un anell commutatiu i unitari. Fixem a un element no nul de A. Proveu que existeix un ideal propi de A maximal entre els ideals que no contenen a.

33. Proveu que els elements de la forma $\pm(1+\sqrt{2})^n$ amb $n \in \mathbf{Z}$ són totes les unitats de l'anell $\mathbf{Z}[\sqrt{2}]$. (Indicació: si u és una unitat amb $1 \leq u < 1+\sqrt{2}$, aleshores $u = 1$.)

PROBLEMES D'ÀLGEBRA ABSTRACTA
III. COSSOS I TEORIA DE GALOIS
Curs 09–10

1. Demostreu que si K té característica $p > 0$, l'aplicació $a \mapsto a^p$ és una immersió $K \to K$ que deixa fixos precisament els elements del cos primer.

2. Demostreu que tot cos finit és perfecte.

3. Sigui K un cos finit de característica p. Demostreu que tot element de K és algebraic sobre el cos primer $\mathbb{Z}_p$.

4. Sigui K un cos de característica diferent de 2. Demostreu que tota extensió E/K de grau 2 és de la forma $E = K(\alpha)$, on $\alpha \in E$ és tal que $\alpha^2 \in K$.

5. Siguin p i q primers diferents. Proveu que $\sqrt{q} \notin \mathbb{Q}(\sqrt{p}\,)$, que el grau $[\mathbb{Q}(\sqrt{p}, \sqrt{q}\,) : \mathbb{Q}]$ és 4 i que $\mathbb{Q}(\sqrt{p}, \sqrt{q}\,) = \mathbb{Q}(\sqrt{p} + \sqrt{q}\,)$.

6. Demostreu que $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,) = \mathbb{Q}(\sqrt{a} + \sqrt{b}\,)$ per a tot $a, b \in \mathbb{Q}$.

7. Siguin F_1, F_2 cossos intermedis de l'extensió finita E/K. Demostreu que si els graus $[F_1 : K]$ i $[F_2 : K]$ són relativament primers, aleshores el grau de la composició és $[F_1F_2 : K] = [F_1 : K][F_2 : K]$.

8. Siguin F_1, F_2 subcossos d'un cos E i $\sigma : E \to L$ una immersió. Demostreu que $(F_1F_2)^\sigma = F_1^\sigma F_2^\sigma$.

9. Sigui $E = K(S)$, i L/K una extensió. Tota K-immersió $K(S) \to L$ queda completament determinada per la imatge dels elements de S.

   Demostreu que una aplicació $\sigma : S \to L$ s'estén a una K-immersió si, i només si, per a cada polinomi $f(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$ i cada família $\alpha_1, \ldots, \alpha_r$ d'elements de S,

$$f(\alpha_1, \ldots, \alpha_r) = 0 \quad \Longleftrightarrow \quad f(\alpha_1^\sigma, \ldots, \alpha_r^\sigma) = 0.$$

10. Siguin $f(X), g(X)$ polinomis amb coeficients en K i L/K una extensió; els polinomis f i g els podem pensar també com a polinomis de $L[X]$. Demostreu que:

    (a) La divisió euclidiana de f per g dóna el mateix quan es fa a l'anell $K[X]$ que quan es fa a $L[X]$; en particular, el quocient i la resta tenen coeficients a K.

    (b) $f \mid g$ a $K[X]$ si, i només si, $f \mid g$ a $L[X]$.

    (c) El màxim comú divisor de f i g calculat a $K[X]$ és el mateix que si el calculem a $L[X]$; en particular, té coeficients a K.

    (d) f i g no són relativament primers a $K[X]$ si, i només si, existeix una extensió de K en què tinguin una arrel comuna.

    (e) Si f és irreductible a $K[X]$ i té una arrel comuna amb g a alguna extensió de K, f divideix g a $K[X]$.

11. Sigui T un element transcendent sobre $\mathbb{F}_p$. Demostreu que el cos $\mathbb{F}_q(T)$ no és perfecte.

12. Siguin E una extensió de K i α, β elements de E tals que α és transcendent sobre K i algebraic sobre $K(\beta)$. Proveu que β és algebraic sobre $K(\alpha)$.

13. Proveu que $\alpha = \sqrt{6 - i\sqrt{3}}$ i $\beta = \sqrt{\sqrt[3]{5} - 2i}$ són algebraics sobre $\mathbb{Q}$. Calculeu el grau $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ i proveu que $\mathbb{Q}(\sqrt[3]{5}, i)$ és una subextensió de $\mathbb{Q}(\beta)$ que té grau 6 sobre $\mathbb{Q}$.

14. Calculeu el polinomi irreductible de $\alpha = \sqrt{3} + \sqrt{5}$ sobre els cossos següents: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$.

15. Siguin α i β elements algebraics sobre un cos K. Comproveu que si

$$\mathrm{Irr}(\alpha, K; X) = \mathrm{Irr}(\beta, K; X),$$

    aleshores els cossos $K(\alpha)$ i $K(\beta)$ són K-isomorfs, però el recíproc no és cert.

16. Siguin L/K una extensió, E/K una extensió algebraica i $K(\alpha)/K$ una extensió simple algebraica.

    (a) Demostreu que el nombre de K-immersions $K(\alpha) \to L$ és igual al nombre d'arrels diferents del polinomi $\mathrm{Irr}(\alpha, K; X)$ al cos L.

(b) Demostreu que el nombre de K-immersions $E \to L$ és menor o igual que $[E : K]$.

17. Sigui $E = K(\alpha)$ una extensió simple algebraica. Digueu com calcular explícitament el polinomi irreductible d'un element $\beta \in E$ en termes de $\mathrm{Irr}(\alpha, K; X)$ i de l'expressió de β en la base de les potències de α.

18. Sigui $E = K(\alpha)$ una extensió simple algebraica, $\beta \in E$. L'aplicació $\lambda : E \to E$, $\lambda(x) = \beta x$ és K-lineal. Demostreu que el seu polinomi característic és una potència de $\mathrm{Irr}(\beta, K; X)$.

19. Sigui α un nombre real tal que $\alpha^4 = 5$. Estudieu la normalitat de les extensions de la torre

$$\mathbb{Q} \subset \mathbb{Q}(i\alpha^2) \subset \mathbb{Q}(\alpha + i\alpha).$$

20. Sigui α una arrel primitiva sisena de la unitat. Trobeu $\mathrm{Irr}(\alpha, \mathbb{Q}; X)$ i el seu cos de descomposició.

21. Descriviu els cossos de descomposició dels polinomis següents:

    (a) $X^5 - 7$ sobre $\mathbb{Q}$.

    (b) $X^6 + X^3 + 1$ sobre $\mathbb{Q}$ i $\mathbb{Q}(\sqrt{-3})$.

    (c) $X^p - 1$, p primer, sobre $\mathbb{Q}$.

    (d) $X^{p^6} - 1$, p primer, sobre $\mathbb{F}_p$.

22. Sigui K un cos de característica diferent de 2, E/K una extensió normal, i $\overline{K}$ una clausura algebraica de K que contingui E. Donat un $a \in E$, demostreu que l'extensió $E(\sqrt{a})/K$ és normal si, i només si, per a tota K-immersió $s : E \to \overline{K}$ existeix un element $b_s \in E$ tal que $a^s = b_s^2 a$.

23. Demostreu que tota extensió algebraica d'un cos finit és normal.

24. Demostreu que K és perfecte si, i només si, tota extensió algebraica de K és separable.

25. Demostreu que un polinomi de grau primer p, irreductible sobre $\mathbb{Q}[X]$, i que tingui exactament dues arrels no reals, té grup de Galois $\mathfrak{S}_p$. Calculeu el grup de Galois dels polinomis següents:

    (a) $X^5 - 4X + 2$.

    (b) $X^5 - 4X^2 + 2$.

(c) $X^5 - 6X^2 + 3$.

(d) $X^7 - 10X^5 + 15X + 5$.

26. Sigui K un cos de característica diferent de 2 i E/K una extensió de Galois de grau 4. Demostreu que $\mathrm{Gal}(E/K) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ si, i només si, $E = K(\alpha, \beta)$ amb $\alpha, \beta \in E \setminus K$ elements tals que $\alpha^2, \beta^2 \in K$ i $\alpha\beta \notin K$.

27. Sigui $f(X) = X^4 + aX^3 + bX^2 + cX + d \in K[X]$ un polinomi separable, i $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ les seves arrels. Diguem $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$. El polinomi $g(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3)$ s'anomena la *resolvent cúbica* del polinomi f. Comproveu que té coeficients a K i expresseu-los en termes dels coeficients de f.

28. Siguin K un cos de característica diferent de 2, $c \in K \setminus K^2$ i $F = K(\sqrt{c})$. Considerem $\alpha = a + b\sqrt{c}$, amb $a, b \in K$, tal que $\alpha \notin F^2$. Sigui $E = F(\sqrt{\alpha})$. Demostreu que són equivalents:

    (a) E/K és de Galois.

    (b) $E = F(\sqrt{\alpha'})$ amb $\alpha' = a - b\sqrt{c}$.

    (c) $\alpha\alpha' = a^2 - b^2c \in K^2$ o $c\alpha\alpha' \in K^2$.

    Proveu que, en aquest cas, el grup $\mathrm{Gal}(E/K)$ és cíclic si, i només si, $c\alpha\alpha' \in K^2$.

29. Descriviu els cossos de descomposició dels polinomis següents i trobeu el seu grup de Galois:

    (a) $X^2 - 9$ sobre $\mathbb{Q}$.

    (b) $X^2 + 2$ sobre $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{-2})$.

    (c) $X^2 + X + 1$ sobre $\mathbb{Q}$, $\mathbb{Q}(i)$ i $\mathbb{Q}(\sqrt{-3})$.

    (d) $X^3 - 5$ sobre $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ i $\mathbb{Q}(\sqrt[3]{5})$.

    (e) $(X^3 - 5)(X^2 + 2)$ sobre $\mathbb{Q}$ i $\mathbb{Q}(i)$.

    (f) $X^4 + 9$ sobre $\mathbb{Q}$.

    (g) $X^4 - 2X^2 - 2$ sobre $\mathbb{Q}$.

30. Determineu el grup de Galois dels polinomis següents:

    (a) $X^3 - 10$ sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{-3})$.

    (b) $X^3 + 3X + 1$ sobre $\mathbb{Q}$.

    (c) $X^3 - X - 1$ sobre $\mathbb{Q}$ i $\mathbb{Q}(\sqrt{-23})$.

(d) $X^4 - 2X^3 + 2X^2 + 2$ sobre $\mathbb{Q}$.

(e) $X^4 + X + 1$ sobre $\mathbb{Q}$.

(f) $X^4 - p$, p primer, sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{p})$ i $\mathbb{Q}(i)$.

(g) $(X^2 - 2)(X^2 - 3)(X^2 - 5)(X^2 - 7)$ sobre $\mathbb{Q}$.

(h) $X^4 - t$ sobre $\mathbb{R}(t)$, t transcendent sobre $\mathbb{R}$.

31. Determineu el grup de Galois sobre el cos de funcions en una variable $\mathbb{C}(t)$ dels polinomis següents:

(a) $X^3 + X + t$.

(b) $X^3 + tX + 1$.

(c) $X^3 - X - t$.

(d) $X^3 - X + t$.

(e) $X^3 - 2tX + t$.

(f) $X^3 + t^2X - t^3$.

32. Siguin K un cos de característica diferent de 2 i $f(X) \in K[X]$. Quin és el grau del polinomi

$$g(X) = \text{Resultant}(f(T), f(X - T), T)?$$

Demostreu que f i g tenen el mateix cos de descomposició. (Suposeu fixada una clausura algebraica de K).

33. Sigui $f(X) = X^4 + aX^2 + b^2$ un polinomi irreductible de $\mathbb{Q}[X]$.

(a) Calculeu el discriminant de f.

(b) Proveu que el grup de Galois de f és isomorf a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Trobeu el reticle de subcossos d'un cos de descomposició de f.

34. Sigui $f \in \mathbf{Q}[x]$ un polinomi irreductible de grau n i sigui G el seu grup de Galois sobre $\mathbf{Q}$. Proveu que si G és abelià, aleshores G té ordre n.

35. Demostreu que si p és primer, el grup de Galois del polinomi $x^p - 2 \in \mathbb{Q}[x]$ és isomorf al grup de matrius

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad | \quad a, b \in \mathbb{F}_p\,,\ a \neq 0 \right\}.$$

Considereu

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad | \quad b \in \mathbb{F}_p \right\}.$$

Descriviu l'extensió $F/\mathbb{Q}$ corresponent a aquest subgrup H. Hi ha altres subextensions del mateix grau $[F : \mathbb{Q}]$?

36. Sigui $f(x) \in \mathbb{Q}[x]$ un polinomi irreductible de grau 3 amb exactament dues arrels no reals. Siguin $\alpha_1 = a + bi$, $\alpha_2 = a - bi$ i $\alpha_3 = c$ les seves arrels, amb $a, b, c \in \mathbb{R}$.

    (a) Calculeu $\Delta(f)$ en termes de a, b, c.

    (b) Calculeu $\mathrm{Gal}_{\mathbb{Q}}(f)$.

    (c) Sigui E el cos de descomposició de f. Construïu el reticle de subextensions de E.

    (d) Calculeu els graus $[\mathbb{Q}(a) : \mathbb{Q}]$ i $[\mathbb{Q}(ib) : \mathbb{Q}]$.