Francesc Bars Cortina

Teoria de Galois explicada en 30 hores.

Apunts de classe:
Grau en Matemàtiques
UAB, 29 de març de 2011
Versió preliminar.

Contingut

Prefaci

La perfecció de les professions
depèn de la perfecció amb què
es coneixen els llurs objectes.

Jaume Balmes (*Vic* 1810 – *Barcelona* 1848)[1]

No vull subvalorar la
severitat del càstig que cau
sobre vosaltres, però confio
que els nostrees conciutadans
seran capaços de resistir
com ho va fer el
valent poble de Barcelona.
(*Daily Telegraph, 19 juny 1940)*

(*Winston Churchill*, *Blenheim Palace* 1874 – *London* 1965)

2

[1]Per a conèixer millor la vessant pedagògica de'n Jaume Balmes suggerim "Criteri i Pedagogia" editat per Univ.Ramon Llull, col.lecció Eusebi Colomer, o bé llegir directament "el Criteri" de Jaume Balmes que trobeu a la web. En l'actualitat hi ha una gran força pels pedagogs actuals d'ensenyament que defensen l'ensenyament sense continguts, actitud molt discutible i què pot afectar a la formació pels futurs científics catalans, i en Jaume Balmes defensava la tesis contrària.

[2]Sempre quan escriu unes notes i fa docència, li recau la pregunta: quin idioma escriure-ho i/o expressar-se (i més amb un món cada cop més globalitzat)? No obstant després de llegir el llibre de'n Josep Benet i Morell "L'intent franquista de genocidi cultural contra Catalunya", és clar que haig d'aportar el meu grà de sorra al lloc on estic i per tant la resposta a aquesta pregunta és evident.

Capítol 1

Nocions preliminars de cossos

1.1 Preliminars d'anells, repàs

Definició 1.1.1. *Un anell R és un conjunt amb dues operacions:*

$$+ : R \times R \to R, (a, b) \mapsto a + b$$

$$* : R \times R \to R, (a, b) \mapsto a * b$$

que satisfà les següents propietats:

1. *R amb l'operació $+$ és un grup abelià, és a dir compleix $+$ les propietats: associativa, existència d'element neutre escrit 0, existència d'invers per tot element de R, i commutativa (de esser grup abelià).*
2. *L'operació producte $*$ és associatiu: $(a * b) * c = a * (b * c)$, $\forall a, b, c \in R$.*
3. *El producte és distributiu respecte la suma:*

$$a * (b + c) = a * b + a * c, \ i \ (a + b) * c = a * c + b * c \ \forall a, b, c \in R.$$

4. *Hi ha un element que diem 1 de R que compleix $1 * r = r * 1 = r \ \forall r \in R$ amb $1 \neq 0$,*

Si tenim que el producte és commutatiu direm que R és un anell commutatiu.

ATENCIÓ: En aquest curs quan direm anell voldrem dir anell commutatiu d'ara en endavant.

Exemple 1.1.2. *Exemples d'anells (commutatius) són $\mathbb{Z}$, $\mathbb{Z}/(n)$, $R[x_1, \ldots, x_n]$ l'anell de polinomis en n variables a coeficients en un anell R.*

Definició 1.1.3. *Sigui R un anell, un subconjunt S de R és un subanell si S amb les operacions de R és un anell.*

Definició 1.1.4. *Sigui R un anell. Un subconjunt $I \neq \emptyset$ de R és un ideal de R si*

1. $\forall a, b \in I$ *tenim* $a + b \in I$,

2. $\forall a \in I$ *i* $\forall r \in R$ *tenim* $r * a \in I$.

Definició 1.1.5. *Considerem R, R' dos anells. Un morfisme d'anells $\varphi : R \to R'$ és una aplicació satisfent:*

$$\varphi(a +_R b) = \varphi(a) +_{R'} \varphi(b)$$

$$\varphi(a *_R b) = \varphi(a) *_{R'} \varphi(b)$$

$$\varphi(1_R) = 1_{R'}.$$

Recordeu que si R és un anell i I ideal de R amb $I \neq R$ llavors R/I té estructura d'anell amb $(a+I)+_{R/I}(b+I) := (a+_R b)+I$ i $(a+I)*_{R/I}(b+I) := (a *_R b) + I$, i $proj : R \to R/I$ definida per $proj(a) := a + I$ és un morfisme d'anells.
També si S subanell de R és te que la inclusió $S \hookrightarrow R$ és un morfisme d'anells.

Proposició 1.1.6 (Teorema d'isomorfisme)**.** *Sigui $f : R \to R'$ un morfisme d'anells. Llavors*

1. $Im(f) := \{f(r) | r \in R\}$ *és un subanell de* R',

2. $Ker(f) := \{r | f(r) = 0\}$ *és un ideal de* R,

3. *existeix un únic isomorfisme d'anells (=morfisme bijectiu d'anells)* $\tilde{f} : R/Ker(f) \to Im(f)$ *definit per* $\tilde{f}([\alpha]) = \tilde{f}(\alpha + Ker(f)) := f(\alpha)$ *(que està ben definit!!!) i compleix que*

$$\iota \circ \tilde{f} \circ proj = f$$

on $\iota : Im(f) \hookrightarrow R'$ la inclusió i $proj : R \to R/Ker(f)$ la projecció de R donada per l'ideal $Ker(f)$.

Observem que amb els anells R (amb unitat) definim el morfisme

$$car_R : \mathbb{Z} \to R$$

$$n \mapsto n * 1_R$$

Definició 1.1.7. *Donat un anell R s'anomena la característica de R al natural més petit m on $Ker(car_R) = (m)$. Escriurem $m = char(R)$ o $m = car(R)$.*

Exemple 1.1.8. *L'anell $\mathbb{Z}$ té $car(\mathbb{Z}) = 0$, l'anell $\mathbb{Z}/(n)$ té $car(\mathbb{Z}/(n)) = n$, l'anell $\mathbb{Q}[x]$ té $car(\mathbb{Q}[x]) = 0$.*

El curs de teoria de Galois estudia cossos i propietats d'ells. Anem-los a recordar.

Definició 1.1.9. *Un cos K és un anell commutatiu (amb unitat) on tot $\alpha \in K - \{0\}$ té invers amb l'operació $*$.*

Exemple 1.1.10. *Recordeu que coneixeu diversos cossos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (aquests tenen característica zero) també recordeu que $\mathbb{Z}/(p)$ amb p primer és un cos de característica p.*

Abans de presentar els "exemples" més importants per un cos per aquest curs anem a donar algunes propietats més de cossos.

Lema 1.1.11. *Sigui R un anell commutatiu. R és un cos si i només si R no té ideals apart de l'ideal (0) i R.*

Demostració. Suposem primer que R és un cos, i sigui $I \neq (0)$ un ideal de R diferent de l'ideal zero, per tant existeix $a \in I - \{0\}$ no zero, del fet de ser R cos tenim $1 = a * (a)^{-1} \in I$ i per tant $I = R$.
Veiem el recíproc. Sigui $b \neq 0$ element de R, volem demostrar que té invers. Considerem l'ideal no zero de R $I = (b)$ per hipòtesi és tot R on existeix $c \in R$ on $b * c = 1 \in I = R$, d'aquí obtenim que R és un cos.

□

Lema 1.1.12. *Sigui $\varphi : K \to R$ un morfisme d'anells amb K un cos. Llavors φ és sempre un morfisme injectiu, (deiem que és un monomorfisme d'anells, bé si R fos un cos parlem de monomorfisme de cossos).*

Demostració. Recordem que $ker(\varphi)$ és un ideal de K, pel lema anterior obtenim que $ker(\varphi) = (0)$ (ja que $= R$ no pot ser perquè el morfisme no és el morfisme zero $1_K \neq 0$ i $1_R = \varphi(1_K) \neq 0_R$). □

Observació 1.1.13. *Si $\varphi : K_1 \to K_2$ és un morfisme d'anells amb K_1 i K_2 cossos, parlarem de morfismes de cossos. Observeu que l'invers d'un element va a l'invers, és a dir $\varphi(a^{-1}) = \varphi(a)^{-1}$ per a $a \in K_1 - \{0\}$.*

Recordeu que un anell commutatiu R s'anomonava domini d'integritat si donat $a * b = 0$ amb $a, b \in R$ llavors a ó b són el zero de R. Teniu molts exemples de dominis: K un cos, $K[x_1, \ldots, x_n]$ anell de polinomis en n variables un un cos K ,... (un exemple típic de no és domini és $\mathbb{Z}/(n)$ amb n no primer o bé $M_2(K)$).

Lema 1.1.14. *Un cos K tan sols pot tenir $car(K) = 0$ o bé p amb p primer.*

Demostració. Sigui $(n) = ker(char_K)$, tenim pel teorema d'isomorfisme que $\mathbb{Z}/(n) \cong Im(f)$ i observeu que $Im(f)$ és un domini d'integritat ja que és un subanell d'un cos, per tant com $\mathbb{Z}/(n)$ tan sols és domini d'integritat quan $n = 0$ o $n = p$ amb p primer obtenint el resultat. □

Qüestió 1.1.15. *Ja coneixeu molts exemples de cossos de car =0, m'hen podrieu donar infinits? Igualment cossos de car p tan sols coneixeu potser $\mathbb{Z}/(p)$, m'hen podeu donar infinits? Bé a final d'aquesta secció haurieu de poder respondre.*

Anem ara a donar dos grans "exemples" per a construir cossos. El primer serà via cos de fraccions,

Fet 1.1.16. *Considerem R un domini d'integritat. Definim*

$$Q(R) := \{(r, s) | r, s \in R, s \neq 0\} / \sim$$

via la relació d'equivalència en $R \times (R - \{0\})$: $(r_1, s_1) \sim (r_2, s_2)$ si $r_1 * s_2 = r_2 * s_1$, escriurem $(r, s) \in Q(R)$ per $\frac{r}{s}$ i mitjançant les operacions:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{(r_1 * s_2 + r_2 * s_1)}{s_1 * s_2}; \ \frac{r_1}{s_1} * \frac{r_2}{s_2} := \frac{r_1 * r_2}{s_1 * s_2},$$

fan que $Q(R)$ un cos on $R \to Q(R)$ via $r \mapsto \frac{r}{1}$ és monomorfisme (per tant via aquest morfisme pensem R dins de $Q(R)$).

Per tant donat un domini d'integritat podem construir un cos on R es troba dins mitjançant el morfisme $r \mapsto \frac{r}{1}$.

Exemple 1.1.17. *1. Si K és un cos $Q(K) \cong K$ (exercici).*

2. Sigui K un cos i $K[x]$ anell de polinomis a coeficients en K. Tenim que

$$Q(K[x]) = \{\frac{p(x)}{q(x)} | p, q \in K[x], q \neq 0\}$$

és un cos que notarem en aquest curs $K(x)$.

3. Si considerem $K[x_1, \ldots, x_n]$ anell de polinomis en n-variables a coeficients en un cos K, escriurem al cos $Q(K[x_1, \ldots, x_n]) = K(x_1, \ldots, x_n)$.

4. $\mathbb{Z}$ domini tenim $Q(\mathbb{Z})$ és un cos observeu que és $\mathbb{Q}$.

5. Considerem l'anell dels enters de Gauss $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ amb $i^2 = -1$ amb l'estructura d'anell dins els complexos. Qui és el cos $Q(\mathbb{Z}[i])$?

Anem ara a repassar un altre exemple de construir cossos, usant els dominis euclidians. Recordem que $a \in R$ (R un domini d'integritat) s'anomena una unitat si a té un invers a R amb l'operació $*$, és dir existeix $h \in R$ on $a * h = h * a = 1_R$. Diem que $a \in R$ és un àtom o irreductible en R si sempre que $a = b * c$ amb $b, c \in R$ llavors b o c són una unitat a R i a no és una unitat de R.

Fet 1.1.18. *Donat K un cos, tenim $K[x]$ anell de polinomis és un domini euclidià* [1]*. En un domini euclideà tot ideal I és principal $I = (p(x))$, i per l'algoritme d'Euclides tenim que l'anell $K[x]/(p(x))$ és un cos si i només si $p(x)$ és polinomi irreductible en $K[x]$ no constant* [2]*.*

Exemple 1.1.19. *1. Observem que x^2+1 és un polinomi irreductible a $\mathbb{Q}[x]$ per tant $\mathbb{Q}[x]/(x^2+1)$ és un cos.*

2. $(\mathbb{Z}/(2))[x]/(x^2+x+1)$ és un cos ja que x^2+x+1 és un polinomi irreductible a $(\mathbb{Z}/(2))[x]$.

Fixeu-vos que $Q[x]/(x^2+1)$ és pot pensar com $\mathbb{Q}$ éspai vectorial. Quina dimensió té?
Podem pensar $\mathbb{Q}(x) = Q(\mathbb{Q}[x])$ com un $\mathbb{Q}$-espai vectorial? En cas afirmatiu, quina dimensió té?

Com observem de l'anterior exemples, per a construir exemples usant el fet 1.1.18 necessitem decidir sobre irreductibilitat de polinomis, aquest és un problema gens trivial i tan sols a $\mathbb{C}[x]$ o a $\mathbb{R}[x]$ és molt fàcil (en el supòsit que poguèssim calcular les arrels del polinomi a $\mathbb{C}$). Anem tot seguit a donar certs criteris d'irreductibilitat que ens poden ser útils en algunes situacions.

[1] Recordeu que $K[x_1, \ldots, x_n]$ amb K un cos, no és domini euclideà si $n \geq 2$ però sempre $K[x_1, \ldots, x_n]$ són dominis de factorització única.

[2] recordeu que quan $p(x)$ no és irreductible en $K[x]$ obtenim que $K[x]/(p(x))$ no és un domini i en particular mai pot ser un cos, observeu que un cos sempre és un domini!

Exemple 1.1.20. *Exemples d'irreductibilitat i factorització.*
Recordeu que $K[x]$ amb K cos és domini euclidià, en particular domini de factorització única (dfu)[3]*; per tant tot $\alpha \in K[x]$ s'escriu de forma única com a producte d'elements irreductibles de $K[x]$ llevat d'ordre i d'unitats, on recordem que les unitats de l'anell $K[x]$ amb el producte és $K - \{0\}$.*[4]

1. *Sempre $x - \alpha$ amb $\alpha \in K$ és irreductible en $K[x]$.*

2. *Si $p(x) \in K[x]$ i $\alpha \in K$ és una arrel de $p(x)$ tenim que $p(x) = (x-\alpha)q(x)$ amb grau $q(x) =$grau $p(x) - 1$, criteri de Ruffini, en particular $x - \alpha$ és un element irreductible en la descomposició en irreductibles del polinomi $p(x)$.*

3. *Si $p(x) \in K[x]$ no té cap arrel de $p(x)$ en K, és irreductible a $K[x]$? NOOOOO sempre, demostreu que la resposta és afirmativa quan $p(x)$ té grau ≤ 3 i doneu un exemple d'un polinomi de grau 4 sobre $\mathbb{Q}[x]$ sense arrels a $\mathbb{Q}$ però que no és irreductible a $\mathbb{Q}[x]$.*

4. *Factorització a $\mathbb{C}[x]$: recordeu que pel teorema fonamental de l'àlgebra tot polinomi no constant a $\mathbb{C}[x]$ té una arrel a $\mathbb{C}$, d'aquest fet conjuntament amb Ruffini s'obté que tot polinomi $p(x) = a_n x^n + \ldots + a_1 x + a_0$ de grau exactament n de $\mathbb{C}[x]$ té exactament n arrels (que podrien anomenar): $\alpha_1, \ldots, \alpha_n$ i per tant tenim la factorització en $\mathbb{C}[x]$:*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = a_n (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$

i per tant els únics polinomis irreductibles a $\mathbb{C}[x]$ són els de grau 1.

5. *Factorització a $\mathbb{R}[x]$. Sigui $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$ un polinomi, en $\mathbb{C}$ hi ha exactament n-arrels, a més observeu que si α és arrel de $p(x)$ tenim que $p(\overline{\alpha}) = 0$ (exercici) on $\overline{\alpha}$ és el conjugat de α, per tant $\overline{\alpha}$ és arrel de $p(x)$. Podem llistar les n-arrels de $p(x)$ via: $\beta_1, \ldots, \beta_s$ arrels reals i $\gamma_{s+1}, \overline{\gamma_{s+1}}, \ldots, \gamma_{s+r}, \overline{\gamma_{s+1}}$ arrels complexes i no reals on $s + 2r = n$. Llavors obtenim que la factorització de $p(x)$ en $\mathbb{R}[x]$ és:*

$$a_n (x-\beta_1) \cdot \ldots \cdot (x-\beta_s) \cdot (x^2 - 2Re(\gamma_{s+1})x + |\gamma_{s+1}|^2) \cdot \ldots \cdot (x^2 - 2Re(\gamma_{s+r})x + |\gamma_{s+r}|^2),$$

on $Re(z)$ és la part real del nombre complex z i $|z|$ denota el mòdul. Per tant els polinomis irreductibles a $\mathbb{R}[x]$ són els de grau 1 o de grau 2 sense arrels a $\mathbb{R}$.

6. *Factorització a $\mathbb{Q}[x]$.*
Ja és més complicat, realment hi ha polinomis irreductibles de qualsevol grau, tot i així tenim el criteris del Lemma de Gauss que fa que factorització a $\mathbb{Q}[x]$ no sigui tan complicat, anem a explicar el Lemma de

[3] Recordeu que un domini R s'anomena domini de factorització única (dfu) si compleix les dues condicions següents:
(i) qualsevol $r \in R - \{0\}$ que no és una unitat de R s'escriu com producte finit d'elements irreductibles o àtoms de R,
(ii) donades $r_1 \cdot \ldots \cdot r_n$ i $s_1 \cdot \ldots \cdot s_m$ dues factoritzacions per a r formada per elements irreductibles es té que $n = m$ i hi ha una permutació de $\{1, \ldots, n\}$ on r_i i $s_{\sigma(i)}$ són elements d'R associats és a dir iguals llevat de multiplicar per una unitat de R.

[4] Recordeu que si R és dfu llavors $R[x]$ és dfu, per tant també $R[x_1, \ldots, x_n]$ és dfu.

Gauss i consequències, ho escrivim en un llenguatge més general.

Sigui R un dfu, donem certs criteris útils per la factorització en $Q(R)[x]$. [5]

Definició 1.1.21. *Sigui R un dfu, i $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in R[x] - 0$. Es defineix el contingut de f (llevat d'unitats) al major factor comú que divideix tots els coeficients no zero de f, que anotem $cont(f)$, es a dir $a_i = cont(f) * b_i$ amb $b_i \in R$ per a $i = 0, \ldots, n$. Si el contingut de f és 1 (o una unitat de R) diem que és primitiu.*

Lema 1.1.22 (Gauss)**.** *Sigui R un dfu. Tenim la següent equivalència:*

$$g \in R[x] \text{ és irreductible en } R[x]$$

$$\text{si i només si}$$

$grau(g) = 0$ *i g irreductible en R ó bé g primitiu i irreductible en $Q(R)[x]$.*

Corol·lari 1.1.23 (Criteri d'Eisenstein)**.** *Considerem $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in R[x]$ amb $a_n \neq 0$ i R dfu. Sigui $\mathbf{p} \in R$ irreductible en R (no unitat) complint:*

(a) $\mathbf{p}$ *no divideix a_n,és a dir $a_n \neq \mathbf{p}r$ amb $r \in R$,*

(b) $\mathbf{p}$ *divideix $a_{n-1}, \ldots, a_1, a_0$;*

(c) $\mathbf{p}^2$ *no divideix a_0;*

llavors $f(x)$ és irreductible en $Q(R)[x]$.

Demostració. Sense pèrdua de generalitat podem suposar $n \geq 2$. Si $f(x)$ factoritza en $Q(R)[x]$ també ho fa en $R[x]$ pel Lemma de Gauss [6] i

$$f(x) = (b_r x^r + \ldots + b_0)(c_s x^s + \ldots + c_0) \tag{1.1}$$

amb $b_i, c_i \in R$, i $r, s < n$. Tenim que $a_0 = b_0 c_0$ i com $\mathbf{p}^2$ no divideix a_0 $\mathbf{p}$ no pot ser un irreductible associat a b_0 i c_0 alhora, tan sols a un d'ells, sense pèrdua de generalitat triem $\mathbf{p}$ divideix b_0. Igualant els termes de grau 1 en la igualtat (1.1) obtenim:

$$a_1 = b_0 c_1 + b_1 c_0$$

on $\mathbf{p}$ apareix en la decomposició de b_1, igualant els termes de grau 2, obtenim $\mathbf{p}$ divideix b_2, continuant iterativament aquest procés obtenim que $\mathbf{p}$ divideix b_i per $i = 0, \ldots, r$ $(r < n)$, però $a_m = b_r c_s$ i $\mathbf{p}$ no apareix per hipòtesi en la decomposició en irreductibles de a_n, en contradicció. □

Fem-ne una aplicació:

[5] Penseu $R = \mathbb{Z}$ i $Q(R)[x] = \mathbb{Q}[x]$; un altre exemple és $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ i $Q(\mathbb{Z}[i])[x]$. PERÒ no penseu que hi ha tans bon llocs a usar!! per exemple $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Q}\}$ no és dfu per tant els criteris que segueixen no ajuden per $Q(\mathbb{Z}[\sqrt{-5}])[x]$.

[6] Observeu que hem de dir més coses per escriure la següent linea, les quals es dedueixen ràpidament de l'enunciat del Lemma de Gauss, exercici

Exemple 1.1.24. *El polinomi de grau n $x^n - p \in \mathbb{Q}[x]$ on p és un primer, és irreductible en $\mathbb{Q}[x]$. En particular en $\mathbb{Q}[x]$ hi ha polinomis irreductibles de qualsevol grau.*

Exercici 1.1.25. *Considerem R un dfu. Sigui $\delta = \frac{a}{b} \in Q(R)$ amb $a, b \in R$ $b \neq 0$ una arrel d'un polinomi*

$$a_m x^m + \ldots + a_1 x + a_0$$

amb $a_i \in R$, i suposem que a, b no tenen cap factor irreductible associat en comú en la descomposició en irreductibles; llavors

$$a = a_0 \ell, \text{ i } b = a_m \kappa \text{ per certs } \ell, \kappa \in R.$$ [7]

Exercici 1.1.26. *Sigui R un domini i I un ideal no buit i diferent de R.*

1. *Comproveu que proj : $R[x] \to (R/I)[x]$ definit per $proj(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n [a_i] x^i$ és un morfisme d'anells on $a_i \in R$ i $[a_i] = a_i + R \in (R/I)$.*
2. *Demostreu que si I és un ideal maximal de R llavors $(R/I)[x]$ és un dfu.*
3. *Suposem R és dfu, suposem també que tenim un polinomi $p(x) \in R[x]$ de grau exactament n, que I és un ideal maximal de R i que $proj(p(x))$ és un polinomi irreductible en $(R/I)[x]$ de grau n, demostreu llavors que $p(x)$ és irreductible en $Q(R)[x]$.*

Comentem que Maple pot factoritzar a $\mathbb{Q}[x]$ o $(\mathbb{Z}/p)[x]$, mitjançant les instruccions:
>factor(polinomi);
>factor(polinomi) mod p; [8]

1.2 Polinomis simètrics

En aquesta secció pensem R un domini, com usual $R[T_1, \ldots, T_n]$ anell de polinomis commutatius en les variables $T_1, \ldots, T_n$ a coefiecient en R. Sigui $f \in R[T_1, \ldots, T_n]$ i $\sigma \in S_n := \{bijecció\ en\ un\ conjunt\ de\ n\ elements\}$ denotem per $f^\sigma \in R[T_1, \ldots, T_n]$ el polinomi que s'obté canviant la variable T_i per la variable $T_{\sigma(i)}$ en l'expressió.

Exemple 1.2.1. *Si $f = 3T_1T_3 + T_2T_4$ i $\sigma = (123) \in S_4$ llavors*

$$f^\sigma = 3T_{\sigma(1)}T_{\sigma(3)} + T_{\sigma(2)}T_{\sigma(4)} = 3T_2T_1 + T_3T_4.$$

Definició 1.2.2. *Donat $f \in R[T_1, \ldots, T_n]$ diem que és simètric si $f^\sigma = f$ per a tot $\sigma \in S_n$.*
Denotem per $R[T_1, \ldots, T_n]^{S_n}$:= conjunt de tots els polinomis simètrics.

Exercici 1.2.3. *$R[T_1, \ldots, T_n]^{S_n}$ és un subanell de $R[T_1, \ldots, T_n]$.*

[7] en particular en un polinomi a $R[x]$ amb R dfu, tenim els candidats a arrels en $Q(R)$ del polinomi!!!

[8] No obstant hi ha paquets més interessants per Àlgebra i qüestions de Teoria de Galois, Teoria de Nombres i Geometria Algebraica usant el programari lliure SAGE

Definició 1.2.4. *Els polinomis*

$$s_k := \sum_{1\leq i_i<\ldots<i_k\leq n} T_{i_1}\cdot\ldots\cdot T_{i_k} = \sum_{M=\{j_1,\ldots,j_k\}} T_{j_1}\cdot\ldots\cdot T_{j_k}\in R[T_1,\ldots,T_n]$$

(on M recorre els subconjunts de $\{1,\ldots,n\}$ que tenen exactament k elements); s'anomenen els polinomis simètrics elementals on k varia entre 1 i n.

Exercici 1.2.5. *Comproveu que $s_k\in R[T_1,\ldots,T_n]^{S_n}$ per $k=1,\ldots,n$.*

Exemple 1.2.6. *1. Fixeu-vos que $s_1=T_1+\ldots+T_n$, $s_n=T_1\cdot\ldots\cdot T_n$.*

2. Definim $\delta:=\prod_{i<j}(T_i-T_j)$. Observeu que $\delta^\sigma=sign(\sigma)\delta$ on $sign(\sigma)$ és la funció signe de S_n; per tant $\Delta:=\delta^2$ és un polinomi simètric.

Teorema 1.2.7. *Tot $p\in R[T_1,\ldots,T_n]^{S_n}$ es pot expressar com un polinomi en $s_1,\ldots,s_n$ a coeficients en R, és a dir:*

$$R[T_1,\ldots,T_n]^{S_n}=R[s_1,\ldots,s_n]\ \ ^{9}.$$

Demostració. És clar que $R[s_1,\ldots,s_n]\subseteq R[T_1,\ldots,T_n]^{S_n}$. Veiem l'altra inclusió (usarem l'anomenat mètode de Waring).
A un monomi: $T_1^{r_1}\cdots T_n^{r_n}$ amb $r_i\geq 0$ natural assignem $(r_1,\ldots,r_n)\in\mathbb{N}^n$ i definim un ordre en $\mathbb{N}^n$ anomenat lexicogràfic mitjançant: $(r_1,\ldots,r_n)>_{lex}(r'_1,\ldots,r'_n)$ si $\exists i$ tal que $r_1=r'_1,\ldots,r_{i-1}=r'_{i-1}$ i $r_i>r'_i$.

Donat $f\in R[T_1,\ldots,T_n]-0$ definim el grau lexicogràfic via $deg_{lex}(f):=(r_1,\ldots,r_n)\in\mathbb{N}^n$ on $(r_1,\ldots,r_n)$ és la n-tupla més gran via $>_{lex}$ dels diferents monomis no zero de f. Definim $deg_{lex}(0)=-\infty$ on definim $-\infty<_{lex}(r_1,\ldots,r_n)$ per qualsevol n-tupla en $\mathbb{N}$.

Deixe'm a l'estudiant demostrar:1) $deg_{lex}(f+g)\leq max\{deg_{lex}(f),deg_{lex}(g)\}$; 2) $deg_{lex}(fg)=deg_{lex}(f)+_{\mathbb{N}^n}deg_{lex}(g)$.

Tornem a la demostració. Observeu $deg_{lex}(s_i)=(1,...,1,0,\ldots,0)$ els primers i-coeficients són 1 i els altres tenen el valor zero. Com f és simètric aleshores

$$deg_{lex}(f)=(r_1,\ldots,r_n),\ amb\ r_1\geq r_2\geq\ldots\geq r_n;$$

sigui $\lambda\in R$ coeficient del monomi on $deg_{lex}(f)$ és màxim, llavors

$$f_1:=f-\lambda s_n^{r_n}s_{n-1}^{r_{n-1}-r_n}\cdot\ldots\cdot s_1^{r_1-r_2}$$

compleix $deg_{lex}(f_1)<_{lex}deg_{lex}(f)$ i f_1 també és simètric. Iterant el procés i com de graus menors que el de f tan sols n'hi ha un nombre finit, obtenim el resultat. □

Exemple 1.2.8. *1. Considerem el polinomi simètric*

$$3T_1^2+3T_2^2-2T_1T_2\in R[T_1,T_2]^{S_2}.$$

[9] Atenció: la notació $R[s_1,\ldots,s_n]$ denota $R[s_1,\ldots,s_n]:=\{p(s_1,\ldots,s_n)|p\in R[T_1,\ldots,T_n]\}$, i no vol dir que s_i siguin variables independents i que no pugui haver-hi alguna relació entre elles no trivial; "(bé realment no hi ha relació entre les s_i's però això és el resultat següent d'aquests apunts, corol.lari 1.2.9!)"

Anem a aplicar el mètode de Waring per escriure'l com a polinomi amb $s_1 = T_1 + T_2$ *i* $s_2 = T_1T_2$.
Observeu primer que $deg_{lex}(3T_1^2+3T_2^2-2T_1T_2) = max((2,0),(0,2),(1,1)) = (2,0)$*, per tant anem a calcular* f_1 *de la demostració anterior:*

$$3T_1^2 + 3T_2^2 - 2T_1T_2 - 3s_2^0 s_1^{2-0} = -8T_1T_2 = -8s_2$$

obtenint que no fa falta reiterar el mètode amb aquest exemple obtenint que

$$3T_1^2 + 3T_2^2 - 2T_1T_2 = 3s_1 - 8s_2.$$

2. *Considerem un polinomi de grau 2 i anomenem per* T_1 *i* T_2 *les seves arrels, és a dir escrivim una expressió*

$$x^2 + ax + b = (x - T_1)(x - T_2).$$

Conclusió els coeficients del polinomi a, b *són els polinomis simètrics elementals respecte* T_1, T_2 *llevat potser de signe. És aquest resultat similar per un polinomi de grau* n*?*

Corol·lari 1.2.9. *Sigui* $p \in R[T_1, \ldots, T_n]$ *un polinomi en* n*-varialbles i suposem que* $p(s_1, \ldots, s_n) = 0$ *amb* s_i *els polinomis simètrics elementals amb les variables* $T_1, \ldots, T_n$*. Llavors* p *és el polinomi zero de l'anell* $R[T_1, \ldots, T_n]$.

Demostració. Si p és una constant no zero no pot donar zero en substituir les variables T_i per s_i. Si p tan sols té un monomi en fer aquesta substitució tampoc pot donar el polinomi zero. Suposem doncs que p té almenys dos monomis diferents. Si $m_1(T_1, \ldots, T_n) = T_1^{a_1} \cdots T_n^{a_n}$ i $m_2(T_1, \ldots, T_n) = T_1^{b_1} \cdots T_n^{b_n}$ són dos monomis diferents de p veiem que $deg_{lex}(m_1(s_1, \ldots, s_n)) \neq deg_{lex}(m_2(s_1, \ldots, s_n))$ i d'aquesta forma si f té dos a més monomis diferents, aquests no es cancel.len ja que hi haurà un que tindrà el grau més gran que els altres obtenint el resultat. Anem doncs a comprovar que $deg_{lex}(m_1(s_1, \ldots, s_n)) \neq deg_{lex}(m_2(s_1, \ldots, s_n))$.

$$deg_{lex}(s_1^{a_1} \cdots s_n^{a_n}) = (a_1 + \ldots + a_n, a_2 + \ldots + a_n, \ldots, a_n)$$

$$deg_{lex}(s_1^{b_1} \cdots s_n^{b_n}) = (b_1 + \ldots + b_n, b_2 + \ldots + b_n, \ldots, b_n)$$

per tant si ambdos *deg* fossin iguals, obtenim (iniciant per l'últim coeficient de la tupla i anant cap a l'esquerra anant restant el coeficient a la posició i amb el de la posició $i + 1$): $a_n = b_n$, $a_{n-1} = b_{n-1}$,... $a_1 = b_1$ però en contradicció del fet que $m_1 \neq m_2$. □

1.3 Resolució d'equacions: problemàtica resolubilitat per radicals.

Heu demostrat el següent resultat:

Teorema 1.3.1 (fonamental de l'Àlgebra)**.** *Tot polinomi de grau* $n \geq 1$ *en* $\mathbb{C}[x]$*:*

$$a_n x^n + \ldots + a_1 x^1 + a_0 \in \mathbb{C}[x]$$

té una arrel en $\mathbb{C}$.

I demostràveu com a conseqüècia:

Corol·lari 1.3.2. *Tot polinomi de grau exactament n en $\mathbb{C}[x]$ té exactament n arrels a $\mathbb{C}$, on aquestes arrels poden repetir-se.*

Exercici 1.3.3. *Demostreu el corol.lari anterior a partir del teorema fonamental del àlgebra.*

Definició 1.3.4. *Un cos $\overline{K}$ s'anomena algebraicament tancat si tot polinomi $p(x) \in \overline{K}[x]$ no constant té una arrel en $\overline{K}$, (en particular $p(x)$ té tantes arrels en $\overline{K}$ com el grau del polinomi $p(x)$).*

Pensant amb polinomis en $L[x]$ on L és un subcos d'un cos algebraicament tancat $\overline{K}$ era natural plantejar-se la següent qüestió:

Qüestió 1.3.5. *Donat un polinomi en $L[x]$,*

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) \in \overline{K}[x]$$

on α_i's són les arrels de $p(x)$ en el cos algebraicament tancat $\overline{K}$ i $a_{n-i} = (-1)^i s_i(\alpha_1, \ldots, \alpha_n) \in L$ on s_i és el polinomi simètric elemental i-èssim, per tant els coeficients del polinomi són funcions de les arrels. Podem escriure les arrels del polinomi $p(x)$ com a funció dels coeficients $a_{n-1}, \ldots, a_0$?

Pensem en aquesta secció d'ara en endavant que $\overline{K} = \mathbb{C}$ per a simplificar.

Considerem un polinomi de grau 2 arbitrari en $L[x]$:

$$\ell(x) = x^2 + bx + c.$$

Busquem $\ell(x) = 0$, escrivim-ho per

$$(x^2 + bx + \frac{1}{4}b^2) - \frac{1}{4}b^2 + c = 0$$

d'aquí obtenim

$$(x + \frac{1}{2}b)^2 = \frac{1}{4}b^2 - c$$

i per tant

$$x + \frac{1}{2}b = \pm\frac{\sqrt{b^2 - 4c}}{2}$$

i obtenim que

$$x = \frac{-b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}$$

una fórmula per les arrels del polinomi de grau 2 involucrant els coeficients del polinomi:b i c amb sumes productes i arrels quadrades.

Qüestió 1.3.6. *Referent a la pregunta (1.3.5), especifiquem-la dient: és possible trobar una fórmula per les arrels d'un polinomi de grau n en funció dels coeficients del polinomi involucrant tan sols suma, productes d'aquests coeficients i números de L, arrels m-èssimes e iteracions d'aquestes operacions?*

Si l'anterior pregunta té resposta positiva per un polinomi $p(x)$ diem que $p(x)$ és resoluble per radicals sobre L. Hem demostrat que en $L[x]$ amb $L \subseteq \mathbb{C}$ tot polinomi de grau 2 és resoluble per radicals sobre L.

Anem a estudiar l'anterior pregunta respecte polinomis de grau 3, la resposta és també afirmativa.

Considerem ara un polinomi de grau 3 arbitrari en $L[x]$:

$$\ell(x) = x^3 + ax^2 + bx + c.$$

Fem el canvi en $\ell(x)$ $y = x + \frac{a}{3}$ obtenim

$$\ell(y) = y^3 + py + q$$

on $p = b - \frac{a^2}{3}$ i $q = c + \frac{2a^3}{27} - \frac{ab}{3}$. Considerem doncs el polinomi

$$g(x) = x^3 + py + q$$

Sigui $\omega = e^{2\pi i/3} \in \mathbb{C}$ arrel de $x^3 - 1$ (de $x^2 + x + 1$) en $\mathbb{C}$ i denotem per $\alpha_1, \alpha_2, \alpha_3$ les tres arrels en $\mathbb{C}$ del polinomi $g(x)$ escrivim ara:

$$\upsilon := \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3,$$
$$\epsilon := \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

Observeu que si expressem υ i ϵ en funció de p, q també ho obtenim per α_i les arrels de g (i desfen el canvi lineal les arrels de $\ell(x)$), ja que tenim les igualtats:

$$\alpha_1 = \frac{1}{3}(\upsilon + \epsilon)$$

$$\alpha_2 = \frac{1}{3}(\omega^2\upsilon + \omega\epsilon)$$

$$\alpha_3 = \frac{1}{3}(\omega\upsilon + \omega^2\epsilon).$$

Per tant per obtenir una fórmula per les arrels de grau 3 via les arrels suma i producte dels coeficients dels polinomis és suficient trobar-la per υ i ϵ.

Fixem-nos ara que:

$$\upsilon\cdot\epsilon = \alpha_1^2+\alpha_2^2+\alpha_3^2+(\omega+\omega^2)(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) = (\alpha_1+\alpha_2+\alpha_3)^2-3(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) = -3p \tag{1.2}$$

on recordeu que x^3+0x^2+px+q recordeu que 0 és el polinomi simètric elemental s_1 avaluat en les arrels del polinomi (llevat potser de signe), p és el polinomi simètric elemental s_2 avaluat en les arrels del polinomi (llevat potser de signe) i q és el polinomi simètric elemental s_3 avaluat en les arrels del polinomi $g(x)$.

Per tant observem que $\upsilon^3\epsilon^3 = -27p^3$. Igualment observem que (recordeu $\alpha_1 + \alpha_2 + \alpha_3 = 0$ ja que el coeficient de x^2 de $g(x)$ és zero):

$$\upsilon^3 + \epsilon^3 = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3 + (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)^3 + (\alpha_1 + \alpha_2 + \alpha_3)^3$$

$$= 3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3 = -27q$$

(on en l'última igualtat hem usat el mètode de Waring per escriure-ho en funció dels simètrics elementals avaluat a les arrels).

Fixem-nos que tenim

$$(x - \upsilon^3)(x - \epsilon^3) = x^2 + 27qx - 27p^3$$

per tant tenim una fórmula via arrels sumes i productes per υ^3 i ϵ^3 donat per:

$$\frac{-27}{2}q \pm \frac{3}{2}(\textit{Arrel quadrada de } -3(4p^3 - 27q^2))$$

obtenim llavors que υ és una arrel cúbica concreta de υ^3 i un cop triat υ obtenim que $\epsilon = \frac{-3}{\upsilon}$ de la igualtat (1.2).

D'aquesta forma tot polinomi de grau 3 en $L[x]$ és resoluble per radicals sobre L.

Una fórmula per radicals de les arrels de polinomis de grau 4 també és possible, amb idees similars amb la de grau 3. Per a graus més gran o igual que 5 tots els intents fracassaven, i no va ser fins Galois que va justificar que realment no era possible trobar expressions com les anteriors usant sumes productes i arrels a partir dels coeficients del polinomi.

Per un polinomi de grau ≥ 5 qualsevol veurem a final de curs que no podem expressar les arrels com expressions d'aquesta forma algebraica via radicals i per tant la qüestió 1.3.6 no té resposta afirmativa. Deixeu-me comentar no obstant que pot haver-hi polinomis concrets de grau ≥ 5 que els podrem resoldre per radicals, però no una fórmula genèrica per tots els polinomis de grau n fixat amb $n \geq 5$.

Finalment comentar que la qüestió 1.3.5 és més general ja que pot usar funcions analítiques a partir dels coeficients. Usant els Thetanullwerke és pot trobar una fórmula per les arrels d'un polinomi de grau arbitrari; per les persones interessades podeu consultar J.Thomae Beitrag zur Bestimmung von $\vartheta(0, 0, \ldots 0)$ durch die Klassenmoduln algebraischer Funktionen en J. Reine Angew. Math. 71 (1870), 201–222; o bé J.Guàrdia: Jacobian nullwerte and algebraic equations en J. Algebra 253 (2002), no. 1, 112–132.

1.4 Extensió de cossos: elements algebraics i transcendents

Definició 1.4.1. *Donats dos cossos K i F diem que F és una extensió de K si $K \subseteq F$ i s'anota F/K.*

Observació 1.4.2. *Si K i F són cossos i $\varphi : K \hookrightarrow F$ un morfisme de cossos tenim $K \cong \varphi(K)$ i l'extensió de cossos $F/\varphi(K)$ a vegades s'escriu F/K si el monomorfisme φ se sobreentén.*

Exemple 1.4.3. *1. Recordem que un cos F té o bé $car(F) = 0$ ó $car(F) = p$ amb p primer.*

(a) si $car(F) = 0$ tenim $\mathbb{Z} \subseteq F$ (via el morfisme car), d'aquí s'obté

$\mathbb{Q} = Q(\mathbb{Z}) \subseteq F$ *de la propietat universal del cos de fraccions* [10] *i* F *és una extensió de* $\mathbb{Q}$ *(via el morfisme car)*

(b) *si* $car(F) = p$ *amb* p *primer tenim via el morfisme car i el terema d'isomorfisme el morfisme bijectiu* $\mathbb{Z}/pZ \to^{\cong} Im(car) \subseteq F$*, per tant podem pensar* F *com una extensió del cos* $\mathbb{Z}/p\mathbb{Z}$ *via aquest morfisme.*

2. *Considerem el cos* $F := K[x]/p(x)$ *amb* $p(x)$ *un polinomi irreductible en* $K[x]$ *amb* K *un cos arbitrari. Observem que podem escriure els elements de* K *mitjançant:*

$$F = \{\beta_0 + \beta_1\overline{x} + \ldots + \beta_{deg(p(x))-1}\overline{x}^{deg(x)-1} | \beta_i \in K\}$$

i podem pensar que F *és una extensió de* K *escrivint* F/K *via la inclusió*

$$K \hookrightarrow F$$

donada per, $k \mapsto k + 0\overline{x} + \ldots + 0\overline{x}^{deg(p)-1}$.

3. $\mathbb{Q}[x]/x^2 - 2$ *és extensió de* $\mathbb{Q}$.

4. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$ *i* $\mathbb{C}/\mathbb{Q}$ *són extensions.*

Notació MOLT IMPORTANT: Sigui R un domini i F un cos on $Q(R) \subset F$ i $\alpha \in F$, denotem per $R[\alpha]$ el subanell de F més petit que conté R i α i és té (exercici)

$$R[\alpha] = \{a_0 + a_1\alpha + \ldots + a_r\alpha^r | \alpha_i \in R, \alpha \in F \ fix\}$$

Si $R = K$ un cos $K[\alpha]$ és el subanell de F més petit que conté K i α i denotarem per

$$K(\alpha) := Q(K[\alpha])$$

el cos de fraccions de $K[\alpha]$.

Més en general donat $\Lambda \subseteq F$ un subconjunt de F denotem per $R[\Lambda]$ el subanell més petit de F contenint R i Λ. Denotem per $K(\Lambda)$ el cos de fraccions de $K[\Lambda]$ amb K un subcos de F.

Considerem ara F/K una extensió de cossos i $\alpha \in F$, definim el morfisme (d'anells) evaluació en α via:

$$ev_\alpha : K[x] \to F$$

$$p(x) \mapsto p(\alpha)$$

Exercici: comproveu ev_α és morfisme d'anells.
És clar $im(ev_\alpha) = K[\alpha]$.

[10] Recordem ara la propietat universal del cos de fraccions, intiutivament diu que $Q(R)$ és el cos més petit on R és troba a dins, formalment és la següent propietat: sigui R un domini, i F un cos arbitrari i suposem que tenim un morfisme injectiu $\phi : R \hookrightarrow F$ d'anells, llavors existeix morfisme (injectiu) de cossos $\underline{\phi} : Q(R) \to F$ complint

$$\phi = \underline{\phi} \circ incl$$

on $incl : R \to Q(R)$ donat per $r \mapsto \frac{r}{1}$.

Lema 1.4.4. *El $ker(ev_\alpha)$ és 0 o bé $= (p(x))$ amb $p(x)$ polinomi irreductible mònic de $K[x]$.*

Demostració. És clar que $ker(ev_\alpha) = (s(x))$ amb $s(x)$ un polinomi que pot ser el polinomi zero o de grau ≥ 1: efectivament, useu el fet que $K[x]$ és d.e. i tot ideal és principal i per tant generat per un element i que $ker(ev_\alpha) \neq K[x]$ perquè $ev_\alpha(k) = k$ per $k \in K$. Suposem doncs $s(x) \neq 0$, per tant un polinomi de grau ≥ 1 veiem que és irreductible. Del teorema d'isomorfisme tenim un morfisme injectiu

$$\tilde{ev_\alpha} : K[x]/(s(x)) \hookrightarrow F$$

com F és cos en particular domini si $s(x) = s_1(x)s_2(x)$ fos reductible ($deg(s_i) \geq 1$) obtenim

$$0 = \tilde{ev_\alpha}([0]) = \tilde{ev_\alpha}([s(x)]) = \tilde{ev_\alpha}([s_1(x)])\tilde{ev_\alpha}([s_2(x)]) \in F$$

però com $[s_i] \neq 0$ obtenim $\tilde{ev_\alpha}([s_i(x)]) \neq 0$ per la injectivitat del morfisme. □

Definició 1.4.5. *Sigui F/K una extensió i $\alpha \in F$. Diem que α és algebraic sobre K si $Ker(ev_\alpha) = (p(x))$ amb $p(x)$ un polinomi mònic irreductible en $K[x]$, i denotem $p(x)$ per $Irr(\alpha, K)[x]$* [11].
Diem que α és transcendent sobre K si $Ker(ev_\alpha) = (0)$.

Exemple 1.4.6.

1. *$\sqrt{2} \in \mathbb{R}$ és algebraic sobre $\mathbb{Q}$, tenim que $Irr(\sqrt{2}, \mathbb{Q})[x] = x^2 - 2$.*
2. *$\pi \in \mathbb{R}$ és algebraic sobre $\mathbb{Q}(\pi)$, tenim que $Irr(\pi, \mathbb{Q}(\pi)) = x - \pi \in \mathbb{Q}(\pi)[x]$.*
3. *Exercici: demostreu que $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ és algebraic sobre $\mathbb{Q}$ amb $Irr(\sqrt{2} + \sqrt{3}, \mathbb{Q})[x] = x^4 - 10x^2 + 1$.*

Lema 1.4.7. *Sigui F/K una extensió.*

1. *$\alpha \in F$ és algebraic sobre K llavors $K[\alpha] = K(\alpha)$,*
2. *$\alpha \in F$ és transcendent sobre K llavors $K[\alpha] \neq K(\alpha)$.*

Demostració. Si α algebraic sobre K tenim $K[x]/(Irr(\alpha, K)[x]) \cong K[\alpha]$ un cos per tant $Q(K[\alpha]) = K[\alpha]$ i recordem que per notació $K(\alpha) := Q(K[\alpha])$.
Si α transcendent, suposem que $K[\alpha] = K(\alpha)$ tenim llavors $\frac{1}{\alpha} \in K[\alpha]$ d'on una igualtat:

$$\frac{1}{\alpha} = a_0 + a_1\alpha + \ldots + a_k\alpha^k$$

amb $a_i \in K$ $a_k \neq 0$, per tant

$$a_0 x + a_1 x^2 + \ldots + a_k x^{k+1} \in Ker(ev_\alpha) = (0)$$

contradicció. □

No és fàcil demostrar que certs nombres complexos (o reals) són transcendents sobre $\mathbb{Q}$, exemples de nombres transcendents sobre $\mathbb{Q}$ són: π, e, $sin(1)$, ... Denotem per $\overline{\mathbb{Q}}$ tots els nombres complexos que són algebraics sobre $\mathbb{Q}$. Es pot

[11] Notació MOLT IMPORTANT!!

demostrar que $\overline{\mathbb{Q}}$ és un conjunt numerable (exercici), per tant hi ha molts més nombres transcedents que algebraics sobre $\mathbb{Q}$. [12]

Per a una lectura i problemes sobre nombres transcendents mireu l'Apèndix A.

[12] Comentar que $\overline{\mathbb{Q}}$ és un cos algebraicament tancat, intenteu-ho demostrar(*)

Capítol 2

Nocions bàsiques d'extensions algebraiques

2.1 Grau d'una extensió de cossos

Si F/K és una extensió de cossos, observeu que F és en particular un K-espai vectorial.

Definició 2.1.1. *Sigui F/K extensió de cossos. Denotem per $[F : K] := dim_K(F)$ la dimensió de F com K-espai vectorial i s'anomena el grau de l'extensió. Si $[F : K]$ és finit direm que F/K és una extensió finita.*

Exemple 2.1.2.

1. *Sigui F/K una extensió amb $[F : K] = 1$ llavors $F = K$.*
2. *$\mathbb{C}/\mathbb{R}$ és una extensió finita, observeu $[\mathbb{C} : \mathbb{R}] = 2$ (una base de $\mathbb{C}$ com $\mathbb{R}$-espai vectorial és $\{1, i\}$).*
3. *Tenim $\mathbb{R}/\mathbb{Q}$ és una extensió no finita, $[\mathbb{R} : \mathbb{Q}] = \infty$ perquè si fos finita llavors $\mathbb{R}$ seria numerable ja que podríem escriure $\mathbb{R} = v_1\mathbb{Q} + \ldots + v_n\mathbb{Q}$ on v_i base de $\mathbb{R}$ com $\mathbb{Q}$-espai vectorial i el conjunt $v_1\mathbb{Q} + \ldots + v_n\mathbb{Q}$ és numerable.*
4. *Com $\sqrt{2}$ és algebraic sobre $\mathbb{Q}$ tenim $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ és una extensió a més finita de grau 2 ja que $\{1, \sqrt{2}\}$ és una $\mathbb{Q}$-base de $\mathbb{Q}[\sqrt{2}]$.*
5. *Considerem el cos $F = K[x]/(p(x))$ amb $p(x)$ irreductible en $K[x]$ de grau n, llavors l'extensió F/K és finita i de grau de l'extensió és n; efectivament una K-base de F és $\{1, [x], [x^2], \ldots, [x^{n-1}]\}$ (exercici per repassar bases d'e.v. i c.l).*
6. *Si α és algebraic sobre K tenim que $K(\alpha) = K[\alpha] \cong^{e\tilde{v}_\alpha{}^{-1}} K[x]/(Irr(\alpha, K)[x])$ on aquest isomorfisme $e\tilde{v}_\alpha$ és K-lineal, observem llavors que*

$$[K[\alpha] : K] = grau(Irr(\alpha, K)[x]$$

on una base és

$$\{1 = e\tilde{v}_\alpha(1), \alpha = e\tilde{v}_\alpha([x]), \alpha^2 = e\tilde{v}_\alpha([x^2]), \ldots, \alpha^{grau(Irr(\alpha,K)[x])-1} = e\tilde{v}_\alpha([x^{grau(Irr(\alpha,K)[x])-1}])\}.$$

7. *Si γ és transcendent sobre K tenim que $ev_\gamma : K[x] \cong K[\gamma]$ i per tant $dim_K(K[\gamma]) = \infty$ per tant com $incl : K[\gamma] \hookrightarrow K(\gamma)$ (com K-espai vectorials) obtenim $[K(\gamma) : K] \geq dim_K(K[\gamma]) = \infty$.*

Proposició 2.1.3. *Sigui $K \subseteq F \subseteq L$ tres cossos (o escrivim les extensions de cossos com $L/F/K$) llavors*

$$[L : K] = [L : F][F : K].$$

Demostració. Podem suposar que $[F : K]$ i $[L : F]$ són finits, altrament si algún d'ambdos són ∞ és clar $[L : K]$ també és infinit. Sigui doncs $[L : F] = n$ i $[F : K] = m$ i sigui [1]

$$\{e_1, \ldots, e_n\} \text{ una } F - \text{base de } L,$$

$$\{y_1, \ldots, y_m\} \text{ una } K - \text{base de } F.$$

Afirmem que $\Delta := \{e_i y_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ és una K-base de L, i per tant s'obté el resultat.
Anem doncs a demostrar que Δ és una base de L com K-espai vectorial:
Demostrem que Δ genera L com K-e.v.:
sigui $\alpha \in L$ obtenim

$$\alpha = \lambda_1 e_1 + \ldots + \lambda_n e_n = (*)$$

amb $\lambda_i \in F$ per tant

$$\lambda_i = \lambda_{i,1} y_1 + \ldots + \lambda_{i,m} y_m,$$

amb $\lambda_{i,j} \in K$, per tant

$$(*) = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{i,j} y_j e_i$$

obtenint que Δ genera L com K-e.v.
Demostrem que el conjunt Δ és K-linealment independent:
Considerem la igualtat

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{i,j} y_j e_i = \sum_{i=1}^{n} (\sum_{j=1}^{m} \alpha_{i,j} y_j) e_i$$

amb $\alpha_{i,j} \in K$; com els vectors e_i són F-l.i. obtenim que $\sum_{j=1}^{m} \alpha_{i,j} y_j = 0 \ \forall i$, ara com y_i són K-l.i. obtenim que $\alpha_{i,j} = 0 \ \forall j, i$. □

Corol·lari 2.1.4. *Suposem que tenim una cadena de cossos*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = F$$

llavors

$$[F : K] = \prod_{i=1}^{n} [K_i : K_{i-1}].$$

Demostració. Exercici al lector. □

[1] Notació K-base de E denota una base de E com a K-espai vectorial

Exemple 2.1.5. *1. Si F/K extensió i $\alpha \in F$ algebraic sobre K tenim la inclusió de cossos $K \subseteq K(\alpha) \subset F$ i com $[F:K] = [F:K(\alpha)][K(\alpha):K]$ i $[K(\alpha):K] = grau(Irr(\alpha, K)[x])$ obtenim*

$$grau(Irr(\alpha, K)[x] \text{ divideix } [F:K].$$

2. Si F/K extensió i si existeix $\alpha \in F$ transcendent sobre K de l'inclusió de cossos $K \subseteq K(\alpha) \subset F$ i com $[K(\alpha):K] = \infty$ i de la proposició anterior $[F:K] = \infty$.

3. Calculeu el grau de l'extensió $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
Fixem-nos que

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

i com $[K(\alpha):K] = grau(Irr(\alpha, K)[x])$ si α algebraic sobre K tenim:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = grau(Irr(\sqrt{2}, \mathbb{Q}(\sqrt{3}))[x])$$

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = grau(Irr(\sqrt{3}, \mathbb{Q})[x]) = grau(x^2 - 3) = 2$$

per acabar tan sols falta trobar $Irr(\sqrt{2}, \mathbb{Q}(\sqrt{3}))[x]$ (sabem que aquest polinomi divideix $Irr(\sqrt{2}, \mathbb{Q})[x] = x^2 - 2$) per tant aquest polinomi mònic és de grau 1 o 2, si fos de grau 1 caldria que $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$, veiem que això no succeeix, efectivament si $\sqrt{2} \in \mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Q}\}$ obtenim $\sqrt{2}^2 = (a + b\sqrt{3})^2$ obtenint $2 = a^2 + 3b^2 + 2ab\sqrt{3}$ com $2, a, b \in \mathbb{Q}$ obtenim $ab = 0$, si $a = 0$ obtenim $2 = 3b^2$ però no té solució amb $b \in \mathbb{Q}$, si $b = 0$ obtenim $2 = a^2$ que tambpoc té solució a $\mathbb{Q}$, per tant demostrem que $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ per tant $Irr(\sqrt{2}, \mathbb{Q}(\sqrt{3})[x] = x^2 - 2$. Per tant obtenim

$$[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Per finalitzar aquesta secció recordem que podem fer càlculs en el Maple per $\mathbb{Q}(c)$ amb c algebraic sobre $\mathbb{Q}$, per exemple
>alias(c=RootOf($X^2 + 2x + 2$));
introdueix c com una arrel d'aquest polinomi sobre $\mathbb{Q}$,
>factor($x^4 + 4$,c);
factoritza aquest polinomi en $\mathbb{Q}(c)$
També donat β algebraic sobre $\mathbb{Q}$ ens ajuda a decidir $Irr(\beta, \mathbb{Q}(\alpha))[x]$, presentem un cas simple,
>alias(d=RootOf($x^3 - x^2 + x + 8$)); d arrel d'aquest polinomi sobre $\mathbb{Q}$,
>factor($x^3 - x^2 + x + 8$,c);
$x^3 - x^2 + x + 8$
Aquest resultat ens diu que $Irr(d, \mathbb{Q}(c))(x) | Irr(d, \mathbb{Q})(x)$ en aquest cas és el mateix. Fem un altre exemple més interessant:
>factor($x^4 + 16$,c);
$(x^2 - 4 + 4c)(x^2 + 4 - 4c)$
per tant si e és una arrel de $x^4 + 16$ tenim $Irr(e, \mathbb{Q})(x) = x^4 + 16$ (exercici fàcil), però $Irr(e, \mathbb{Q}(c))(x)$ serà un dels dos polinomis de grau 2 anteriors, cal decidir quin d'ambdos és (via l'elecció que triem c dins a una immersió fixa en $\mathbb{C}$).

2.2 Extensions simples. Teorema d'Steinitz.

Sigui F/K una extensió de cossos.

Definició 2.2.1. *F/K s'anomena simple (o una extensió simple) si existeix $\delta \in F$ on $F = K(\delta)$, diem en aquest cas que δ és un element primitiu de F sobre K.*

Exemple 2.2.2.
1. *$\mathbb{C}/\mathbb{R}$ és simple ja que $\mathbb{R} \subseteq \mathbb{R}(i) \subseteq \mathbb{C}$ i tenim $[\mathbb{C} : \mathbb{R}] = 2 = [\mathbb{R}(i) : \mathbb{R}]$ i per tant $\mathbb{C} = \mathbb{R}(i)$.*
2. *$Q(K[x]) = K(x)$ és simple sobre K (cas simple i transcendent, realment és com un $\mathbb{P}^1$ sobre K, geometria algebraica!)*
3. *$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ és simple sobre $\mathbb{Q}$, ja que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$!!! (exercici: demostreu l'anterior igualtat de cossos).*

No és fàcil donada una extensió de cossos F/K si és simple o no. El següent teorema és de gran ajuda

Teorema 2.2.3 (Steinitz)**.** *Sigui F/K una extensió finita. Llavors F/K és simple si i només si hi ha un nombre finit de cossos entre K i F.*[2]

Demostració. Farem la demostració suposant que K és un cos amb infinit elements, no obstant el resultat també és correcte quan K és un cos finit tot i que no escriurem la demostració en aquests apunts. [3]
Suposem primer que F és simple sobre K,és a dir $F = K(\delta)$ amb $\delta \in F$.
Observeu primer el següent fet general, per a inclusions de cossos $K \subseteq E \subseteq F$ fixem-nos que tenim la següent divisibilitat de polinomis en $E[x]$:

$$Irr(\delta, E)[x] | Irr(\delta, K)[x].$$

Tornem ara a la prova suposant $F = K(\delta)$ i anem a demostrar que hi ha un nombre finit de cossos entre F/K. Considerem el conjunt

$$\mathcal{C} := \{E | E \text{ subcos entre } K \text{ i } F\}$$

i l'aplicació de conjunts

$$\psi : \mathcal{C} \to F[x]$$

$$E \mapsto Irr(\delta, E)[x] \in E[x] \subseteq F[x]$$

Demostrem que ψ és injectiva:
Si $Irr(\delta, E_1)[x] = Irr(\delta, E_2)[x] = c_0 + c_1 x + \ldots + x^\ell$ pertany a $E_1[x]$ i a $E_2[x]$,

[2] Fora del curs de Teoria de Galois: Si F/K no és finita i imaginem que F té un element transcendent sobre K anomenem-lo $t \in F$, llavors sempre F/K té una infinitat de cossos intermedis, i la pregunta de quan F/K és simple és més complicada i es troba la resposta dins l'estudi en geometria algebraica aritmètica, un exemple és $F = Q(\mathbb{Q}[x, y]/(y^2 - 4x^3 - 4))$ que correspon a una corba el.líptica sobre $\mathbb{Q}$ on $\mathbb{Q} \subseteq \mathbb{Q}(x) \subseteq F$ on x és una variable lliure, ser simple $F/\mathbb{Q}$ és equivalent a dir F és una recta projectiva sobre $\mathbb{Q}$ on en l'exemple $Q(\mathbb{Q}[x, y]/(y^2 - 4x^3 - 4))$ s'obté que no és simple sobre $\mathbb{Q}$, en geometria algebraica aritmètica l'estudi de la simplicitat és llegeix amb el gènere de la corba algebraica, que correspon al nombre de forats de la corba com veieu en un curs de geometria diferencial o topología, i a l'acció de grups d'extensions finites del cos $\mathbb{Q}$ dins els nombres $\mathbb{C}$

[3] Exercici, intenteu feu la demostració del teorema d'Steinitz per quan K és un cos finit.

en particular $E' := K(c_0, \ldots, c_{\ell-1})$ compleix $E' \subseteq E_i$ per $i = 1, 2$ i obtenim la divisibilitat següents:

$$Irr(\delta, E_i)[x] | Irr(\delta, E')[x] | c_0 + c_1 x + \ldots + x^\ell$$

per $i = 1, 2$ (l'ultima divisibilitat perquè $c_0 + c_1 x + \ldots + x^\ell \in E'[x]$); per tant obtenim

$$Irr(\delta, E_1)[x] = Irr(\delta, E_2)[x] = Irr(\delta, E')[x]$$

d'aquí obtenim

$$[F : E_1] = [F : E_2] = [F : E] = \left\{ \begin{array}{l} [F : E_1][E_1 : E'] \\ [F : E_2][E_2 : E'] \end{array} \right.$$

per tant $[E_1 : E'] = 1 = [E_2 : E']$ d'on $E_1 = E' = E_2$ obtenint la injectivitat.
Considerem ara la $Im(\psi)$, es troba dins els divisors mònics del polinomi $Irr(\delta, K)[x]$ en $F[x]$, de la factorització en polinomis mònics irreductibles en $F[x]$

$$Irr(\delta, K)[x] = p_1(x) \cdot \ldots \cdot p_s(x) \in F[x]$$

el nombre de divisors mònics de $Irr(\delta, K)[x]$ en $F[x]$ és

$$\sum_{i=0}^{s} \left(\begin{array}{c} s \\ i \end{array} \right) = 2^s$$

on el nombre combinatori s entre i correspon a triar exactament i dels s factors irreductibles de $Irr(\delta, K)[x]$ en $F[x]$. Per tant hi ha un nombre finit de cossos intermedis.
Anem a demostrar la implicació contrària. Suposem que solament hi ha un número finit de cossos intermedis i demostrem llavors que F/K és una extensió simple.
Siguin $\alpha, \beta \in F$ qualsevol, considerem $\gamma_a := \alpha + a\beta$ amb $a \in K$, com K és infinit i com hi ha un nombre finit de cossos intermedis entre K i F obtenim que existeixen $a_1, a_2 \in K$ amb $a_1 \neq a_2$ complint

$$K(\gamma_{a_1}) = K(\gamma_{a_2}).$$

Escrivim llavors el sistema lineal de dos equacions i dos incògnites en $K(\gamma_{a_1})$ següent:

$$\left\{ \begin{array}{l} x + ay = \gamma_{a_1} \\ x + by = \gamma_{a_2} \end{array} \right.$$

fixem-nos que és sistema compatible determinat en $K(\gamma_{a_1})$ i una solució del mateix sistema en F és (α, β) per tant resulta que $(\alpha, \beta) \in K(\gamma_{a_1})^2$ per tant $\alpha, \beta \in K(\gamma_{a_1})$ d'on

$$K(\alpha, \beta) \subseteq K(\gamma_{a_1}) \subseteq K(\alpha, \beta)$$

per tant $K(\alpha, \beta) = K(\gamma_{a_1})$. Anem finalment a demostrar l'implicació que ens interessa. Triem $\alpha \in F$ on $[K(\alpha) : K]$ maximal, si $F \neq K(\alpha)$ existeix $\beta \in F - K(\alpha)$ però tenim que existeix $\gamma_{a'}$ on $K(\alpha, \beta) = K(\gamma_{a'})$ pel que hem demostrat a sobre per tant

$$K(\alpha) \subsetneq K(\alpha, \beta) = K(\gamma_{a'}) \subseteq F$$

però en contradicció de triar α on $[K(\alpha) : K]$ maximal i $F \neq K(\alpha)$, obtenint la implicació desitjada. □

Exemple 2.2.4. *Recordeu que abans hem comentat que* $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ *per tant aquesta extensió és simple sobre* $\mathbb{Q}$ *i pel teorema anterior tenim que hi ha un nombre finit de cossos intermedis (la demo del teorema d'Steinitz també us diu una cota superior pel nombre de cossos intermedis entre* $K(\delta)/K$*, quina és per la extensió* $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$*?).*

Observació 2.2.5. *Fixeu-vos que la demostració d'Steinitz us dona un mètode de trobar elements primitius per una extensió* $K(\alpha,\beta)/K$ *en cas d'haver-hi un nombre finit de cossos intermedis, cal buscar-los de la forma* $\alpha + a\beta$ *amb* $a \in K$*.*

Exercici 2.2.6. *Demostreu que l'extensió* $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$ *és simple sobre* $\mathbb{Q}$ *i trobeu-ne un element primitiu.*

2.3 Extensions algebraiques. Extensions de morfismes.

Definició 2.3.1. *Una extensió* F/K *és algebraica si* $\forall \alpha \in F$ *és algebraic sobre* K*.*

Proposició 2.3.2. *Sigui* F/K *una extensió, són equivalents:*

1. $[F:K] < \infty$*,*
2. F/K *és algebraica i* $F = K[\alpha_1,\ldots,\alpha_n] = K(\alpha_1,\ldots,\alpha_n)$*,*
3. *existeixen* $\gamma_1,\ldots,\gamma_n \in F$ *on* $F = K(\gamma_1,\ldots,\gamma_n)$ *on* γ_i *és algebraic sobre* $K(\gamma_1,\ldots,\gamma_{i-1})$ *per* $i = 1,\ldots,n$*.*

Demostració. (i)⇒(ii) Com F/K finita, sigui $\alpha_1,\ldots,\alpha_\ell$ una K-base de F amb ℓ finit, per tant $F = K[\alpha_1,\ldots,\alpha_\ell]$ i com F és cos tenim $K[\alpha_1,\ldots,\alpha_\ell] = K(\alpha_1,\ldots,\alpha_\ell)$. Demostrem que F/K és algebraica, sigui $\beta \in F$ tenim llavors que $\{1,\beta,\beta^2,\ldots,\beta^\ell\}$ són K-linealment dependents, per tant obtenim una equació

$$\lambda_0 + \lambda_1\beta + \ldots + \lambda_\ell\beta^\ell = 0$$

amb $\lambda \in K$ per tant β és arrel del polinomi $\lambda_0 + \lambda_1 x + \ldots + \lambda_\ell x^\ell \in K[x]$ d'on β és algebraic sobre K.
(ii)⇒(iii): és clar α_i és algebraic sobre K, per tant és algebraic sobre $K(\alpha_1,\ldots,\alpha_{i-1})$, per tant triant $\gamma_i := \alpha_i$ obtenim l'enunciat.
(iii)⇒(i): Podem escriure la cadena de cossos:

$$K \subseteq K(\gamma_1) \subseteq K(\gamma_1,\gamma_2) \subseteq \ldots \subseteq K(\gamma_1,\ldots,\gamma_n) = F$$

i com $[K(\gamma_1,\ldots,\gamma_i) : K(\gamma_1,\ldots,\gamma_{i-1})] < \infty$ perquè γ_i és algebraic sobre $K(\gamma_1,\ldots,\gamma_{i-1})$, obtenim usant Corol.lari 2.1.4 que $[F:K] < \infty$. □

Corol·lari 2.3.3. *Sigui* F/K *una extensió i* $\alpha_1,\ldots,\alpha_n \in F$ *algebraics sobre* K*, llavors* $K(\alpha_1,\ldots,\alpha_n)/K$ *és algebraica, en particular si* α,β *algebraics sobre* K *tenim que* $\alpha+\beta$*,* $\alpha\beta$ *i* α^{-1} *són algebraics sobre* K*.*

La demostració és evident. Escrivim una altra conseqüència de l'anterior proposició,

Corol·lari 2.3.4. *Sigui $K \subseteq F \subseteq L$ inclusió de cossos. Tenim,*

$$L/K \text{ algebraica} \Leftrightarrow L/F \text{ i } F/K \text{ algebraiques.}$$

Demostració. $\Rightarrow$ és clar. ($\Leftarrow$): sigui $\alpha \in L$ llavors $\exists f(x) \in F[x] - 0$ on $f(\alpha) = 0$ per ser L/F algebraica. Escrivim $f(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} + x^n \in F[x]$ com F/K algebraica tenim que $c_i \in F$ són algebraics sobre K per tant per la proposició anterior obtenim $K(\alpha, c_0, \ldots, c_{n-1})$ és algebraic sobre K (ja que α és algebraic sobre $K(c_0, \ldots, c_{n-1})$) obtenint que α és algebraic sobre K. □

Primeres nocions d'extensió de morfismes

Donat $\varphi : K \to L$ un morfisme de cossos (recordeu que sempre és injectiu) i F/K una extensió, volem estudiar les maneres d'extendre φ al cos F, és a dir

Qüestió 2.3.5. *denotem $K' = \varphi(K)$, (recordem que tenim $K' \cong K$), existeix $\tilde{\varphi} : F \hookrightarrow L$ complint que $\tilde{\varphi}_{|K} = \varphi$?* [4]

Donat $\varphi : K \hookrightarrow L$ l'estenem a l'anell de polinomis via $\underline{\varphi} : K[x] \to L[x]$ un morfisme d'anells definit per $a_0 + \ldots + a_nx^n \mapsto \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$; observeu que obtenim via $\underline{\varphi}$ un isomorfisme entre $K[x]$ i $K'[x]$.
Pensem en aquesta secció la pregunta anterior quan $F = K[\alpha]$ amb α algebraics sobre K.

Proposició 2.3.6. *Sigui $\varphi : K \hookrightarrow L$ morfisme de cossos i $\alpha \in F$ algebraic sobre K on F/K una extensió. Donat $\beta \in L$, existirà una extensió del morfisme $\tilde{\varphi} : K(\alpha) \hookrightarrow L$ complint $\tilde{\varphi}(\alpha) = \beta$ si i només si β és una arrel del polinomi $\underline{\varphi}(Irr(\alpha, K)[x])$.*

Demostració. Demostrem que si existeix $\tilde{\varphi}$ amb $\tilde{\varphi}(\alpha) = \beta$ llavors β és arrel del polinomi $\underline{\varphi}(Irr(\alpha, K)[x])$. Efectivament, escrivim $Irr(\alpha, K)[x] = x^n + a_{n-1}x^{n-1}\text{‘}\ldots + a_0$ i observeu les següents igualtats

$$0 = \tilde{\varphi}(0) = \tilde{\varphi}(Irr(\alpha, K)[\alpha]) =$$

$$\tilde{\varphi}(\alpha)^n + \ldots + \tilde{\varphi}(\alpha)\tilde{\varphi}(a_1) + \tilde{\varphi}(a_0) = \beta^n + \tilde{\varphi}(a_{n-1})\beta^{n-1} + \ldots \tilde{\varphi}(a_0) = \underline{\varphi}(Irr(\alpha, K)[x])(\beta)$$

on l'ultima expressió és avaluar a β el polinomi en $L[x]$ $\underline{\varphi}(Irr(\alpha, K)[x])$.
Anem a l'altra implicació.($\Leftarrow$). Escrivim $K' := \varphi(K)$. Tenim l'isomorfisme d'anells:

$$\underline{\varphi} : K[x] \to K'[x]$$

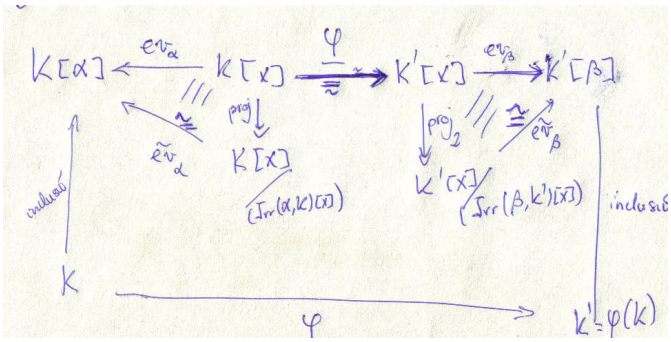
$$a_nx^n + \ldots + a_0 \mapsto \varphi(a_n)x^n + \ldots + \varphi(a_1)x + \varphi(a_0)$$

i observeu que $\underline{\varphi}$ porta polinomis irreductibles en $K[x]$ a polinomis irreductibles en $K'[x]$, per tant $\underline{\varphi}(Irr(\alpha, K)[x])$ és un polinomi irreductible en $K'[x]$ i com β és arrel d'aquest polinomi per hipòtesi, tenim

$$\underline{\varphi}(Irr(\alpha, K)[x]) = Irr(\beta, K')[x],$$

tenim el següent diagrama:

[4] La notació $\Phi_{|K} = \varphi$ per un morfisme $\Phi : F \to L$ amb F/K una extensió, vol dir que $\Phi(k) = \varphi(k)\ \forall k \in K$, és a dir que la restricció del morfisme Φ en K coincideix amb el morfisme φ.



observeu que $Ker(proj_2 \circ \underline{\varphi}) = \underline{\varphi}^{-1}((Irr(\beta, K')[x])) = (Irr(\alpha, K)[x])$ per tant pel teorema d'isomorfisme existeix un morfisme d'anells

$$\tilde{\varphi}' : K[x]/Irr(\alpha, K)[x] \to K'[x]/Irr(\beta, K')[x]$$

complint $\tilde{\varphi}' \circ proj = proj_2 \circ \underline{\varphi}$ i per tant podem definir l'extensió del morfisme via

$$\tilde{\varphi} := \tilde{ev}_\beta^{-1} \circ \tilde{\varphi}' \circ \tilde{ev}_\alpha.$$

□

Corol·lari 2.3.7. *Siguin $K(\alpha)/K$, i $K'(\alpha')/K'$ dues extensions algebraiques i simples amb $\varphi : K \to K'$ isomorfisme. Llavors: existeix $\tilde{\varphi} : K(\alpha) \to K'(\alpha')$ amb $\tilde{\varphi}_{|K} = \varphi$ i $\tilde{\varphi}(\alpha) = \alpha' \Leftrightarrow \underline{\varphi}(Irr(\alpha, K)[x]) = Irr(\alpha', K')[x]$.*

Exercici 2.3.8. *Considerem $incl : \mathbb{Q} \hookrightarrow \mathbb{R}$ i $\alpha \in \mathbb{R}$ algebraic sobre $\mathbb{Q}$. Quants morfisme podem pujar $incl$ en $\tilde{incl} : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{R}$ on $\tilde{incl}_{|\mathbb{Q}} = incl$?*

Proposició 2.3.9. *Sigui L/K una extensió algebraica i $\tau : L \to L$ morfisme de cossos on $\tau_{|K} = id$. Llavors τ és isomorfisme.*

Demostració. Sol cal demostrar que τ és epimorfisme. Sigui $\alpha \in L$ i considerem el conjunt finit

$$R := \{arrels\ en\ L\ de\ Irr(\alpha, K)[x]\}$$

Sigui $\beta \in R$ observem llavors les igualtats següents:

$$Irr(\alpha, K)[\tau(\beta)] = \tau(Irr(\alpha, K)[\beta]) = \tau(0) = 0$$

per tant τ envia en conjunt R a ell mateix, com τ és injectiva i R és finit tenim τ envia bijectivament R a R d'on existeix $\gamma \in R$ on $\tau(\gamma) = \alpha$ ja que $\alpha \in R$ per definició del conjunt R. □

Definició 2.3.10. *Donat L/K una extensió escrivim $Aut_K(L)$ al conjunt dels isomorfismes de cossos $\varphi : L \to L$ on $\varphi_{|K} = id$.*

Exercici 2.3.11. *Comproveu que $Aut_K(L)$ és un grup.*

Exercici 2.3.12. *1. Calculeu $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$.*

2. Demostreu que $Aut_{\mathbb{Q}}(\mathbb{Q}(i)) = \{id, c\}$ on c denota la conjugació complexa.

2.4 Punts construïbles amb regle i compàs.

Ens aquesta secció construïble significarà construïble amb un regle no marcat i un compàs.
Suposem que tenim:

1. un compàs, (instrument per a dibuixar circumferències)
2. un regle sense marques (instrument per a dibuixar rectes entre dos punts),
3. Dos punts que es troben a longitud 1, diem-los-hi $(0, 0)$ i $(1, 0)$, què els pensem que es troben en un plà.

Amb aquests elements permetem fer les següents operacions:

1. dibuixar una linea que uneix dos punts construïts (parlarem d'una linea construïble),
2. dibuixar una circumferència amb radi una distància entre dos punts construïbles i centre un punt construïble (parlarem de circumferència construïble).

Definició 2.4.1. *Un punt $P = (a, b) \in \mathbb{R}^2$ s'anomena construïble si hi ha una seqüència de punts finita*

$$(0, 0), (1, 0), P_1, \ldots, P_j = P$$

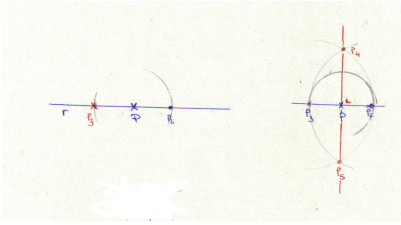
on cada P_i s'obté com:

1. *Intersecció de dos línies construïbles diferents obtingudes cadascuna d'elles d'unir dos punts dels P_ℓ amb $\ell < i$,*
2. *intersecció d'una linea construïble i una circumferència construïble construïts a partir dels P_ℓ amb $\ell < i$,*
3. *intersecció de dues circumferències construïbles usant tan sols els punts P_ℓ amb $\ell < i$.*

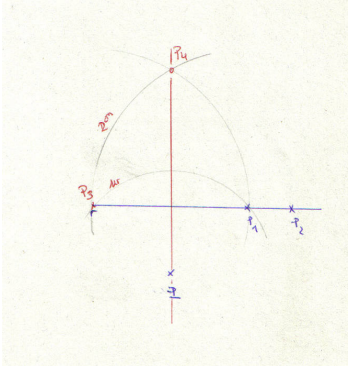
Observació 2.4.2. *Observem alguns punts construïbles:*

1. $(\mathbb{Z},0)$ *són punts construïbles, efectivament inicieu* $(0,0)$ *i (1,0), podem dibuixar l'eix OX (recta construïble) i la circumferència construïble amb radi 1 (diferencia entre (0,0) i (1,0)) i centre (1,0) per a obtenir el punt (2,0), fent aquest procés podeu obtenir* $(\mathbb{N},0)$ *i fàcilment dibuixant la circumferència de radi 1 en el punt (0,0) obteniu (-1,0) construïble i podeu obtenir* $(\mathbb{Z},0)$ *són punts construïbles.*

2. *Donat un punt* P *construïble i una recta construïble que passa pel punt* P*, la recta perpendicular a l'anterior i que passe per* P *és una recta construïble, efectivament:*



3. *Donat un punt construïble* P *i una recta construïble* r *(que passe per dos punts construïbles* α_1,α_2*), llavors la recta paral.lela a la recta* r *que pase pel punt* P *és una recta construïble, efectivament:*



i useu ara l'apartat d'abans.

4. *Donat un punt* $P=(a,b)\in\mathbb{R}^2$ *construïble llavors* $(a,0)$ *i* $(0,b)$ *són construïbles ja que* $x=0$ *e* $y=0$ *són rectes construïbles i usant l'apartat anterior obtenim fàcilment el resultat.*
Igualment donat dos punts construïbles $(a,0)$ *i* $(0,b)$ *llavors* (a,b) *és construïble, ja que es construïble la paral.lela a* $x=0$ *pel punt* $(a,0)$ *i es construïbla la paral.lela a* $y=0$ *pel punt* $(0,b)$*. Igualment si* $(a,0)$ *construïble també* $(0,a)$ *construïble (useu per exemple circumferència de radi a centrada (0,0) i la recta* $y=0$ *és construïble), per tant* $\mathbb{Z}^2$ *són punts construïbles de* $\mathbb{R}^2$*.*

Definició 2.4.3. *Un $\alpha \in \mathbb{R}$ s'anomena construïble si es possible construir un segment de longitud $|\alpha|$ el valor absolut de α (és a dir és α construïble si s'obté com la distància entre dos punts construïbles de $\mathbb{R}^2$).*

Lema 2.4.4. *$\alpha \in \mathbb{R}$ construïble $\Leftrightarrow$ $(\alpha, 0)$ és un punt construïble.*

Demostració. $\Leftarrow$ es clar, *distancia*$((0,0),(\alpha,0)) = \alpha$.
$\Rightarrow$: sigui α la distancia entre P', Q dos punts construïbles que són dos punts dins una cadena de punt construïts:

$$(0,0),(1,0),P_1,\ldots,P_\ell$$

fixem-nos que podem triar $P_{\ell+1} = (\alpha, 0)$ finalitzant la demostració. Efectivament, triem la circumferència de centre $(0,0)$ i radi $|\alpha|$ i la recta construïble $y = 0$ via (0,0) i (1,0), l'intersecció obtenim els punts construïbles $(-\alpha, 0)$ i $(\alpha, 0)$ i triem $P_{\ell+1}$ $(\alpha, 0)$. □

En temps dels grecs hi havia en particular aquests tres problemes clàssics de geometria:

1. És possible duplicar el cub? És a dir donar un cub de costat 1 i volum 1 podem construïr el cub de volum 2, és a dir podem construir la longitud real $\sqrt[3]{2}$?

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

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

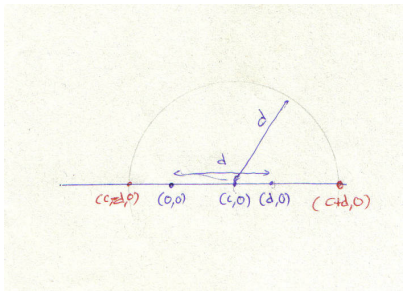
Demostrarem al final d'aquesta secció que usant teoria de galois (teoria de cossos) que les respostes anteriors totes tenen resposta negativa. Traslladem el problema de construcció a la teoria de cossos.

Lema 2.4.5. *Siguin $c, d \in F \subseteq \mathbb{R}$ amb F cos es t'e:*

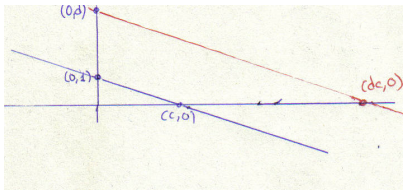
1. *si c i d construïbles llavors també ho són $c + d$, $c - d$, cd i c/d per $d \neq 0$ aquest últim,*

2. *si $c > 0$ construïble llavors $\sqrt{c}$ és construïble.*

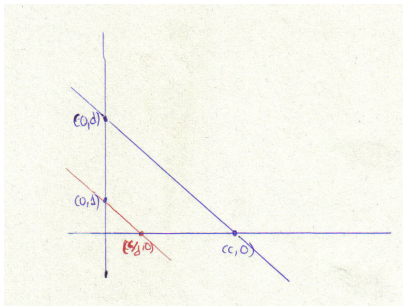
Demostració. 1. tenim que $(c,0),(d,0)$ dos punts construïbles dibuixant la circumferència construïble de radi d centrada al punt $(c,0)$ obtenim que $(c+d,0)$ i $(c-d,0)$ com els punts construïbles com mostra el dibuix següent de l'intersecció recta construïble $y = 0$ i la circumferència construïble anterior:



per construir cd construïm la paral.lela per punt construïble $(0,d)$ de la recta construïble que passe pels punts $(0,1)$ i $(c,0)$ com mostra el dibuix següent:

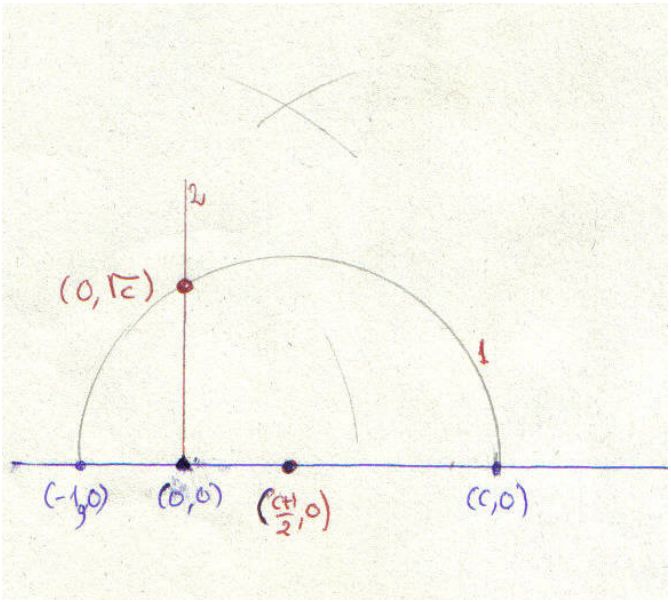


per c/d s'obté del tall de la recta construïble $y=0$ amb la recta construïble pel punt $(1,0)$ paral.lela a la recta construïble que passe pels punts construïbles $(0,d)$, $(c,0)$ com mostrem amb el dibuix següent:



2. si c construïble es suficient demostrar que el punt $(\sqrt{c},0)$ és un punt construïble, i aquest punt s'obté de la forma següent: el punt $(\frac{c-1}{2},0)$ és construïble ja que és el punt mig del segment dels punts construïbles $(-1,0)$, $(c,0)$ és un punt construïble, d'aquí podem construir la circumferència

construïble de centre $(\frac{c-1}{2}, 0)$ i radi $c - (\frac{c+1}{2})$ i la recta construïble $x = 0$ que passe pel punt $(0, 0)$, (i aplicant el teorema de Tales: sigui C un punt d'una circumferència de diàmetre AB diferent de A i B, llavors ACB és un angle recte) s'obté el punt $Q = (0, x)$ amb $x = \sqrt{c}$ com mostra el següent dibuix:



efectivament, observeu que $tg(\alpha) = \frac{x}{1} = \frac{c}{x}$ on α és angle centrat al $(-1, 0)$ del triangle rectangle $(-1, 0)\hat{Q}(0, 0)$ i també és angle centrat al punt Q del triangle rectangle $(c, 0)\hat{Q}(0, 0)$.

□

Del lema anterior obtenim els següents conseqüències,

Corol·lari 2.4.6. *Com $\mathbb{Z}$ és construïble obtenim que $\mathbb{Q}$ també és construïble. Si $\alpha_1, \ldots, \alpha_m$ són construïbles tenim llavors que tot $\beta \in \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ és construïble del apartat (i) del lema anterior.*

Anem ara a demostrar el resultat principal per punts construïbles. Anem primer a introduir certes notacions.

Sigui F un subcos de $\mathbb{R}$, el F-plà indica $F \times F \subseteq \mathbb{R} \times \mathbb{R}$, un F-punt denota $(\alpha, \beta) \in F \times F$; una F-linea en $\mathbb{R} \times \mathbb{R}$ és una recta de la forma $ax + by + c = 0$ amb $a, b, c \in F$; una F-circumferència en $\mathbb{R} \times \mathbb{R}$ és una expressió del tipus $(x - a)^2 + (y - b)^2 = c^2$ amb $a, b, c^2 \in F$.

Lema 2.4.7. *Siguin L, L' F-línies diferents i C, C' F-circumferències diferents. Llavors*

1. *$L \cap L' = \emptyset$ o bé es tallen en un F-punt.*
2. *$L \cap C = \emptyset$ o talle en 1 o 2 punts de $F[\sqrt{e}] = F(\sqrt{e})$ per algun $e \in F$ $e \geq 0$.*

3. *$C \cap C' = \emptyset$ o talle en 1 o 2 punts de $F[\sqrt{e}] = F(\sqrt{e})$ per algun $e \in F$ $e \geq 0$.*

Teorema 2.4.8. *Un nombre real c és construïble si i només si hi ha una cadena finita de cossos*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s \subset \mathbb{C}$$

amb $c \in K_s$ complint $[K_{i+1} : K_i] \leq 2$ per $i = 0, \ldots, s-1$.

Demostració. $\Rightarrow$ com c és construïble, obtenim una cadena de punts construïbles:

$$(0,0) = P_0, P_1 = (1,0), \ldots, P_s = (c,0)$$

on P_0, P_1 són $\mathbb{Q}$-punts, i cada P_i és K_{i-1}-punt ó $K_{i-1}[\sqrt{e_i}]$ per cert $e_i > 0$ on K_{i-1} és el cos més petit, extensió de $\mathbb{Q}$, on P_{i-1} és un punt definit, és a dir que les seves coordenades estan en aquest cos. Triant ambdues de les situacions anterior per K_i obtenim $P_s \in K_s$ i per construcció $[K_i : K_{i-1}] \leq 2$ amb $K_0 = \mathbb{Q}$.
$\Leftarrow$: suposem que tenim la cadena de cossos

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s$$

fem $\cap\mathbb{R}$, observem que $c \in K_s \cap \mathbb{R}$ per hipòtesi,

$$\mathbb{Q} = K_0 \cap \mathbb{R} \subseteq K_1 \cap \mathbb{R} \subseteq \ldots \subseteq K_s \cap \mathbb{R}$$

i escrivim $K_i' := K_i \cap \mathbb{R}$. És clar que $[K_r' : \mathbb{Q}] = 2^n$ anem a demostrar per inducció en n que tot $c \in K_r'$ és construïble si té la cadena de subcossos en grau 2. Quan $n = 0$ és clar, cert per $n = k-1$ veiem-ho cas $n = k$, sigui $c \in K_s'$ i tenim $[K_s' : K_{s-\ell}'] = 2$ (per cert $\ell \geq 1$) on existeix $\alpha \in K_s'$ on $Irr(\alpha, K_{s-\ell}')[x] = x^2 + bx + d$ i $K_s' = K_{s-\ell}'(\sqrt{b^2 - 4d})$ on una $K_{s-\ell}'$-base de K_s' és $\{1, \sqrt{b^2-4d}\}$ per tant $c = \beta_1 1 + \beta_2\sqrt{b^2-4d}$ amb $\beta_i \in K_{s-\ell}'$ i com $[K_{s-\ell}' : \mathbb{Q}] = 2^{k-1}$ per hipòtesi d'inducció β_i són construïbles i $b^2 - 4d$ construïbles, per un lema anterior obtenim que $\sqrt{b^2-4d}$ construïble i també $c = \beta_1 1 + \beta_2\sqrt{b^2-4d}$ és construïble obtenim per inducció el resultat. □

Corol·lari 2.4.9. *Si $c \in \mathbb{R}$ és construïble llavors $[\mathbb{Q}(c) : \mathbb{Q}]$ és una potència de 2.*

Demostració. Si c és construïble tenim una cadena

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s$$

amb $c \in K_s$ on $[K_s : \mathbb{Q}] = \prod [K_i : K_{i-1}] = 2^k$ per cert enter k i com $\mathbb{Q}(c) \subseteq K_s$ obtenim $[\mathbb{Q}(c) : \mathbb{Q}]$ divideix 2^k obtenint el resultat. □

Com a conseqüència podem resoldre els tres famosos problemes grecs

Corol·lari 2.4.10. *No és possible construïr amb regle i compàs els següents problemes:*

1. *la duplicació del cub,*
2. *la quadratura del cercle*
3. *la trisecció de l'angle.*

Demostració. 1. per la duplicació del cub cal construir l'element $\sqrt[3]{2}$ però fixem-nos $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = grau(Irr(\sqrt[3]{2}, \mathbb{Q})[x]) = 3$ i per tant no pot ser construïble pel corol.lari anterior.

2. per la quadratura del cercle cal construir el nombre $\sqrt{\pi}$ però com π és transcendent sobre $\mathbb{Q}$ també ho és $\sqrt{\pi}$ sobre $\mathbb{Q}$ i $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ no és una potència finita de 2.

3. per la trisecció de l'angle cal trobar un angle que no pugui triseccionar-se, veieu appendix B per fer-ho explícit. Exercici al lector.

□

Per més informació sobre construcció en regle i compàs i altres construccions consulteu i llegiu l'apèndix B d'aquests apunts.

Capítol 3

Engrandint el grup $Aut_K(L)$

El grup $Aut_K(L)$ serà de gran importància en l'estudi de l'extensió L/K, cal tenir pressent resultats coneguts de teoria de grups. Escrivim una llista dels resultats necessaris en l'appendix C d'aquests apunts els quals els treballeu a la classe de seminaris o pràctiques.

3.1 Algunes consideracions del grup $Aut_K(L)$

Donat L/K una extensió, tenim el grup (amb la composició) $Aut_K(L) = \{\varphi : L \to L \; isomorfisme \; de \; cossos \; amb \; \varphi_{|K} = id\}$ on els elements d'aquest grup també anomenarem K-automorfisme de L.

Recordem els següents resultats de §2.3:

1. Si F/K és una extensió algebraica i $\varphi : F \hookrightarrow F$ amb $\varphi_{|K} = id$ llavors φ és un isomorfisme.

2. Si tenim $\psi : K \to K'$ un isomorfisme i $K' \subseteq L$, $K \subseteq M$ i $\alpha \in M$ algebraic sobre K, llavors:
   existeix $\tilde{\varphi} : K(\alpha) \hookrightarrow L$ amb $\tilde{\varphi}_{|K} = \psi$ si i només si $\tilde{\varphi}(\alpha) = \beta$ on β és arrel en L de $\underline{\psi}(Irr(\alpha, K)[x]) \in K'[x]$ (fixem-nos que en aquesta situació $Im(\tilde{\varphi}(K(\alpha))) = K(\beta)$), a més $\tilde{\varphi}$ és únic amb $\tilde{\varphi}(\alpha) = \beta$ i $\tilde{\varphi}_{|K} = \psi$.

Corol·lari 3.1.1. *Sigui $K(\alpha)/K$ una extensió algebraica i $g(x) := Irr(\alpha, K)[x]$. Llavors*

$$|Aut_K(K(\alpha))| = \ell$$

on ℓ és el nombre d'arrels d'$Irr(\alpha, K)[x]$ en el cos $K(\alpha)$.

Demostració. És clar dels dos fets recordats just abans d'aquest corol.lari, un K-automorfisme de $K(\alpha)$ ve determinat per $\varphi(\alpha)$ ja que $\varphi_{|K} = id$ i $\varphi(\alpha)$ ha d'esser arrel del polinomi $\underline{id}(Irr(\alpha, K)[x])$ en $K(\alpha)$ i un cop triada aquesta arrel el K-automorfisme de $K(\alpha)$ és únic. □

Corol·lari 3.1.2. *Si L/K finita llavors $|Aut_K(L)| \leq [L : K]$.*

Abans de iniciar la demostració anem a fer alguna reflexió sobre $\varphi \in Aut_K(L)$ amb L/K finita. Del fet L/K finita $L = K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n)$ amb

$\alpha_i \in L$ algebraics sobre K. Escrivint $K_0 = K$ i $K_i = K_{i-1}(\alpha_i)$ per $i = 1, \ldots, n$ tenim una cadena de cossos:

$$K = K_0 \subset K_1 \subset \ldots \subset K_{n-1} \subset K_n = L$$

on denotem $\varphi_i := \varphi_{|_{K_i}} : K_i \to L$ i per construcció $\varphi_i|_{K_{i-1}} = \varphi_{i-1}$ per $i = 1, \ldots, n$ on $\varphi_n = \varphi$ i $\varphi_0 = id$. Com K_i/K_{i-1} és extensió simple donada per l'element α_i tenim que $\varphi_i(\alpha_i)$ ha d'anar a una arrel de l'irreductible α_i (sobre K_{i-1} portat pel morfisme $\underline{\varphi_{i-1}}$ el polinomi[1]) en L caracteritzant de forma única el morfisme (pensant que la restricció de φ en K_{i-1} és φ_{i-1}), i sabem que existeix i únivocament determinada la elecció de $\varphi_i(\alpha_i)$ per què prové del morfisme $\varphi \in Aut_K(L)$, per tant tenim una injecció:

$$\varphi \mapsto (\varphi_0, \varphi_1, \ldots, \varphi_n).$$

Anem ara a fer la demostració del corol.lari. Anem a explicitar que tuples de morfismes $(\psi_0, \psi_1, \ldots, \psi_n)$ amb $\psi_i : K_i \hookrightarrow L$ amb $\psi_{i|_{K_{i-1}}} = \psi_{i-1}$ per $i \geq 1$ i $\psi_0 = id$ i demostrarem que n'hi ha com a molt $[L : K]$ demostrant el corol.lari.

Demostració. Efectivament anem a demostrar que donat ψ_i tan sols hi ha com a molt $[K_{i+1} : K_i]$ maneres de definir ψ_{i+1} complint que la restricció a K_i és ψ_i i llavors de la regla multiplicativa de combinatòria i la fórmula de graus obtenim que el nombre de posibles tuples són:

$$[K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdot \ldots \cdot [K_1 : K_0] = [K_n : K_0] = [L : K]$$

provant el corol.lari.

Per tant ens falta demostrar que les possibles extensions de ψ_i a un morfisme $\psi_{i+1} : K_{i+1} \hookrightarrow L$ tan sols n'hi ha com a molt $[K_{i+1} : K_i]$ per $i = 0, \ldots, n-1$. Això ja ho hem demostrat, efectivament, recordem-ho: per fer aquesta extensió d'aquest morfisme tan sols hem de dir a on α_{i+1} de ser K_{i+1}/K_i extensió simple ($K_{i+1} = K_i(\alpha_{i+1})$) amb la restricció que $\psi_{i+1|_{K_i}} = \psi_i$. Hem vist que per poder extendre el morfisme ψ_i i definir ψ_{i+1} tan sols cal imposar $\psi_{i+1}(\alpha_{i+1})$ sigui una arrel en L del $\underline{\psi_i}(Irr(\alpha_{i+1}, K_i)[x])$ (i això determina únivocament ψ_{i+1}), en particular si en L no té arrels no podem pujar-ho!!! Per tant, com a molt en L hi ha

$$[K_{i+1} : K_i] = grau(Irr(\alpha_{i+1}, K_i)[x] = grau(\underline{\psi_i}(Irr(\alpha_{i+1}, K_i)[x]))$$

arrels (n'hi pot haver-hi menys, per exemple quan L no té totes les arrels d'aquest polinomi, o bé aquests polinomis tenen arrels repetides, ...), provant finalment el resultat. □

Observació 3.1.3. *Fixeu-vos per tal que $Aut_K(L)$ sigui exactament $[L : K]$ cal succeir dues coses, la primera es que el nombre d'arrels per $\underline{\psi_i}(Irr(\alpha_{i+1}, K_i)[x])$ en L sigui el grau d'aquest polinomi, i també que aquests polinomis irreductibles no tinguin arrels repetides, i en particular les arrels en L d'aquest polinomi són totes diferents.*

[1] Recordeu que donat $\psi : K \hookrightarrow K'$ morfisme de cossos definim $\underline{\psi} : K[x] \hookrightarrow K'[x]$ definit per $a_n x^n + \ldots + a_1 x + a_0 \mapsto \psi(a_n)x^n + \ldots + \psi(a_1)x + \psi(a_0)$, recordeu que $\underline{\psi}$ és morfisme d'anells.

Observació 3.1.4. *Fixeu-vos per donar un automorfisme de $K(\alpha_1,\ldots,\alpha_n)$ fixant K, es suficient saber les imatges per l'automorfisme d'α_1,...,α_n, però aquestes imatges no poden anar a qualsevol lloc!!!.*

Exemple 3.1.5. *Uns exemples càlcul automorfismes de cossos.*

1. *Calculem $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3+\sqrt{11}}))$.*
   Una forma: Com $\mathbb{Q}(\sqrt{3+\sqrt{11}})$ és extensió simple, tot automorfisme ha de portar aquest element a una arrel del $Irr(\sqrt{3+\sqrt{11}},\mathbb{Q})[x]$, calculem-hi l'irreductible, és fàcil veure

   $$Irr(\sqrt{3+\sqrt{11}},\mathbb{Q})[x]|x^4-6x^2-2$$

   però esclar que ambdos són el mateix ja que per Eisenstein x^4-6x^2-2 és irreductible (per tant $|Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3+\sqrt{11}}))| \leq [\mathbb{Q}(\sqrt{3+\sqrt{11}}):\mathbb{Q}]=4$. Hem de buscar les arrels del polinomi x^4-6x^2-2 en $\mathbb{Q}(\sqrt{3+\sqrt{11}})$ (pensant totes les arrels dins $\mathbb{C}$ podeu trobar que $\{\pm\sqrt{3+\sqrt{11}},\pm\sqrt{3-\sqrt{11}}\}$ són les arrels en $\mathbb{C}$). Per tant com $\mathbb{Q}(\sqrt{3+\sqrt{11}})\subset\mathbb{R}$ tenim que $\pm\sqrt{3-\sqrt{11}}\notin \mathbb{Q}(\sqrt{3+\sqrt{11}})$ per tant tenim tan sols dos automorfismes, la identitat i l'altre definit via:

   $$\varphi_2(\sqrt{3+\sqrt{11}}) = -\sqrt{3+\sqrt{11}}$$

   on $\varphi_2\circ\varphi_2 = id$, (aquí $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3+\sqrt{11}}))\cong\mathbb{Z}/(2)$ ja que és l'únic grup de dos elements).

2. *Calculem $Aut_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2},w])$ on $w^3=1$ on $w=e^{2\pi i/3}=i\frac{\sqrt{3}}{2}+\frac{1}{2}$.*
   Veureu en l'exemple 3.2.7, que $Irr(w,\mathbb{Q}(\sqrt[3]{2})[x] = x^2+x+1$, i que $[\mathbb{Q}[\sqrt[3]{2},w]:\mathbb{Q}]=6$, escrivim $L=\mathbb{Q}(\sqrt[3]{2},w)$.
   Anem ara a calcular-hi el grup d'automorfismes.
   Calculem primer $\varphi_1:\mathbb{Q}(\sqrt[3]{2})\to L$, és únivocament determinat i existeixen si $\varphi_1(\sqrt[3]{2})$ ha d'anar a una arrel de $\underline{\varphi_0}(Irr(\sqrt[3]{2},\mathbb{Q})[x]) = \underline{id}(Irr(\sqrt[3]{2},\mathbb{Q})[x]) = x^3-2$ (podeu pensar també que en el cas simple els automorfismes venen de permutacions en les arrels i cal saber quines es donen i quines no) les tres arrels d'aquest polinomi són $\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}$ i com són de L podem definir exactament tres monomorfismes $\mathbb{Q}(\sqrt[3]{2})\hookrightarrow L$ mitjançant:

   $$\psi_1(\sqrt[3]{2}) = \sqrt[3]{2}, \psi_1 = (inclusio)$$

   $$\psi_2(\sqrt[3]{2}) = w\sqrt[3]{2}$$

   $$\psi_3(\sqrt[3]{2}) = w^2\sqrt[3]{2}.$$

   Anem a veure si podem pujar cadascún aquests monomorfismes a $\varphi_2: L\to L$ on la restricció a $M:=\mathbb{Q}(\sqrt[3]{2})$ és un dels anteriors, per a definir-ho:
   cas $\psi_1 = inclusio$, hem de definir quina imatge ha de tenir w, ha d'anar a una arrel de $\underline{\varphi_1}(Irr(w,M)[x]) = x^2+x+1$, per tant tenim dos aixecaments (ja que les dos arrels són a L que corresponen a: w, w^2), tenim doncs que de ψ_1 tenim dos automorfismes:

   $$\phi_1 = id, \phi_1(w) = w, \phi_1(\sqrt[3]{2}) = \sqrt[3]{2},$$

$$\phi_2, donat\ per\ \phi_2(w) = w^2,\ \phi_2(\sqrt[3]{2}) = \sqrt[3]{2}.$$

cas ψ_2, hem de definir quina imatge ha de tenir w, ha d'anar a una arrel de $\underline{\psi_2}(Irr(w,M)[x]) = x^2+x+1$ (fixeu-vos que en aquest exemple el polinomi x^2+x+1 va al mateix polinomi ja que els coeficients es troben a $\mathbb{Q}$ i no en M, però usualment els coeficients seran a M i via el morfisme donarà un altre polinomi d'aplicar-hi aquest morfisme als coeficients), per tant tenim dos aixecaments (ja que les dos arrels d'aquest polinomi x^2+x+1 són a L que són:w, w^2), tenim doncs que de ψ_2 ens puja a dos automorfismes:

$$\phi_3, \phi_3(w) = w, \phi_3(\sqrt[3]{2}) = w\sqrt[3]{2},$$

$$\phi_4, donat\ per\ \phi_4(w) = w^2,\ \phi_4(\sqrt[3]{2}) = w\sqrt[3]{2}.$$

cas ψ_3, hem de definir quina imatge ha de tenir w, ha d'anar a una arrel de $\underline{\psi_3}(Irr(w,M)[x]) = x^2+x+1$ (fixeu-vos que en aquest exemple el polinomi x^2+x+1 va al mateix polinomi ja que els coeficients es troben a $\mathbb{Q}$ i no en M, però usualment els coeficients seran a M i via el morfisme donarà un altre polinomi d'aplicar-hi aquest morfisme als coeficients), per tant tenim dos aixecaments (ja que les dos arrels d'aquest polinomi x^2+x+1 són a L que són les arrels:w, w^2), tenim doncs que de ψ_3 ens puja a dos automorfismes:

$$\phi_5, \phi_5(w) = w, \phi_5(\sqrt[3]{2}) = w^2\sqrt[3]{2},$$

$$\phi_6, donat\ per\ \phi_6(w) = w^2,\ \phi_6(\sqrt[3]{2}) = w^2\sqrt[3]{2}.$$

Per tant $|Aut_{\mathbb{Q}}(L)| = [L:\mathbb{Q}] = 6$ en aquest cas. Quin grup és? Grups de 6 elements hi ha (llevat iso) $\mathbb{Z}/(6)$ i S_3, en el nostre cas és fàcil veure que no és commutatiu (Exercici) per tant és isomorf a S_3.

3. *Les biquadràtiques. Considerem l'element $\sqrt{a}+\sqrt{b} \in \mathbb{C}$ amb a, b racionals no quadrats (és a dir cap d'ells és un quadrat a $\mathbb{Q}$) i que a/b no és un quadrat. Considerem el cos $L = \mathbb{Q}(\sqrt{a}+\sqrt{b})$. Calculem aquí el grup $Aut_{\mathbb{Q}}(L)$.*
És un càlcul semblant al del primer parcial que

$$Irr(\sqrt{a}+\sqrt{b}, \mathbb{Q})[x] | x^4 - 2(a+b)x^2 + (a+b)^2 - 4ab.$$

És un exercici per a vosaltres demostrar ara que aquest polinomi de grau 4 és irreductible sota les condicions aritmètiques que hem imposat a a i $a\,b$. Un cop comprovat s'obté doncs que $[L:\mathbb{Q}] = 4$, i fixeu-vos que les arrels del polinomi són $\pm\sqrt{a}\pm\sqrt{b}$ (també es poden escriure per: $\pm\sqrt{(a+b)\pm 2\sqrt{ab}}$, on observeu que l'expressió en forma radical de les arrels no és única). Quines de les arrels es troben en L i quines no? Anem-ho a raonar de la forma següent, veiem que $L = \mathbb{Q}(\sqrt{a},\sqrt{b})$ i un cop vist això és clar que totes les arrels són a L.
Evidentment $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\sqrt{a},\sqrt{b})$, i fixeu-vos

$$[\mathbb{Q}(\sqrt{a},\sqrt{b}):\mathbb{Q}] = grau(Irr(\sqrt{a}, \mathbb{Q}(\sqrt{b})[x]) grau(Irr(\sqrt{b},\mathbb{Q})[x])$$

com $Irr(\sqrt{b},\mathbb{Q})[x] = x^2 - b$ i $Irr(\sqrt{a},\mathbb{Q}(\sqrt{b})[x] | x^2 - a$ l'extensió $\mathbb{Q}(\sqrt{a}+\sqrt{b})/\mathbb{Q}$ té grau 2 o 4, però com L es troba a dins i té grau 4 vol dir que

aquesta extensió és de grau 4 i $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

Anem ara finalment a calcular $Aut_{\mathbb{Q}}(L)$*, tenim que com hi ha exactament 4 arrels* $\pm\sqrt{a} \pm \sqrt{b}$ *en* L *obtenim exactament 4 automorfismes:*

$$\varphi_1 = id$$
$$\varphi_2(\sqrt{a} + \sqrt{b}) = \sqrt{a} - \sqrt{b}$$
$$\varphi_3(\sqrt{a} + \sqrt{b}) = -\sqrt{a} - \sqrt{b}$$
$$\varphi_4(\sqrt{a} + \sqrt{b}) = -\sqrt{a} + \sqrt{b}.$$

És una comprovació (exercici per a vosaltres, feu-ho!!) que $\varphi_i \circ \varphi_i = id$ *per tant tot element té ordre 2, com un grup isomorf a 4 elements sempre és commutatiu i tot element no trivial tingui ordre dos és el grup* $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$*. Doneu tots els subgrups de* $Aut_{\mathbb{Q}}(L)$*[Exercici].*

3.2 Cos de descomposició d'un polinomi

Sigui $f(x) \in K[x]$ polinomi i L/K una extensió de cossos, diem que f descompon sobre L (o $L[x]$) si $f(x) = \lambda(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) \in L[x]$ (és a dir $\alpha_i \in L$, $\lambda \in K$ ja que $f \in K[x]$).
Diem que L/K és un cos de descomposició de f sobre L si compleix les dues condicions següents:

1. f descompon sobre $L[x]$,
2. no hi ha un subcos L' complint $K \subset L' \subset L$ amb $L' \neq L$ on f descompon sobre L'.

Proposició 3.2.1. *Sigui* M/K *una extensió on* $f(x) \in K[x]$ *descompon en* M *com* $f(x) = \lambda(x - \alpha_1) \ldots (x - \alpha_n) \in M[x]$*, llavors* $K(\alpha_1, \ldots, \alpha_n)$ *és un cos de descomposició de* f *sobre* K*.*

Demostració. és clar que f descompon en $K(\alpha_1, \ldots, \alpha_n)$. Si $L' \subset K(\alpha_1, \ldots, \alpha_n)$ contenint K i f descompon en L' via $f(x) = \lambda(x - \alpha_1) \ldots (x - \alpha_n) \in L'[x]$ per la unicitat de la descomposició, obtenint que $\alpha_i \in L'$ per $i = 1, \ldots, n$, i per tant $K(\alpha_1, \ldots, \alpha_n) \subset L'$. □

Observació 3.2.2 (sobre Automorfismes!)**.** *Sigui* $L = K(\alpha_1, \ldots, \alpha_n)$ *cos de descomposició sobre* K *d'un polinomi* $f(x)$ *de grau* n *on* $\alpha_1, \ldots, \alpha_n$ *les arrels de* $f(x)$ *en* L*, i considerem* $\varphi \in Aut_K(L)$*. Ja hem dit en l'observació 3.1.4 que* φ *queda determinat si sabem quan val* φ *pels* α_i*'s. Fixeu-vos que* $\underline{\varphi}(f(x)) = \underline{id}(f(x)) = f(x)$ *demostrant-nos que en fer* $x = \alpha_i$ *el morfisme* φ *porta una arrel de* $f(x)$ *a una arrel de* $f(x)$*. Per tant si ordenem les arrels diferents de* f *via* $\alpha_1, \ldots, \alpha_m$ $(m \leq n)$*, i escrivim*

$$\Sigma = \{arrels\ de\ f(x)\ en\ L\}$$

i considerem les permutacions en el conjunt Σ *amb* $|\Sigma| = m$*, obtenim un morfisme de grups injectiu (exercici):*

$$Rep : Aut_K(L) \hookrightarrow S_m$$

definit via $Rep(\varphi)(i) = j$ *on* $\varphi(\alpha_i) = \alpha_j$ *amb* $\varphi \in Aut_K(L)$.
Aquest morfisme és molt útil per a saber quin grup correspon $Aut_K(L)$ *i sempre pensar* $Aut_K(L)$ *com a un subgrup del permutacions d'arrels d'un polinomi* f *si* L *és cos de descomposició de* f *sobre* K. *("Ahhh!! no sempre totes les permutacions es donen!!!! es a dir Rep no ha de ser epi necessàremant ").*

Una aplicació: Considerem $L = \mathbb{Q}(2^{1/3}, w) = \mathbb{Q}(2^{1/3}, w2^{1/3}, w^2 2^{1/3})$ *el cos de descomposició de* x^3-2 *dins* $\mathbb{C}$, *on té arrels aquest polinomi* $2^{1/3}, w2^{1/3}, 2^{1/3}w^2$, *en l'exemple 3.1.5.2 hem vist que és un grup de 6 elements, però ara sabem que*

$$Rep : Aut_{\mathbb{Q}}(L) \hookrightarrow S_3$$

i com S_3 *té 6 elements segur que tenim que aquest grup és isomorf a* S_3.
Escrivim els 6 elements de $Aut_{\mathbb{Q}}(L)$ *de l'exemple 3.1.5.2 via el morfisme de grups Rep; tenim* $\Sigma = \{2^{1/3}, w2^{1/3}, w^2 2^{1/3}\}$, *i considerem* $\alpha_1 = 2^{1/3}, \alpha_2 = w2^{1/3}$ *i* $\alpha_3 = w^2 2^{1/3}$. *Tenim*

$$Res : Aut_{\mathbb{Q}}(L) \hookrightarrow S_3$$

$$\phi_1 \mapsto id$$

$$\phi_2 \mapsto (2,3)$$

$$\phi_3 \mapsto (1,2,3)$$

$$\phi_4 \mapsto (1,2)$$

$$\phi_5 \mapsto (1,3,2)$$

$$\phi_6 \mapsto (1,3)$$

Anem a explicat un d'aquests i els altres feu-ho vosaltres, fem-ho per ϕ_5 *definit per* $\phi_5(2^{1/3}) = w^2 2^{1/3}$ *i* $\phi_5(w) = w$, *hem de calcular* ϕ_5 *a les tres arrels de* $x^3 - 2$ *ja que* L *és cos de descomposició de* $x^3 - 2$ *sobre* $\mathbb{Q}$: $\phi_5(2^{1/3}) = w^2 2^{1/3}$, $\phi_5(w2^{1/3}) = \phi_5(w)\phi_5(2^{1/3}) = w \cdot w^2 2^{1/3} = 2^{1/3}$, *i* $\phi_5(w^2 2^{1/3}) = \phi_5(w)^2\phi_5(2^{1/3}) = w^2 \cdot w^2 2^{1/3} = w2^{1/3}$ *per tant la permutació que surt és amb l'ordre triat dels* α_i*'s és* $(1,3,2)$.

Observació 3.2.3. *Fixeu-vos que donat* $f \in K[x]$ *si podem pensar un cos* M *que conté* K *de forma que* $f(x)$ *factoritzi en* $M[x]$ *en factors de grau 1, la proposició anterior ens dona una manera senzilla de pensar el cos de descomposició, això sempre ho podrem pensar per* $K = \mathbb{Q}$ *amb* $M = \mathbb{C}$. *El que segueix es construir un cos de descomposció encara que no hi tinguem aquest* M, *veieu no obstant observació 3.2.9.*

Recordem el teorema de Kronecker, ja repassat en el curs:
si $g(x)$ és un polinomi irreductible en $K[x]$ tenim que $M := K[x]/(g(x))$ (pensem $M = \{k_0 + k_1\overline{x} + \ldots + k_{grau(g)-1}\overline{x}^{g-1} | k_i \in K\}$ és un cos i $\overline{x} \in M$ i si $g(x) = x^n + a_{n-1}x^n + \ldots + a_1 x + a_0$ tenim $\overline{x}^n = -a_{n-1}\overline{x}^{n-1} - \ldots - a_1\overline{x} - a_0)$ $\overline{x}$ és ara una arrel del polinomi $g(x)$ en M on pensem $K \hookrightarrow M$ via $k_0 \mapsto k_0$

Observació 3.2.4. *Fixeu-vos que $\mathbb{Q}[x]/(x^3-2)$ és una extensió de $\mathbb{Q}$ introduint un element $\overline{x}$ amb la propietat $\overline{x}^3 = 2$. També tenim el cos $\mathbb{Q}[\sqrt[3]{2}]$ dins els complexos que és una extensió de $\mathbb{Q}$ amb l'element $\sqrt[3]{2}$ amb aquesta propietat. Aquests dos cossos són isomorfs (useu el morfisme evaluació), però com a cossos són diferents, fixeu-vos que $\mathbb{Q}[x]/(x^3-2)$ no es dins els nombres complexos, realment hi ha més d'una manera de definir un morfisme d'aquest cos a un cos isomorf a ell dins els nombres complexos, un és el cos $\mathbb{Q}[\sqrt[3]{2}]$, se us acudeix algún altre?*

Proposició 3.2.5. *Sigui K un cos i $f \in K[x]$ polinomi de grau ≥ 1. Llavors existeix un cos de descomposició F de $f(x)$ sobre K de forma que $[F:K] \leq n!$. A més, si F'/K és un altre cos de descomposició de F sobre K aleshores existeix un isomorfisme de cossos $\varphi : F \to F'$ amb $\varphi_{|K} = id$.*

Demostrem primer la primera part.

Demostració. Inducció $grau(f) = n$. Per $n = 1$ és clar el mateix K. Sigui $f(x)$ de grau $n \geq 2$, usant el teorema de Kronecker tenim que existeix E_1/K amb $[E_1 : K] \leq n$ on f té una arrel en E_1 (hi posem una arrel d'algun factor irreductible de f) per tant obtenim

$$f(x) = (x - \alpha_1)h(x) \in E_1[x]$$

per hipòtesi d'inducció existeix $\tilde{F}/E_1$ on h descompon totalment, en particular f i per la fórmula de graus en una torre de cossos tenim:

$$[\tilde{F} : K] = [\tilde{F} : E_1][E_1 : K] \leq (n-1)! \cdot n = n!$$

com $F \subset \tilde{F}$ (corresponent a agafar totes les arrels de f en $\tilde{F}$, i per tant existeix), obtenim $[F : K] \leq n!$. □

Veiem ara referent a la unicitat del cos de descomposició via isomorfisme. Ho farem també per inducció però demostrarem un lema més general que implica el resultat de la proposició anterior que ens falta demostrar:

Lema 3.2.6. *Sigui $f \in K[x]$ i $\psi : K \to^{\cong} K'$ un isomorfisme on $g(x) = \underline{\psi}(f(x))$. Sigui E/K extensió on E és un cos de descomposició de f, i E'/K' extensió on E' és un cos de descomposició per a g. Llavors existeix un aixecament $\tilde{\psi} : E \to E'$ que és isomorfisme on $\tilde{\psi}_{|K} = \psi$.*

Nosaltres per la proposició anterior prenem $K = K'$ i $\psi = id$.

Demostració. Inducció $grau(f) = n$. Si $n = 1$: $E = K$ i $E' = K'$ el resultat és clar. Sigui $n > 1$ i $f(x) = h(x)\ell(x)$ on pensem $\ell(x)$ irreductible de grau > 1 (si no existeix, f descompon en K i per tant el resultat és clar), per tant $g(x) = \underline{\psi}(h(x))\underline{\psi}(\ell(x)) = h_1(x)\ell_1(x)$ amb $\ell_1(x)$ irreductible. Sabem que existeixen $\alpha \in E$ i $\alpha_1 \in E'$ arrels de $\ell(x)$ i $\ell_1(x)$ respectivament en llurs cossos de descomposició per tant obtenim que existeix un lifting:

$$\hat{\psi} : K(\alpha) \to^{\cong} K'(\alpha_1)$$

on $\hat{\psi}_{|K} = \psi$, ara tenim que E és cos descomposició de $f(x)/(x-\alpha)$ sobre $K(\alpha)$ i E' de $g(x)/(x-\alpha_1)$ sobre $K'(\alpha')$; per hipòtesi d'inducció podem aixecar $\hat{\psi}$ a un isomorfisme $\tilde{\psi} : E \to^{\cong} E'$ on restringit a $K(\alpha)$ és $\hat{\psi}$ i per tant restringit a K és ψ com volíem demostrar. □

Exemple 3.2.7. *Trobeu un cos de descomposició per* x^p-2 *sobre* $\mathbb{Q}$, p *sempre denota un primer enter.*
El polinomi és irreductible per Eisenstein, si ho pensem dins $\mathbb{C}$ *(cos de descomposició tots són isomorfs, per àlgebra tots tenen les mateixes propietats però potser per altres coses per exemple analisis en ells,i.e. topologia, cal vigilar!!!) les arrels són* $2^{1/p} \in \mathbb{R}$, *i* $2^{1/p}w^j$ *amb* $j = 1, \ldots, p-1$ *on* $w = e^{2i\pi/p}$, *per tant* $F := \mathbb{Q}[2^{1/p}, 2^{1/p}w, \ldots, 2^{1/p}w^{p-1}]$ *és un cos de descomposició, observeu que* $w = \frac{2^{1/p}w}{2^{1/p}} \in F$ *i és clar que* $F \subset \mathbb{Q}[2^{1/p}, w]$ *on* $F = \mathbb{Q}[2^{1/p}, w]$. *Anem a*

calcular $[\mathbb{Q}[2^{1/p}, w] : \mathbb{Q}]$, *sabem que és de grau* $\leq p!$ *pel resultat anterior. És clar que*

$$\Pi := [\mathbb{Q}(2^{1/p}) : \mathbb{Q}] = grau(x^p - 2) = p$$

$$\Omega := [\mathbb{Q}(w) : \mathbb{Q}] = grau(Irr(w, \mathbb{Q})[x]) = grau(x^{p-1} + \ldots + x + 1) = p - 1$$

(la segona igualtat prové d'un exercici de classe de problemes d'irreductibilitat), com Π, Ω *divideixen* $[F : \mathbb{Q}]$ *i són coprimers (*$(\Pi, \Omega) = 1$*) obtenim que*

$$[\mathbb{Q}[2^{1/p}, w] : \mathbb{Q}] \geq p(p-1)$$

però fixeu-vos:

$$[\mathbb{Q}[2^{1/p}, w] : \mathbb{Q}] = [\mathbb{Q}(2^{1/p}, w) : \mathbb{Q}(2^{1/p})][\mathbb{Q}[2^{1/p}] : \mathbb{Q}] =$$

$$grau(Irr(w, \mathbb{Q}[2^{1/p}])[x]) \cdot grau(Irr(2^{1/p}, \mathbb{Q})[x]) \leq (p-1) \cdot p$$

i per tant obtenim que el grau és exactament $p(p-1)$.

Observació 3.2.8. *L'anterior exemple ens observa que per a donar el cos de descomposició ens ajuda molt pensar les arrels en algun lloc que hi siguin totes, fixeu-vos si ho pensem amb abstracte, construiríem primer el cos:*

$$E_1 := \mathbb{Q}[x]/x^p - 2$$

on en E_1 *hem introduït una arrel del polinomi* $x^p - 2$ *però ara es fa més dificil comprovar que* E_1 *no és cos de descomposició del polinomi* $x^p - 2$ *sobre* $\mathbb{Q}$, *és a dir comprovar que realment en* E_1 *no hi ha un nombre* $\alpha \neq 1$ *on* $\alpha^p = 1$ *amb* $\alpha := a_0 + a_1\overline{x} + \ldots + a_{p-1}\overline{x}^{p-1}$ *amb* $a_i \in \mathbb{Q}$ *on* $\overline{x}$ *compleix* $\overline{x}^p = 2$.

Observació 3.2.9 (IMPORTANT)**.** *Existència de la clausura algebraica.*
Donat un cos K *qualsevol, podem construir en abstracte una extensió* K^{alg}/K *que compleix la següent propietat: que tot polinomi sobre* $K[x]$ *descompon (amb factors de grau 1) totalment en* $K^{alg}[x]$, *i els elements de* K^{alg} *són algebraics sobre* K *(*K^{alg} *conté totes les arrels dels polinomis sobre* $K[x]$ *i tot element de* K^{alg} *és arrel d'un polinomi sobre* $K[x]$*). Aquest* K^{alg} *s'anomena clausura algebraica del cos* K *(i és única llevat d'isomorfisme) i usualment s'anota per* $\overline{K}$.
Fixeu-vos que donat un polinomi $p(x)$ *in* $K[x]$ *sempre podem pensar que un cos de descomposició de* $p(x)$ *sobre* K *està dintre d'aquest cos* $\overline{K}$, *i entre tots els cossos de descomposició de* $p(x)$ *exactament un es troba dins de* $\overline{K}$. *(Una referència per a demostrar la existència d'aquesta clausura la trobeu detallada en l'apèndix §A.2).*

Exercici: Demostreu que l'anterior definició de clausura algebraica $\overline{K}$ per a K coincideix amb la ser $\overline{K}/K$ una extensió algebraica sobre K complint que $\overline{K}$ és un cos algebraicament tancat, (és a dir que tot polinomi sobre $\overline{K}[x]$ té una arrel en $\overline{K}$).

Observació 3.2.10. *Comentar que Maple pot factoritzar a $\mathbb{Q}[x]$ o $(\mathbb{Z}/p)[x]$, mitjançant:*
>factor(polinomi);
>factor(polinomi) mod p;

Observem també aquí que podem fer càlculs en el Maple per $\mathbb{Q}(\alpha)$ amb α algebraic, per exemple
>alias(c=RootOf(X^2+2x+2));
introduix c com una arrel d'aquest polinomi,
>factor(x^4+4,c);
factoritza aquest polinomi en $\mathbb{Q}(c)$
També donat β algebraic sobre $\mathbb{Q}$ ens ajuda a decidir $Irr(\beta, \mathbb{Q}(\alpha))$, presentem un cas simple,
>alias(d=RootOf(x^3-x^2+x+8)); d arrel d'aquest polinomi sobre $\mathbb{Q}$,
>factor(x^3-x^2+x+8,c);
x^3-x^2+x+8
Aquest resultat ens diu que $Irr(d, \mathbb{Q}(c))(x) | Irr(d, \mathbb{Q})(x)$ en aquest cas és el mateix. Fem un altre exemple més interessant:
>factor(x^4+16,c);
$(x^2-4+4c)(x^2+4-4c)$
per tant si e és una arrel de x^4+16 tenim $Irr(e, \mathbb{Q})(x) = x^4+16$ (exercici fàcil), però $Irr(e, \mathbb{Q}(c))(x)$ serà un dels dos polinomis de grau 2 anteriors, hem de trobar amb quin dels dos e és una arrel.

Anem a introduir els cossos finits, abans fem el següent lema,

Lema 3.2.11. *Sigui $f(x) \in K[x]$ un polinomi de grau > 1. Llavors f té arrels múltiples (en qualsevol cos de descomposició) si i només si $mcd(f, f') \neq 1$ on f' denota la derivada formal del polinomi f (i.e. si $f(x) = a_n x^n + \ldots + a_1 x + a_0$ es defineix $f'(x) = na_n x^{n-1} + \ldots + 2a_2 x + a_1$, penseu que podem estar en cossos com els de característica $p > 0$)*

si S cos de característica $p > 0$ tenim $(a+b)^{p^l} = a^{p^l} + b^{p^l}$ per l enter i $a, b \in S$ ja que els coeficients combinatoris són a $\mathbb{Z}$ i $p | \binom{p}{k}$ per $k = 1, \ldots, p-1$; i fixeu-vos que si $S = \mathbb{F}_p$ tenim $a \in \mathbb{F}_p$ tenim $a^p = a$ pel petit Teorema de Fermat. Fixeu-vos també que si $p(x) = a_0 + a_1 x + \ldots + a_n x^n \in S[x]$ amb $car(S) = p > 0$ tenim $(p(x))^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots + a_n^p x^{np} \in S[x]$.

Exemple 3.2.12. *El polinomi $f(x) = x^p - 1$ en $\mathbb{F}_p[x]$ té arrels múltiples ja que $f'(x) = px^{p-1} = 0$ en $\mathbb{F}_p[x]$ per tant $mcd(f, f') = f \neq 1$. Efectivament $f(x) = x^p - 1 = (x-1)^p$ en $\mathbb{F}_p[x]$.*
El polinomi $g(x) = x^p - t \in \mathbb{F}_p(t)[x]$ és irreductible per Eisenstein i fixeu-vos $g'(x) = 0$, per tant g té arrels múltiples, efectivament $g(x) = (x - t^{1/p})^p \in \mathbb{F}_p(t^{1/p})[x]$.

Demostració. Sigui E un cos de descomposició per a $f(x)$, si té arrels repetides, diem $\alpha \in E$ la derivada de $f(x)$ en $E[x]$ tindrà el factor $x-\alpha$ per tant $(x-\alpha)$ divideix el $mcd(f,f')$ en $E[x]$, i per tant aquest no és trivial en $E[x]$, però el $mcd(f,f')$ pertany a $K[x]$ i si fos 1 també ho seria a $E[x]$, per tant el resultat. □

Cossos Finits. Tots els cossos finits.

Lema 3.2.13. *Si K és un cos finit llavors $|K| = p^n$ per cert p primer.*

Demostració. Si K té caracteristica zero $\mathbb{Z}$ seria un subanell de K via el morfisme característica (del repàs d'anells del curs, recordeu-ho!), i també el cos quocient de $\mathbb{Z}$ que és $\mathbb{Q}$ s'injectaria en K. Per tant si K és finit K ha de tenir característica $p > 0$ i $\mathbb{F}_p \subset K$ on la inclusió és via el morfisme característica. Fàcilment tenim doncs que K és un $\mathbb{F}_p$-espai vectorial. D'aquí K és un $\mathbb{F}_p$-espai vectorial de dimensió finita si K és finit i per tant $|K| = p^n$ per a cert $n \in \mathbb{N}_{\geq 1}$. □

Proposició 3.2.14. *Considerem el polinomi $x^q - x \in \mathbb{F}_p[x]$ amb $q = p^n$. Sigui K un cos de descomposició d'aquests polinomi sobre $\mathbb{F}_p$. K és un cos finit de q-elements.*

Demostració. Ja sabem de l'existència de K anem a veure que té q elements. Considereu,

$$F_1 := \{\alpha \in K | \alpha^q = \alpha\}$$

(fixeu-vos que són exactament les arrels del polinomi $x^q - x$), veiem que F_1 és un cos, pel petit teorema de Fermat $\beta \in \mathbb{F}_p$ tenim $\beta^p = \beta$ i en particular $\beta^q = \beta$ on $\mathbb{F}_p \subseteq F_1$, i donats $\alpha, \beta \in F_1$ és clar que tenim $(\alpha+\beta)^{p^n} = \alpha + \beta$, $(\alpha\beta)^{p^n} = \alpha\beta$ i $\alpha^{-1} = \alpha^{q-2}$ per $\alpha \neq 0$ i $q > 2$ (o $\alpha^{-1} = \alpha$ quan $\mathbb{F}_2^*$), on F_1 subcos de K i com té totes les arrels del polinomi $F_1 = K$ a més té exactament q elements ja que $mcd(x^q + x, 1) = 1$. □

Lema 3.2.15. *Tot cos de q elements és isomorf a un cos de descomposició pel polinomi $x^q - x$.*

Demostració. F finit, $F^* = F - \{0\}$ grup abelià d'ordre $q-1$ on $x^{q-1} = 1$ $\forall x \in F^*$ per tant $x^q = x$ $\forall x \in F$ on $F \subset E$ on E un cos descomposició per $x^q - x$ i com amb dos tenen q elements tenim $F \cong E$. □

Exercici 3.2.16. *Demostreu que si F cos finit F^* és un grup abelià cíclic. A un generador d'aquest grup cíclic en F s'anomena un element primitiu pel cos F.*

Observació 3.2.17. *Donat un cos finit $\mathbb{F}_p$, i fixant una clausura algebraica $\overline{\mathbb{F}}_p$ al cos de descomposició de $x^q - x$ dins $\overline{\mathbb{F}}_p$ s'anota per $\mathbb{F}_q$, cos finit per q elements, on $q = p^n$ per a cert $n \in \mathbb{N}_{\geq 1}$.*

Exemple 3.2.18. *Considerem $x^2+x+1 \in \mathbb{F}_2[x]$ polinomi irreductible. Considerem el cos $\mathbb{F}_2[x]/(x^2+x+1)$ que té quatre elements: $0, 1 \in \mathbb{F}_2$ i $\overline{x}, \overline{x}+1$, observeu que $(\mathbb{F}_2[x]/(x^2+x+2))^*$ és un grup cíclic d'ordre 3 i tot $\alpha \in \mathbb{F}_2[x]/(x^2+x+1)$ compleix $\alpha^4 = \alpha$. Efectivament, escrivim-ho per $\overline{x}+1$:*

$$(\overline{x}+1)^2 = \overline{x}^2 + 1 = \overline{x} + 1 + 1 = \overline{x}$$

$$(\overline{x}+1)^3 = \overline{x}(\overline{x}+1) = \overline{x}^2 + \overline{x} = \overline{x} + 1 + \overline{x} = 1,$$

$$(\overline{x}+1)^4 = (\overline{x}+1)^3(\overline{x}+1) = (\overline{x}+1).$$

Exemple 3.2.19. *Recordem $Frob : E \to E$ amb $x \mapsto x^p$ és un morfisme de cossos si E té característica $p > 0$ [Exercici].*
Calculem ara $Aut_{\mathbb{F}_p}(\mathbb{F}_q)$ amb $q = p^n$. Fixem-nos

$$Frob : \mathbb{F}_q \to \mathbb{F}_q$$

i $Frob(\alpha) = \alpha^p = \alpha$ per $\alpha \in \mathbb{F}_p$ (pel petit Teorema de Fermat: $n^p \equiv n(mod\ p)$), a més és clar $Frob$ és automorfisme ja que és mono entre conjunts finits amb el mateix nombre d'elements.

Recordem que $\mathbb{F}_q$ és cos de descomposició del polinomi $x^q - x$, i fixem-nos que $Frob^n(\delta) = Frob \circ \ldots^n \circ Frob(\delta) = \delta^{p^n} = \delta^q = \delta$ per $\delta \in \mathbb{F}_q$ per tant $Frob^n = id \in Aut_{\mathbb{F}_p}(\mathbb{F}_q)$, a més no hi ha una potència inferior del $Frob$ que doni la identitat (ja que si $Frob^m = id$ tenim $\delta^{p^m} = \delta$ per tot $\delta \in \mathbb{F}_q$ i per tant $\mathbb{F}_q$ ésta dins el cos de descomposició de $x^{p^m} - x$ que té menys elements!!!). Per tant tenim

$$< Frob > \leq Aut_{\mathbb{F}_p}(\mathbb{F}_q),$$

on $| < Frob > | = n$. Sabem que $|Aut_{\mathbb{F}_p}(\mathbb{F}_q)| \leq [\mathbb{F}_q : \mathbb{F}_p] = n$ ($\mathbb{F}_q$ com $\mathbb{F}_p$-espai vectorial té dimensió n), per tant obtenim

$$< Frob > = Aut_{\mathbb{F}_p}(\mathbb{F}_q)$$

i és un grup abelià cíclic d'ordre $n = [\mathbb{F}_q : \mathbb{F}_p]$.

Observació 3.2.20. *Comentar que Maple conté un paquet de Teoria de Galois per a fer càlculs en cossos finits, per exemple pot trobar un element primitiu per $\mathbb{F}_q$, crideu-lo mitjançant: readlib(GF), s'usa $GF(q)$ per denotar cos finit en q-elements, i la notació és també del fet d'acreditar a Galois també la construcció de cossos finits en general.*

3.3 Extensions normals

Definició 3.3.1. *Sigui F/K una extensió algebraica. Diem que F/K és normal si tot $f(x) \in K[x]$ irreductible en $K[x]$ que té una arrel en F descompon (totalment) en $F[x]$ (i.e. si $f(x)$ irreductible en $K[x]$ i té una arrel en F llavors totes les arrels de $f(x)$ estan a F i $f(x)$ factoritza en factors de grau 1 en $F[x]$).*

Exemple 3.3.2.

1. *$\mathbb{C}/\mathbb{Q}$ no compleix la condició de normalitat ja que $\mathbb{C}/\mathbb{Q}$ no és algebraica (tot i que si compleix que tot polinomi que té una arrel en $\mathbb{C}$ descompon en $\mathbb{C}[x]$), en $\mathbb{C}$ tenim nombres transcendents sobre $\mathbb{Q}$ com per exemple π.*
   Recordem ara l'observació 3.2.9, i pensem $\overline{\mathbb{Q}} \subset \mathbb{C}$, tenim llavors que $\overline{\mathbb{Q}}/\mathbb{Q}$ és normal, recordeu que vau demostrar a problemes que $[\overline{\mathbb{Q}} : \mathbb{Q}]$ no és finit.

2. *Considerem $\mathbb{F}_q/\mathbb{F}_p$ és normal ja que $g(x) \in \mathbb{F}_p[x]$ irreductible i té arrel en $\mathbb{F}_q$ llavors $g(x)|x^q - x$ i com $\mathbb{F}_q$ té totes les arrels del polinomi $x^q - x$ també les de $g(x)$.*

3. *Considerem* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. *Aquesta extensió no és normal, ja que* x^3-2 *irreductible sobre* $\mathbb{Q}[x]$ *i en* $\mathbb{Q}(\sqrt[3]{2})$ *tan sols hi tenim una de les tres arrels del polinomi. (Observeu que* $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{id\}$ *i tenim que* $|Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))| = 1 \leq [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$*).*

4. *Considerem* $\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}$, *on* $w \neq 1$ *amb* $w^3 = 1$, *pensem* $w = e^{2\pi i/3}$, *on* $\mathbb{Q}(\sqrt[3]{2})$ *és un cos de descomposició del polinomi* x^3-2 *sobre* $\mathbb{Q}[x]$. *Veurem que en aquest cas és normal, veieu el proper teorema.*

En aquest curs a partir d'ara majoritàriament treballarem per extensions finites, tot i que moltes coses es poden fer per a extensions no finites.

Teorema 3.3.3. *Sigui* E/K *una extensió finita.*
E/K *és normal si i només is* E *és cos de descomposició sobre* K *d'algun* $f \in K[x]$.

Demostració. Com E/K finita escrivim $E = K(\alpha_1, \ldots, \alpha_n)$ amb α_i algebraics sobre K.

Suposem primer que E/K normal. Escrivim $g_i(x) = Irr(\alpha_i, K)[x]$, de la hipòtesi de normalitat cada $g_i(x)$ té totes les arrels en E ja que $\alpha_i \in E$, d'aquí obtenim que en E el polinomi

$$f(x) = g_1(x) \cdot \ldots \cdot g_n(x) \in K[x]$$

descompon en factors de grau 1, per tant E cos de descomposició de f.

Suposem ara E cos de descomposició per algun $f(x) \in K[x]$ i si diem $\gamma_1, \ldots, \gamma_m$ les arrels f en E, $E = K(\gamma_1, \ldots, \gamma_m)$. Sigui $g(x) \in K[x]$ irreductible on $\exists \beta_1 \in E$ arrel de g en E, volem demostrar que totes les arrels de $g(x)$ són llavors en E, si el grau 1 o tan sols en un cos de descomposició de g té una arrel ja estem, suposem doncs $g(x)$ té dues arrels β_1 i β_2. Considerem $M = E(\beta_1, \ldots, \beta_s)$ un cos de descomposició de $g(x)$ sobre E on β_i's són les arrels de $g(x)$ (aquest cos conté $K(\beta_1, \ldots, \beta_n)$ que seria un cos de descomposició de g sobre K, però fixeu-vos l'ordre en escriure-ho de la importància de on hem construït les arrels del polinomi).
Tenim que existeix un isomorfisme $\varphi : K(\beta_1) \to K(\beta_2)$ amb $\varphi_K = id$ portant $\beta_1 \mapsto \beta_2$ ja que $\underline{\varphi}(Irr(\beta_1, K)) = \underline{id}(g(x)) = g(x)$ i β_2 és arrel de $g(x)$. Usant ara el resultat 3.2.6 obtenim que l'isomorfisme puja a un isomorfisme $\hat{\varphi} : E \to E'$ on E cos descomposició de f i E' cos de descomposició $\underline{\varphi}(f(x)) = f(x)$ sobre $K(\beta_2)$ ja que $f \in K[x]$, però pensant $E' \subset M$ tenim $E' = K(\beta_2, \gamma_1, \ldots, \gamma_m) = E(\beta_2)$, com de l'iso tenim $[E : K] = [E' : K] = [E(\beta_2) : K] = [E(\beta_2) : E][E : K]$ i per tant $E(\beta_2) = E$ provant $\beta_2 \in E$. □

Corol·lari 3.3.4. *Sigui* E/K *extensió normal i finita. Sigui* $K \subset F \subset E$ *on* F *cos. Llavors* E/F *és normal i finita.*

Demostració. E és cos de descomposició de f sobre K, doncs també és cos de descomposició de f sobre F. □

Exemple 3.3.5. *Hem vist que* $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$ *és normal, per tant* $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}(\sqrt[3]{2})$ *també és una extensió normal, però observeu que* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *no és una extensió normal.*

Proposició 3.3.6. *Sigui E/K extensió finita normal. Sigui $K \subset F \subset E$ extensió cossos. Suposem que tenim un morfisme de cossos $\varphi : F \hookrightarrow E$ on $\varphi_{|K} = id$. Llavors φ s'extén almenys a un $\hat{\varphi} \in Aut_K(E)$ on $\hat{\varphi}_{|F} = \varphi$ i $\hat{\varphi}_{|K} = id$.*

Demostració. Com E/K normal finita, tenim que E cos descomposició de $f(x) \in K[x]$. També E cos descomposició de f sobre F, fixem-nos $\varphi : F \to^{\cong} \varphi(F) \subset E$ i com $\varphi(f(x)) = f(x)$ del fet $f \in K[x]$ i $\varphi_{|K} = id$ obtenim del lemma 3.2.6 (E també és cos descomposició de f sobre $\varphi(F)$) que el morfisme s'aixeca a un isomorfisme $\hat{\varphi} : E \to E$ amb $\hat{\varphi}_{|F} = \varphi$ i $\hat{\varphi}_{|K} = id$. □

Proposició 3.3.7. *Sigui E/K extensió normal i finita, i considerem $Aut_K(E)$. Sigui F un cos on $K \subset F \subset E$. Llavors:*

$$F/K \text{ normal si i només si } \varphi(F) = F \ \forall \varphi \in Aut_K(E),$$

(on $\varphi(F) = F$ no vol dir que és fix per a cada element $f \in F$, sinó que porta un element del cos F a un element del cos F).

Demostració. Suposem primer que F/K és normal, i $\sigma \in Aut_K(E)$. Sigui $\alpha \in F$, considerem $Irr(\alpha, K)[x]$ tenim $Irr(\alpha, K)[\sigma(\alpha)] = \sigma(Irr(\alpha, K)[\alpha]) = \sigma(0) = 0$ per tant $\sigma(\alpha)$ arrel $Irr(\alpha, K)[x]$ i com descompon sobre F ja que F/K normal tenim $\sigma(\alpha) \in F$, per tant $(K \subseteq)\sigma(F) \subseteq F$ i com $[\sigma(F) : K] = [F : K]$ tenim $\sigma(F) = F$.

Suposem ara que $\sigma(F) = F \ \forall \sigma \in Aut_K(E)$. Sigui $\alpha \in F$, considerem $Irr(\alpha, K)[x]$ que té una arrel en F, per veure normalitat és suficient demostrar que aquest polinomi descompon en F. Com E/K normal i $\alpha \in E$ tenim que $Irr(\alpha, K)[x]$ descompon en E, sigui β una arrel d'$Irr(\alpha, K)[x]$ (que pertany a E, E/K normal), per tant tenim un morfisme $\varphi : K(\alpha) \hookrightarrow K(\beta) \subset E$ de cossos on $\varphi_{|K} = id$. Com E cos descomposició de cert f sobre K (pel teorema 3.3.3) i també és cos descomposició de f sobre $K(\alpha)$ i $K(\beta)$) pel lema 3.2.6 anterior φ puja a un $\sigma \in Aut_K(E)$ per tant $\sigma(\alpha) = \beta \in F$ per hipòtesi, provant el que volem. □

3.4 Elements separables i extensions separables

Sigui $f \in K[x]$ un polinomi, i sigui E un cos de descomposició per a $f(x)$. Diem que $f(x)$ és separable si tots els polinomis irreductibles que divideixen f en $K[x]$ no tenen arrels múltiples en E.

Definició 3.4.1. *Sigui M/K una extensió i $\alpha \in M$. Diem que α és separable sobre K si és algebraic sobre K i $Irr(\alpha, K)[x]$ és un polinomi separable.*
Diem que M/K és una extensió separable si tot $\alpha \in M$ és separable sobre K.

És fàcil observar:

Lema 3.4.2. *Si M/K finita i separable i $K \subseteq L \subseteq M$ llavors M/L i L/K són extensions separables.*

Demostració. Que L/K separable és clar ja que $\alpha \in L \subset M$ tenim $Irr(\alpha, K)[x]$ no té arrels múltiples en un cos de descomposició. Veiem M/L separable, tenim

$m \in M$ $Irr(m,K)[x]$ no té arrels múltiples en un cos de descomposició, però observeu que $Irr(m,L)[x]|Irr(m,K)[x]$ en $L[x]$ però en particular el polinomi $Irr(m,L)[x]$ tampoc tindrà arrels múltiples en un cos de descomposició per aquest polinomi. □

Observació 3.4.3. *Recordem de nou que si $K(\alpha)/K$ és extensió finita simple de grau d, i tenim $j : K \hookrightarrow L$, tenim que $Irr(\alpha,K)[x]$ té grau d. Recordem que podem pujar el morfisme a $\hat{j} : K(\alpha) \to L$ amb $\hat{j}_{|K} = j$ de ℓ maneres on ℓ són les arrels diferents en L del polinomi $\underline{j}(Irr(\alpha,K)[x])$, per tant per haver-hi exactament d hem d'imposar que totes les arrels d'aquest polinomi son a L ("normalitat") i que aquest polinomi irreductible no tingui arrels repetides ("separabilitat").*

Es té el següent resultat que no demostrarem:

Proposició 3.4.4. *Si L/K extensió finita de grau d i $j : K \hookrightarrow M$ monomorfisme. Si L/K separable, $m_\alpha(x) = Irr(\alpha,K)[x]$ i $\underline{j}(m_\alpha(x))$ descompon sobre M per a cada $\alpha \in L$ llavors hi ha exactament d morfismes de $\Phi_i : L \to M$ complint $\Phi_{i|K} = j$.*
Altrament si existeix $\alpha \in L$ no separable sobre K o bé algun $\underline{j}(m_\alpha)$ no descompon sobre M hi ha estrictament menys de d morfismes $\Phi : L \hookrightarrow M$ complint $\Phi_{|K} = j$.

Demostrem un resultat més particular per a recordar-nos de la demostració del corol.lari 3.1.2 on la demostració de la proposició anterior és similar a la proposició que segueix.

Exercici 3.4.5. *Demostreu la proposició 3.4.4.*

Proposició 3.4.6. *Si L/K extensió finita de grau d i $incl : K \hookrightarrow L$ monomorfisme corresponent a la inclusió. Si L/K separable, $m_\alpha(x) = Irr(\alpha,K)[x]$ i $\underline{id}(m_\alpha[x]) = m_\alpha(x)$ dsecompon sobre L per a cada $\alpha \in L$ llavors hi ha exactament d automorfismes $\Phi_i : L \to L$ complint $\Phi_{i|K} = incl_{|K} = id$.*
Altrament si existeix $\alpha \in L$ no separable sobre K o bé algun $\underline{id}(m_\alpha[x])$ no descompon sobre L hi ha estrictament menys de d morfismes.

Demostració. Veiem primer si existeix α on no és separable sobre K o bé $m_\alpha(x)$ no decompon sobre L llavors $|Aut_K(L)| < [L : K]$. Recordant i tenint present la demostració del corol.lari 3.1.2, prenem $\alpha_1 = \alpha$ i escrivim $L = K(\alpha, \alpha_2, \ldots, \alpha_n)$ amb $[K(\alpha) : K] \neq 1$, en la demostració del corol.lari 3.1.2 vam demostrar $|Aut_K(L)|$ és igual al nombre d'aixecaments de monomorfismes de L a L que es poden obtenir per a cada $\beta : K(\alpha) \hookrightarrow L$ on la restricció de β a K és la identitat. Fixant β d'aquests monos de L a L n'hi ha com a molt $[L : K(\alpha)]$ de possibles per a cada β. Sabem que el nombre de morfismes β's és el nombre d'arrels de $m_\alpha(x)$ en L que és $< [K(\alpha) : K]$ per hipòtesi en α, per tant el nombre d'automorfismes és

$$|Aut_K(L)| \leq [L : K(\alpha)]\#\beta's < [L : K(\alpha)][K(\alpha) : K] = [L : K].$$

Anem ara imposar que tot $\alpha \in L$ és separable sobre K i $m_\alpha(x)$ descompon en L per a tot α. Com L/K finita escrivim $L = K(\alpha_1, \ldots, \alpha_n)$. Denotem per $K_i = K(\alpha_1, \ldots, \alpha_i)$ vam demostrar que per a pujar un morfisme $\varphi : K_i \hookrightarrow L$ a r morfismes $K_{i+1} \hookrightarrow L$ on la restricció a K_i sigui φ la condició necessàrea i

suficient es que $\underline{\varphi}(Irr(\alpha_{i+1}, K_i)[x])$ tingui exactament r arrels diferents en L, fixem-nos ara que

$$Irr(\alpha_{i+1}, K_i)[x] | Irr(\alpha_{i+1}, K)[x]$$

i

$$\underline{\varphi}(Irr(\alpha_{1+1}, K_i)[x]) | \underline{\varphi}(Irr(\alpha_{i+1}, K)[x]) = Irr(\alpha_{i+1}, K)[x]$$

ja que $\varphi_{|K} = id$ com el polinomi de la dreta descompon en L sense arrels repetides ja que α_{i+1} separable, tenim que les arrels diferents en L de $\underline{\varphi}(Irr(\alpha_{1+1}, K_i)[x])$ és exactament $[K_i(\alpha_{i+1}) : K_i]$ i per tant cada φ s'aixeca en $[K_{i+1} : K_i]$ morfismes, començant per K_0 fins arribar a $K_n = L$ obtenim que $|Aut_K(L)| \geq \prod_{i=0}^{n-1}[K_{i+1} : K_i] = [L : K]$ per tant la igualtat. □

Donat L/K finita sempre $\alpha \in L$ són separables? NOOOOOOOOOO!!!!

Anem-ho a estudiar una mica, tot i que molt poc aquest curs.

Fixeu-vos si $\alpha \in L \setminus K$ no separable llavors $Irr(\alpha, K)[x] = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in K[x]$ $(n \geq 2)$ té arrels múltiples en un cos de descomposició per tant tenim

$$(mcd(Irr(\alpha, K)[x], Irr(\alpha, K)[x]')) \neq (1) \text{ en } K[x]$$

per la irreductibilitat de $Irr(\alpha, K)[x]$ en $K[x]$ l'única possibilitat és quan

$$(nx^{n-1} + \ldots + a_1 =) Irr(\alpha, K)[x]' = 0 \in K[x]$$

és a dir és el polinomi zero per tant:

Proposició 3.4.7. *Sigui L/K extensió algebraica i suposem que $car(K) = 0$, llavors és L/K separable.*

Per tant elements no separables és particular per cossos amb $car(K) = p > 0$, i del fet que la derivada del polinomi irreductible ha de ser zero, els polinomis irreductibles amb arrels múltiples són de la forma:

$$p(x) = a_0 + a_1x^p + a_2x^{2p} + \ldots + a_nx^{pn} \in S[x]$$

on S cos amb $car(S) = p > 0$ (p denota sempre primer).

Exemple 3.4.8. *1. $\mathbb{F}_q/\mathbb{F}_p$ és separable ja que tot $\alpha \in \mathbb{F}_q$ és una arrel de $x^q - x$ i per tant $Irr(\alpha, \mathbb{F}_p)[x] | x^q - x$ i la derivada de $x^q - x$ és -1 per tant $gcd(x^q - x, -1) = 1$ no té arrels múltiples $x^q - x \in \mathbb{F}_q[x]$ i per tant tampoc $Irr(\alpha, \mathbb{F}_p)[x]$ (en $\mathbb{F}_q[x]$ on recordeu $\mathbb{F}_q$ és un cos de descomposició per a $x^q - x$).*

2. Tota extensió algebraica de $\mathbb{Q}$ és separable ja que $car(\mathbb{Q}) = 0$.

3. L'extensió $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ de grau p no és separable, és fàcil demostrar $p(x) = Irr(t, \mathbb{F}_p(t^p))[x] = x^p - t^p$ i $p'(x) = 0 \in \mathbb{F}_p(t^p)[x]$ per tant té $p(x)$ arrels repetides en el cos de descomposició, efectivament comproveu:

$$x^p - t^p = (x - t)^p \in \mathbb{F}_p(t)[x].$$

Observació 3.4.9. *Recordem de nou que: si S cos de característica $p>0$ tenim $(a+b)^{p^l}=a^{p^l}+b^{p^l}$ per l enter i $a,b\in S$ ja que els coeficients combinatoris són a $\mathbb{Z}$ i $p|\begin{pmatrix} p \\ k \end{pmatrix}$ per $k=1,\ldots,p-1$; i fixeu-vos que si $S=\mathbb{F}_{p^l}$ tenim $a\in\mathbb{F}_{p^l}$ tenim $a^{p^l}=a$ per definició del cos finit $\mathbb{F}_{p^l}$.*
Fixeu-vos també que si $p(x)=a_0+a_1x+\ldots+a_nx^n\in S[x]$ amb $car(S)=p>0$ tenim $(p(x))^p=a_0^p+a_1^px^p+a_2^px^{2p}+\ldots+a_n^px^{np}\in S[x]$.

Si tenim elements separables sobre K és el cos que genera K i aquests elements una extensió separable sobre K? La resposta és sí, anem-ho a justificar tot seguit. (Ho demostrem com una aplicació de la proposició 3.4.4)

Proposició 3.4.10. *Sigui L/K finita, escrivim $L=K(\alpha_1,\ldots,\alpha_n)$. Si α_1 és separable sobre K i α_i és separable sobre $K(\alpha_1,\ldots,\alpha_{i-1})$ per $i=2,\ldots,n$ llavors L/K és una extensió separable.*

Demostració. Fem-ho per inducció en n. Per $n=1$ $L=K(\alpha)$, sigui E un cos descomposició de $Irr(\alpha,K)[x]$ amb $L\subseteq E$. Hem demostrat abans (bé ja fa una mica) que el nombre de monomorfismes de $K(\alpha)$ en E de forma que la restricció en K sigui la identitat són exactament el nombre d'arrels diferents de $Irr(\alpha,K)[x]$ en E, com α separable i E cos de descomposició, tenim que hi ha exactament $grau(Irr(\alpha,K)[x])=[L:K]$-morfismes, per tant per la proposició 3.4.4 L/K és separable.

Suposem cert per $k\geq 1$ i veiem-ho per a $k+1$. $L=K(\alpha_1,\ldots,\alpha_{k+1})$ i escrivim $K_j=K(\alpha_1,\ldots,\alpha_j)$ amb $1\leq j\leq k+1$). Considerem E el cos de descomposició de $f(x)=\prod_{i=1}^{k+1}Irr(\alpha_i,K)[x]$ (cada α_i és algebraic ja que L/K finita). Per hipòtesi d'inducció K_k/K és separable, per tant tenim que hi ha $[K_k:K]$-morfismes de K_k en E on la restricció a K és el morfisme identitat ja que E conté un cos de descomposició E' de $\prod_{i=1}^{k}Irr(\alpha_i,k)[x]$ i per tant $m_\alpha(x)$ descompon en E' (i per tant també en E) per tot $\alpha\in K_k$. Sigui φ un d'aquests monomorfismes, $\varphi:K_k\hookrightarrow E$ on $\varphi_{|K}=id$. Anem a veure quan morfismes podem pujar $\hat{\varphi}:L\hookrightarrow E$ amb $\hat{\varphi}_{|K_k}=\varphi$. Hem demostrat que n'hi ha tants com arrels diferents en E del polinomi $\underline{\varphi}(Irr(\alpha_{k+1},K_k)[x])$, aquest polinomi no té arrels repetides per hipòtesi α_{k+1} separable sobre K_k a més

$$\underline{\varphi}(Irr(\alpha_{k+1},K_k)[x])|\underline{\varphi}(Irr(\alpha_{k+1},K)[x])=Irr(\alpha_{k+1},K)[x]$$

i com E té totes les arrels de $Irr(\alpha_{k+1},K)[x]$ també té totes les arrels de $\underline{\varphi}(Irr(\alpha_{k+1},K_k)[x])$, demostrant que hi ha exactament $[L:K_k]$ possibles $\hat{\varphi}$, per tant tenim que els monomorfismes de L a E n'hi ha com a mínim $[L:K_k][K_k:k]=[L:k]$, per tant L/K és separable usant proposició 3.4.4.

□

Corol·lari 3.4.11. *Sigui L/K una extensió, i siguin $\alpha_1,\ldots,\alpha_n$ elements algebraics i separables sobre K llavors $K(\alpha_1,\ldots,\alpha_n)/K$ és una extensió separable.*

Demostració. Directe de l'anterior resultat ja que si α_i separable sobre K també ho és sobre $K(\alpha_1,\ldots,\alpha_{i-1})$ per $i\geq 2$, ja que $Irr(\alpha_i,K(\alpha_1,\ldots,\alpha_{i-1})[x]|Irr(\alpha_i,K)[x]$.

□

Corol·lari 3.4.12. *Si L/K és cos de descomposició d'un polinomi separable $f(x)\in K[x]$, llavors L/K és separable.*

Demostració. $L = K(\alpha_1, \ldots, \alpha_n)$ on α_i són les arrels de $f(x)$ on $Irr(\alpha_i, K)[x]|f(x)$ en $K[x]$ i per tant no tenen arrels multiples d'on $\alpha_1, \ldots, \alpha_n$ són separables sobre K, aplicant la proposició anterior finalitzem. □

Corol·lari 3.4.13. *Si L/M i M/K són extensions finites separables llavors L/K és separable.*

Demostració. Com L/M i M/K finites escrivim $L = M(\beta_1, \ldots, \beta_m)$, $M = K(\alpha_1, \ldots, \alpha_n)$, per tant $L = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$. Els α_i són separables sobre K per ser M/K separable en particular α_i separable sobre $K(\alpha_1, \ldots, \alpha_{i-1})$. Sabem també que β_i són separables sobre M i en particular sobre $K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_{i-1})$ aplicant la proposició 3.4.10 finalitzem. □

Capítol 4

Teorema principal de la teoria de Galois finita

4.1 Extensions de Galois. Teorema d'Artin.

Definició 4.1.1. *Sigui L/K una extensió algebraica, diem que L/K és de Galois si és normal i separable. En aquest cas escriurem $Gal(L/K)$ pel grup $Aut_K(L)$.*

Proposició 4.1.2. *Sigui L/K finita. Llavors:*

$$L/K \text{ Galois si i només si } |Aut_K(L)| = [L : K].$$

Demostració. Suposem L/K Galois, per cada $\alpha \in L$ tenim $Irr(\alpha, K)[x]$ descompon en L i no té arrels repetides, per tant per la proposició 3.4.6 hi ha exactament $[L : K]$ morfismes i com sempre $|Aut_K(L)| \leq [L : K]$ obtenim una implicació.

Suposem ara que $|Aut_K(L)| = [L : K]$. Sigui $\alpha \in L$, com finita considerem $Irr(\alpha, K)[x]$ és suficient demostrar que té totes les arrels en L (per demostrar normalitat, penseu-ho un moment!!!) i que no té arrels repetides per obtenir la condició de separabilitat. Anem-ho a fer.
Seguim la demostració de $|Aut_K(L)| \leq [L : K]$: Considerem $\alpha = \alpha_1$ vam demostrar que

$$|Aut_K(L)| \leq [L : K(\alpha)] \cdot A$$

on A és el nombre d'arrels diferents en L de $Irr(\alpha, K)[x]$; com sempre $A \leq [K(\alpha) : K]$ i tenim ara que $|Aut_K(L)| = [L : K]$ per hipòtesi, obtenim $A = [K(\alpha) : K]$ on per tant el nombre d'arrels diferents en L de $Irr(\alpha, K)[x]$ és justament el grau, és a dir descompon en L aquest polinomi i no té arrels repetides, demostrant el que voliem.

□

Corol·lari 4.1.3. *Si F/K és una extensió finita de Galois i M és un cos tal que $K \subseteq M \subseteq F$ tenim F/M és Galois.*

Demostració. Com F/K Galois es normal, cos de descomposició d'un polinomi sobre K, triant el mateix polinomi s'obté que F/M és normal. Referent a la separabilitat, com F/K separable, $Irr(\alpha, M)[x]|Irr(\alpha, K)[x]$ per tot $\alpha \in F$ per tant no tindrà tampoc arrels múltiples on F/M és separable. □

Fixem L/K una extensió finita i sigui $Aut_K(L)$ el grup d'automorfismes de L que deixa fix K.

Sigui $H \leq Aut_K(L)$ un subgrup, definim

$$\Phi(H) := L^H := \{x \in L | \sigma(x) = x, \forall \sigma \in H\}$$

que conté K i és subcos de L, per tant tenim un cos

$$K \subset L^H \subset L$$

és a dir:

$$\Phi : \{subgrups\ Aut_K(L)\} \to \{subcos\ de\ L\ que\ conté\ K\}$$

$$H \mapsto L^H.$$

Igualment donat un cos F entre K i L (és a dir $K \subseteq F \subseteq L$) definim el subgrup de $Aut_K(L)$ següent:

$$\Psi(F) := \{\sigma \in Aut_K(L) | \sigma(v) = v, \forall v \in F\} \leq Aut_K(L),$$

és a dir

$$\Psi : \{subcos\ L\ conté\ K\} \to \{subgrups\ Aut_K(L)\}.$$

Lema 4.1.4. *Sigui L/K extensió i $H \leq Aut_K(L)$, i F un cos intermedi entre L i K és té:*

1. $H \subseteq \Psi(\Phi(H))$,
2. $F \subseteq \Phi(\Psi(F))$,
3. $\Phi \circ \Psi \circ \Phi(H) = \Phi(H)$,
4. $\Psi \circ \Phi \circ \Psi(F) = \Psi(F)$.

Demostració. Per (i) resseguint les definicions és clar que

$$H \subseteq \Psi(\Phi(H)) = \{\sigma \in Aut_K(L) | \sigma(x) = x, \forall x \in \Phi(H) = L^H\}.$$

Per (ii) resseguint les definicions també és obvi: fixem-nos que $\Psi(M)$ són automorfismes que fixen M en cada punt, per tant els elements de L que queden fixats per $\Psi(M)$ s'hi troba M.
Per (iii), fixem-nos que per (ii) tenim $\Phi(H) \subset \Phi\Psi(\Phi(H))$, veiem l'altra inclusió. Fixeu-vos que aplicar Φ en dos subgrups $H_1 \subset H_2$ s'obté per definició $\Phi(H_2) \subseteq \Phi(H_1)$ canvia el sentit de la inclusió, per tant de (i) com $H \subseteq \Psi(\Phi(H))$ tenim que $\Phi\Psi\Phi(H) \subseteq \Phi(H)$ obtenint (iii).
Un argument semblant de (iii) us serveix per demostrar (iv), exercici. □

Teorema 4.1.5. *Sigui F/K extensió finita, $H \leq Aut_K(F)$, considerem F^H subcos de F que conté K. Llavors F/F^H és Galois, en particular $[F : F^H] = |H|$.*

Demostració. Observem que és clar que $H \leq Aut_{F^H}(F)$ ja que F^H està fixat element a element per cada element de H, per tant tenim

$$|H| \leq |Aut_{F^H}(F)| \leq [F : F^H].$$

Volem demostrar igualtat, la igualtat prové del següent resultat d'Artin □

Teorema 4.1.6 (Artin)**.** *Sigui F/K extensió finita,$H \leq Aut_K(F)$, considerem F^H subcos de F que conté K, i $m = |H|$ el nombre d'elements del grup H. Considerem $m+1$ elements qualsevol de F: $u_1, \ldots, u_{m+1}$, llavors aquests $m+1$-elements són F^H-linealment dependents, per tant $[F : F^H] \leq m$.*

Demostració. Suposem que $u_1, \ldots, u_{m+1}$ son F^H-linealment independents.

Considerem el sistema lineal homogeni de n equacions amb $n+1$-incògnites en el cos F següent:

$$\sum_{i=1}^{n+1} \sigma(u_i)x_i = 0 \tag{4.1}$$

per tot $\sigma \in H$. Com és sistema compatible indeterminats, siguin doncs $a_1, \ldots, a_{n+1} \in F$ no tots zero solució del sistema (4.1) i triem-la aquesta amb $|\{i|a_i \neq 0\}|$ el més petit possible. Sense pèrdua de generalitat (feu una reordenació si cal) podem pensar $a_{n+1} \neq 0$. Tenim llavors

$$\sigma(u_{n+1}) = \sum_{j=1}^{n} \sigma(u_j)b_j \tag{4.2}$$

on $b_j = -a_j a_{n+1}^{-1}$ per $j = 1, \ldots, n$ per tot $\sigma \in H$, en particular per $\sigma = id$ obtenim

$$u_{n+1} = \sum_{j=1}^{n} u_j b_j$$

i com per hipòtesi u_i són F^H-linealment independents obtenim algun $b_j \notin F^H$, sense pèrdua de generalitat podem suposar que $b_1 \notin F^H$. Com $b_1 \notin F^H$, existeix $\tau \in H$ on $\tau(b_1) \neq b_1$, per tant aplicant τ a l'equació (4.2) obtenim

$$\tau\sigma(u_{n+1}) = \sum_{i=1}^{n} \tau\sigma(u_j)\tau(b_j) \tag{4.3}$$

però fixeu-vos que $\sigma\tau = \sigma' \in H$ i podem escriure el sistema de (4.2) mitjançant:

$$\tau\sigma(u_{n+1}) = \sum_{i=1}^{n} \tau\sigma(u_j)b_j \tag{4.4}$$

restant (4.3)-(4.4) obtenim

$$0 = \sum_{j=1}^{n} \tau\sigma(u_j)(\tau(b_j) - b_j)$$

$\forall \sigma \in H$, per tant fent $\sigma' = \tau\sigma$:

$$0 = \sum_{j=1}^{n} \sigma'(u_j)(\tau(b_j) - b_j)$$

$\forall \sigma' \in H$ per tant:

$$|\{j|\tau(b_j) - b_j \neq 0\}| \leq |\{i|a_i \neq 0\}| - 1$$

i com $\tau(b_1) \neq b_1$ per tant és una solució no trivial del sistema (4.1) amb menys elements no zero (si $a_i = 0$ tenim $b_i = 0$ resseguint la demostració) en contra de la minimalitat triada per la solució del sistema. □

Demostració. [segueix demostració teorema 4.1.5] El resultat s'obté d'aplicar ara l'anterior resultat d'Artin. □

4.2 Teorema fonamental de la Teoria de Galois finita

Hem vist que per extensions de Galois finites F/K hi ha tants elements en el grup d'automorfismes com el grau, a més hem vist que subgrups H donen cossos intermedis F^H, demostrem que tots els cossos intermedis són així, és a dir el grup $Aut_K(F) = Gal(F/K)$ i tots els subgrups ens donen una bijecció amb tots els cossos que hi ha entre K i F pel cas F/K extensió finita i Galois.

Teorema 4.2.1 (fonamental de la teoria de Galois finita)**.** *Sigui F/K una extensió finita de cossos que és Galois, llavors:*

1. *les aplicacions Φ i Ψ de la secció anterior són bijeccions, és a dir tenim una bijecció entre subgrups de $Gal(F/K)$ amb els subcossos entre K i F.*
2. *si $H_1, H_2 \leq Gal(F/K)$, tenim F^{H_1}, F^{H_2}:*

   $$\exists \sigma \in Gal(F/K) \text{ on } \sigma(F^{H_1}) = F^{H_2} \Leftrightarrow H_1 = \tau H_2 \tau^{-1}$$

   per cert $\tau \in Gal(F/K)$, a més aquest τ és σ^{-1}.

   En particular (recordeu $H \trianglelefteq G$ subgrup normal, si i nomes si $\tau H \tau^{-1} = H$ $\forall \tau \in G$) tenim:

   $$F^H/K \text{ Galois} \Leftrightarrow H \trianglelefteq Gal(F/K)$$

   i aquest cas $Gal(F^H/K) \cong Gal(F/K)/Gal(F/F^H)$.

Demostració. Demostrem primer (i). Demostrem primer per $H \leq Gal(F/K)$ que $\Psi\Phi(H) = H$.
Fixem-nos $\Phi(H) = F^H$ i sabem per Artin F/F^H Galois on $|Gal(F/F^H)| = [F : F^H] = |H|$ i com $H \leq Gal(F/F^H)$ (per definició de F^H) obtenim $H = Gal(F/F^H) = Aut_{F^H}(F)$ on per definició $\Psi(\Phi(H)) = Aut_{F^H}(F)$ obtenint $\Psi\Phi(H) = H$.

Veiem ara que $\Phi\Psi(M) = M$ per tot cos intermedi (provant que $\Phi\Psi = id$ i d'abans $\Psi\Phi = id$):

Observem que $\Phi(\Psi(M)) = \Phi(Aut_M(F)) = F^{Aut_M(F)}$, i tenim la inclusió de cossos (recordeu que F/K Galois tenim F/M Galois corol.lari **??**):

$$M \subseteq F^{Gal(F/M)} \subseteq F$$

Com F/M Galois $[F : M] = |Gal(F/M)|$ i del teorema d'Artin tenim $[F : F^{Gal(F/M)}] = |Gal(F/M)|$ per tant $M = F^{Gal(F/M)} = \Phi\Psi(M)$.

Demostrem ara l'apartat (ii): anomenem també F_1 a F^{H_1} i F_2 a F^{H_2} sigui $\sigma \in Gal(F/K)$ on $\sigma(F^{H_1}) = F^{H_2}$, tenim llavors per tot $b \in F^{H_2}$ $\sigma^{-1}(b) \in F_1$ d'aquí $\tau(\sigma^{-1}(b)) = \sigma^{-1}(b)$ per $\tau \in H_1$ on $(\sigma\tau\sigma^{-1})(b) = b$ per la definició (i la bijecció demostrada de (i)) obtenim que $\sigma\tau\sigma^{-1} \in H_2$ per tant $\sigma H_1\sigma^{-1} \subseteq H_2$, i l'altra inclusió surt fent un argument anàleg amb $b \in F^{H_1}$ enlloc de F^{H_2} i $\tau \in H_2$ enlloc de H_1(exercici) per obtenir $\sigma^{-1}H_2\sigma \subseteq H_1$ d'on $H_2 \subseteq \sigma H_1\sigma^{-1}$.
Anem ara a demostrar la implicació que $H_1 = \tau H_2\tau^{-1}$ per cert τ (tenim $\tau^{-1}H_1\tau = H_2$) s'obté llavors $\tau^{-1}(F^{H_1}) = F^{H_2}$, efectivament; si $a \in F_1$ i $\beta \in H_1$ tenim:

$$\tau^{-1}\beta\tau(\tau^{-1}a) = \tau^{-1}a$$

com tots els elements de H_2 són de la forma $\tau^{-1}\beta\tau$ obtenim que $\tau^{-1}a \in F_2$ d'on $\tau^{-1}(F_1) \subseteq F_2$, l'altra inclusió es fa semblantment canviant els papers de F_1 i H_1 per F_2 i H_2 (exercici).

Anem a demostrar la part final referent a subgrups normals.
Si ara F^{H_1}/K normal, tenim $\sigma(F^{H_1}) = F^{H_1}$ per tot $\sigma \in Gal(F/K)$ (useu proposició 3.3.7) per tant obtenim del que just hem demostrat ara fa un moment que $\sigma H_1\sigma^{-1} = H_1$ per tot $\sigma \in Gal(F/K)$ per tant $H_1 \trianglelefteq Gal(F/K)$.

Suposem ara $H_1 \trianglelefteq Gal(F/K)$, tenim $\sigma(F_1) = F_1$ per tot $\sigma \in Gal(F/K)$ altre cop per la caracterització de la proposició 3.3.7 obtenim F_1/K és normal.

Falta demostrar per completar la demostració del teorema que donat $H = Gal(F/F^H)$ (la igualtat és d'Artin) i suposem $H \trianglelefteq Gal(F/K)$, hem vist F^H/K és Galois, ens falta demostrar:

$$Gal(F^H/K) \cong Gal(F/K)/H.$$

Per fer-ho definim

$$f : Gal(F/K) \to Gal(F^H/K)$$

$$\sigma \mapsto \sigma_{|F^H}$$

(està ben definida perquè F^H/K normal i per tant la restricció en F^H dona automorfisme pel resultat 3.3.7). És epimorfisme de grups ja que tot morfisme $\tau \in Gal(F^H/K)$ puja a F ja que F és cos descomposició de cert polinomi $\ell(x)$ sobre F^H (que podem pensar sobre $K[x]$ ja que F/K normal) i F també és cos de descomposició sobre F^H del polinomi $\underline{\tau}(\ell(x))$ (que és igual a $\ell(x)$ si $\ell(x) \in K[x]$, $\tau_{|K} = id$) i per tant puja a $Gal(F/K)$ useu lemma 3.2.6. Clarament $\gamma \in Ker(f)$ γ fixa cada element de F^H per tant $\gamma \in Gal(F/F^H) = H$ (d'on $Ker(f) \leq H$) i és clar que $H \leq Ker(f)$, per tant pel teorema d'isomorfisme per a grups obtenim el resultat. □

Exemple 4.2.2. *Considereu l'extensió $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$. Demostreu que és de Galois, doneu tots els cossos intermedis (reticle de cossos) i tots els subgrups de grups de Galois.*

Per veure que és Galois, es suficient veure que és normal ja que estem en característica zero, i per tant veure que és cos de descomposició d'algun polinomi sobre el cos base, en el nostre cas sobre $\mathbb{Q}$. Observem que tenim la següent torre de cossos:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$$

i $[\mathbb{Q}(\sqrt[4]{2} : \mathbb{Q}] = grau(Irr(\sqrt[4]{2}, \mathbb{Q})[x]) = grau(x^4 - 2) = 4$ *(irreductible per Eisenstein). Fixem-nos les arrels de* $x^4 - 2$ *en* $\mathbb{C}$ *són* $\pm\sqrt[4]{2}$ *i* $\pm i\sqrt[4]{2}$ *per tant el cos de descomposició* $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$*, i tenim que és Galois l'extensió, com* $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ *obtenim* $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = grau(Irr(i, \mathbb{Q}(\sqrt[4]{2}))[x]) = grau(x^2 + 1) = 2$ *i per tant* $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 4$*. Sabem que* $|Aut_{\mathbb{Q}}(\mathbb{Q}(sqrt[4]2, i))| = |Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 8$ *de ser Galois, anem a calcular aquest grup de 8 elements.*

Observació 4.2.3. Per a una extensió simple algebraica $K(\alpha)/K$ **recordeu que per a calcular** $\sigma \in Aut_K(K(\alpha))$**, anomenant** $p(x) = Irr(\alpha)[x]$**, és suficient dir a on va** $\sigma(\alpha)$**. I aquest** $\sigma(\alpha)$ **ha d'esser una arrel de** $p(x)$ **en** $K(\alpha)$**.**

Per a una extensió que no està expressada com extensió simple però que és algebraica i finita com per exemple $K(\alpha, \beta)$ **recordem com es calcula el grup automorfismes** $Aut_K(K(\alpha, \beta))$**. Considerem la torre de cossos:**

$$K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$$

on té grau

$$[K(\alpha, \beta) : K] = grau(Irr(\alpha, K)[x]) \cdot grau(Irr(\beta, K(\alpha))[x]),$$

anomenem $p(x) = Irr(\alpha, K)[x]$ **i** $q(x) = Irr(\beta, K(\alpha))[x]$**. Llavors** $\sigma \in Aut_K(K(\alpha, \beta))$ **ve determinat de dir quan val en** $\sigma(\alpha)$ **(que ha d'esser una arrel de** $p(x)$ **en** $K(\alpha, \beta)$**) i en** $\sigma(\beta)$ **(que ha d'esser una arrel de** $q(x)$ **en** $K(\alpha, \beta)$ *de la manera com hem construït la torre de cossos, fixeu-vos que* $q(x)$ *no és* $Irr(\beta, K)[x]$*!!!).*

Les arrels de $Irr(\alpha, \mathbb{Q})[x] = x^4 - 2$ *en* $\mathbb{Q}(\sqrt[4]{2}, i)$ *són* $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$*; les arrels de* $Irr(\beta, \mathbb{Q}(\alpha))[x] = x^2 + 1$ *en* $\mathbb{Q}(\sqrt[4]{2}, i)$*, amb arrels* $i, -i$*.*
per tant $\sigma \in Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ *tenim 8 morfismes:*

$$\sigma_1 = id,$$

$$\sigma_2(\sqrt[4]{2}) = i\sqrt[4]{2},\ \sigma_2(i) = i;$$

$$\sigma_3(\sqrt[4]{2}) = -\sqrt[4]{2},\ \sigma_3(i) = i;$$

$$\sigma_4(\sqrt[4]{2}) = -i\sqrt[4]{2},\ \sigma_4(i) = i;$$

$$\sigma_5(\sqrt[4]{2}) = \sqrt[4]{2},\ \sigma_5(i) = -i;$$

$$\sigma_6(\sqrt[4]{2}) = i\sqrt[4]{2},\ \sigma_6(i) = -i;$$

$$\sigma_7(\sqrt[4]{2}) = -\sqrt[4]{2},\ \sigma_7(i) = -i;$$

$$\sigma_8(\sqrt[4]{2}) = -i\sqrt[4]{2},\ \sigma_8(i) = -i.$$

No obstant fixem-nos per saber quin grup és, és més fàcil pensar el grup dins un grup permutacions S_n*. Per això és més útil pensar-ho com que és Galois és el particular el cos de descomposició d'un polinomi i per tant observem (recordem) el següent:*

Observació 4.2.4. Sigui F/K Galois finita, per tant F és cos de descomposició d'un polinomi $p(x)$ amb arrels diferents $\alpha_1, \ldots, \alpha_n$. Tenim que $F = K(\alpha_1, \ldots, \alpha_n)$, i $\sigma \in Gal(F/K)$ queda determinat en conèixer $\sigma(\alpha_i)$ per $i = 1, \ldots, n$. Com un automorfisme que deixa fix K porte les arrels α_i del polinomi $p(x) \in K[x]$ a arrels de $p(x)$, obtenim que un automorfisme dóna una permutació de les arrels del polinomi $p(x)$, d'aquí s'obté que tenim una injecció de grups

$$g : Gal(F/K) \hookrightarrow S_n$$

pensant S_n com les permutacions del conjunt de les n arrels de $p(x)$ $\{\alpha_1, \ldots, \alpha_n\}$.

Tornem al nostre exemple. L'anterior fet ens permet pensar el grup $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ com un subgrup de S_4 ja que $\mathbb{Q}(\sqrt[4]{2}, i)$ és cos descomposició pel polinomi $x^4 - 2$, tenim que té arrels: $\Sigma := \{\alpha_1 := \sqrt[4]{2}, \alpha_2 := -\sqrt[4]{2}, \alpha_3 := i\sqrt[4]{2}, \alpha_4 := -i\sqrt[4]{2}\}$ amb aquest ordre d'elecció de les arrels. Anem a descriure el monomorfisme g de grups en aquest exemple:

$$g : Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \hookrightarrow S_4$$

$$g(\sigma_1) = id \mapsto id$$

$$g(\sigma_2) = (1, 3, 2, 4)$$

$$g(\sigma_3) = (1, 2)(3, 4)$$

$$g(\sigma_4) = (1, 4, 2, 3)$$

$$g(\sigma_5) = (3, 4)$$

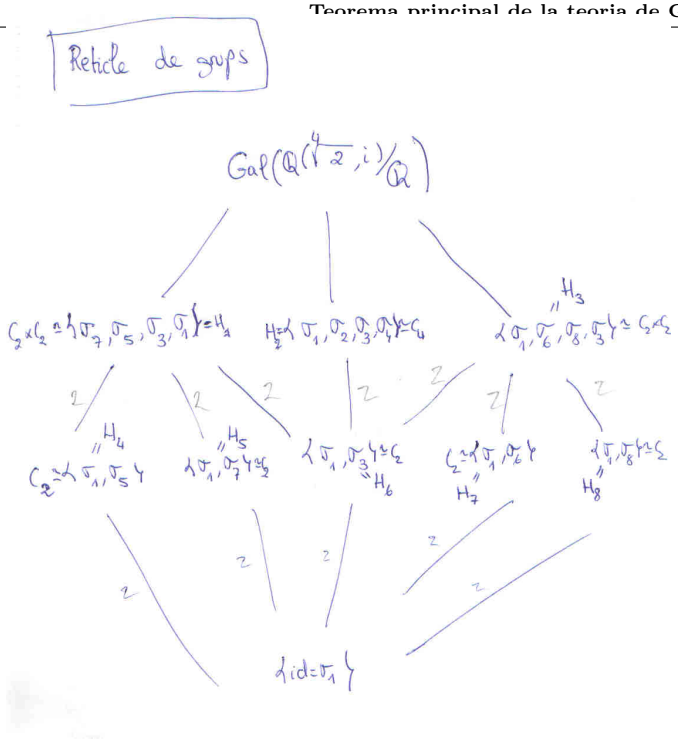
$$g(\sigma_6) = (1, 3)(2, 4)$$

$$g(\sigma_7) = (1, 2)$$

$$g(\sigma_8) = (1, 4)(2, 3)$$

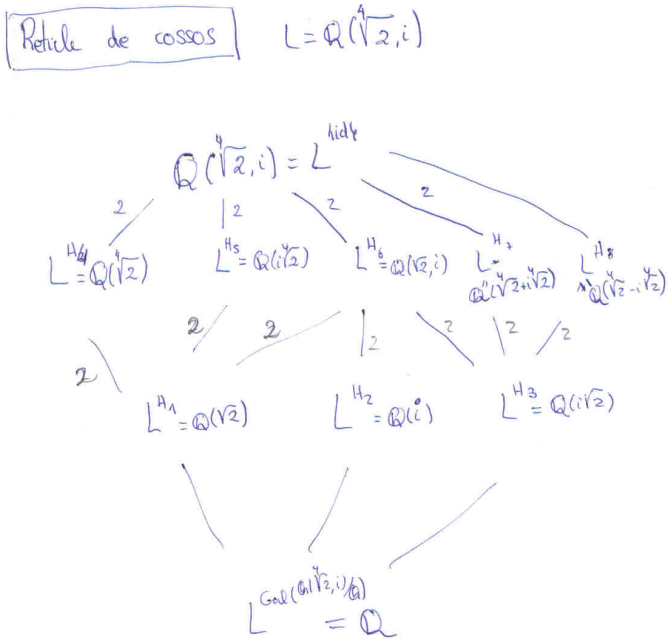
és un grup no abelià de vuit elements. Dins S_4 és més simple fer el reticle de grups:

Reticle de subgrups per $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$:



Observeu fàcilment que els subgrups H_1, H_2 i H_3 (seguim la notació del reticle dibuixat!) són normals sobre $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ ja que són d'índex 2 i sabem que tot subgrup d'index 2 és normal (veieu appèndix C).

Usant ara la correspondència bijectiva de Galois tenim un reticle de cossos entre $\mathbb{Q}$ i $\mathbb{Q}(\sqrt[4]{2})$ següent:



Fixeu-vos que les extensions $L^{H_1}/\mathbb{Q}$, $L^{H_2}/\mathbb{Q}$, $L^{H_3}/\mathbb{Q}$ i $L^{H_6}/\mathbb{Q}$ són Galois ja que $H_i \trianglelefteq Gal(L/\mathbb{Q})$ per $i = 1, 2, 3, 6$, a més fixeu-vos que els graus corresponen als índexs de grups (veieu els colors en les rames dels reticles!). (Usualment és més fàcil mirant els cossos intermedis quins són Galois sobre $\mathbb{Q}$: fixeu-vos que H_4 i H_5 són conjugats ja que el morfisme σ del grup de Galois que envia $\sqrt[4]{2}$ a $i\sqrt[4]{2}$ fa $\sigma(F^{H_4}) = F^{H_5}$ i per tant no +s normal (useu la segona part del teorema fonamental de Galois), un altre cas es H_7 i H_8, fixeu-vos que la conjugació complexa $\iota \in Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ fa que $\iota(L^{H_7}) = L^{H_8}$ i per tant no són ext. normals sobre $\mathbb{Q}$, i H_7 i H_8 no són subgrups normals.

Anem ara a explicitar com hem calculat els cossos intermedis anteriors. Fem-ho amb detall per un cos intermedi, per exemple per calcular $L^{H_7} = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$ on $H_7 = \{id = \sigma_1, \sigma_6\}$.
Una $\mathbb{Q}$-base per $L/\mathbb{Q}$ és: $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{2^3}, i, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{2^3}\}$ (mireu la demostració de $[L : K] = [L : M][M : K]$ per a trobar base pel cas no simple), sigui $\ell \in L$ volem trobar els elements fix pel subgrup $H_7 = \{id, \sigma_6\}$, és a dir cal resoldre:

$$id(\ell) = \ell,\ \sigma_6(\ell) = \ell.$$

La primera no ens diu res però si la segona, fixem-nos que podem escriurem

$$\ell = q_1 1 + q_2\sqrt[4]{2} + q_3\sqrt{2} + q_4\sqrt[4]{2^3} + q_5 i + q_6 i\sqrt[4]{2} + q_7 i\sqrt{2} + q_8 i\sqrt[4]{2^3} \in L$$

amb $q_i \in \mathbb{Q}$ i anem a imposar que $\sigma_6(\ell) = \ell$ en aquesta base del $\mathbb{Q}$-espai vectorial L:

$$\sigma_6(\ell) = q_1 1 + q_2\sigma_6(\sqrt[4]{2}) + q_3\sigma_6(\sqrt{2}) + q_4\sigma_6(\sqrt[4]{2^3}) + q_5\sigma_6(i) + q_6\sigma_6(i\sqrt[4]{2}) + q_7\sigma_6(i\sqrt{2}) + q_8\sigma_6(i\sqrt[4]{2^3}) =$$

$$= q_1 1 + q_2 i\sqrt[4]{2} + q_3(-(\sqrt{2})) + q_4(-i\sqrt[4]{2^3}) + q_5(-i) + q_6\sqrt[4]{2} + q_7(i\sqrt{2}) + q_8(-\sqrt[4]{2^3})$$

igualant amb ℓ obtenim el sistema lineal homogeni següent:

$$\begin{cases} q_1 = q_1 \\ q_2 = q_6 \\ q_3 = -q_3 \\ q_4 = -q_8 \\ q_5 = -q_5 \\ q_7 = q_7 \end{cases}$$

d'aquí obtenim $q_3 = q_5 = 0$ i $q_2 = q_6$ i $q_4 = -q_8$ i q_7, q_1 lliures (tenim 4 graus llibertat, és clar com $\mathbb{Q}$-espai vectorial el cos té dimensió 4 sobre $\mathbb{Q}$!!!) fixem-nos doncs que hem obtingut:

$$L^{H_7} = \{q_1 1 + q_2(\sqrt[4]{2} + i\sqrt[4]{2} + q_4(\sqrt[4]{2^3} - i\sqrt[4]{2^3}) + q_7 i\sqrt{2} | q_1, q_2, q_4, q_7 \in \mathbb{Q}\}$$

fixem-nos que $L^{H_7} = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$ ja que $(\sqrt[4]{2} + i\sqrt[4]{2})^2 = 2i\sqrt{2}$ i $(\sqrt[4]{2} + i\sqrt[4]{2})^3 = -2(\sqrt[4]{2^3} - i\sqrt[4]{2^3})$ i per tant una $\mathbb{Q}$-base de L^{H_7} és $1, \sqrt[4]{2} + i\sqrt[4]{2}, (\sqrt[4]{2} + i\sqrt[4]{2})^2, (\sqrt[4]{2} + i\sqrt[4]{2})^3$ que és la usual per l'extensió simple $\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})/\mathbb{Q}$.

Corol·lari 4.2.5. *Sigui F/K extensió finita i separable. Llavors F és una extensió simple sobre K, és a dir $F = K(b)$ per cert $b \in F$ algebraic i separable sobre K.*

Demostració. Com F/K és finita tenim $F = K(\beta_1, \ldots, \beta_\ell)$ amb β_i algebraics sobre K. Considerem $f(x) = \prod_{i=1}^{\ell} Irr(\beta_i, K)[x] \in K[x]$, i F' un cos de descomposició de $f(x)$ sobre K que contingui F (això últim és factible ja que $\beta_i \in F$ i pensem F' un cos de descomposició de $f(x)$ sobre F que coincideix amb F' anterior), per tant F'/K normal. Com β_i's separables sobre K $f(x)$ no té arrels múltiples i per tant totes les arrels γ_j de f en F' són separables i com $F' = K(\gamma_j's)$ obtenim F'/K és una extensió separable, d'aquí F'/K és una extensió de Galois finita. Com el reticle de grups per a $Gal(F'/K)$ és finit (és a dir hi ha un nombre finit de subgrups), els cossos intermedis entre F' i K n'hi ha també un nombre finit (usem la correspondència bijectiva de Galois del teorema fonamental), en particular entre F i K (F és un cos intermedi de K i F) hi ha un nombre finit de cossos, llavors usant el teorema d'Steinitz 2.2.3 obtenim que F/K és una extensió simple. □

Exemple 4.2.6. *Hem considerat abans l'extensió $\mathbb{Q}(\sqrt[4]{2}, i)$ ara hem demostrat tot just a sobre que és una extensió simple sobre $\mathbb{Q}$ (ja que és finita i separable sobre $\mathbb{Q}$). Per tant podem usar la demostració del teorema d'Steinitz per a trobar un element primitiu, és a dir un element δ on*

$$\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\delta).$$

Anem-ho a fer: recordeu que la demostració del teorema d'Steinitz 2.2.3 ens suggereix que aquest element és de la forma $\sqrt[4]{2}+ai$ amb $a \in \mathbb{Q}$. Pensem ara del fet que l'extensió $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ és simple pel resultat anterior, un element primitiu δ ha de complir que $Irr(\delta, \mathbb{Q})[x]$ ha de tenir grau 8 (ja que: $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$) i sabem que els automorfismes han de portar una arrel de $Irr(\delta, \mathbb{Q})[x]$ a una arrel d'aquest mateix polinomi (ja que $\underline{\sigma_i}(Irr(\delta, \mathbb{Q})[x]) = \underline{id}(Irr(\delta, \mathbb{Q})[x])$ i per tant $Irr(\delta, \mathbb{Q})[\sigma_i(\delta)] = \sigma_i(Irr(\delta, \mathbb{Q})[\delta]) = \sigma_i(0) = 0$) i a $\mathbb{Q}(\sqrt[4]{2}, i)$ hi han de ser les 8 arrels diferents d'aquest polinomi (per esser normal i del fet que l'anterior polinomi irreductible sobre $\mathbb{Q}$ té una arrel en aquell cos normal sobre $\mathbb{Q}$), amb aquesta idea fem el següent:
veiem que $\sigma_i(\sqrt[4]{2} + i)$ va a 8 valors diferents de $\mathbb{Q}(\sqrt[4]{2}, i)$ i per tant podem triar $\delta = \sqrt[4]{2} + i$ com a element primitiu per l'extensió, anem-ho a comprovar. (Penseu que una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[4]{2}, i)$ és $1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{8}$ (recordem la demostració de $[L : K] = [L : M][M : K]$ de com obteníem una K-base per L, nosaltres tenim $L = \mathbb{Q}(\sqrt[4]{2}, i)$ $M = \mathbb{Q}(\sqrt[4]{2})$ i $K = \mathbb{Q}$ on una $\mathbb{Q}$-base per M és $1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}$, i una M-base per L és $1, i$)

$$\sigma_1(\sqrt[4]{2} + i) = \sqrt[4]{2} + i,$$
$$\sigma_2(\sqrt[4]{2} + i) = i\sqrt[4]{2} + i,$$
$$\sigma_3(\sqrt[4]{2} + i) = -\sqrt[4]{2} + i,$$
$$\sigma_4(\sqrt[4]{2} + i) = -i\sqrt[4]{2} + i,$$
$$\sigma_5(\sqrt[4]{2} + i) = \sqrt[4]{2} - i,$$
$$\sigma_6(\sqrt[4]{2} + i) = i\sqrt[4]{2} - i,$$
$$\sigma_7(\sqrt[4]{2} + i) = -\sqrt[4]{2} - i,$$
$$\sigma_8(\sqrt[4]{2} + i) = -i\sqrt[4]{2} - i,$$

que tots són diferents les imatges (useu per exemple que donen vectors diferents de L respecte la $\mathbb{Q}$-base anterior). Per tant,

$$\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} + i).$$

També obtenim

$$Irr(\sqrt[4]{2} + i, \mathbb{Q})[x] = \prod_{j=1}^{8}(x - \sigma_j(\sqrt[4]{2} + i)) = x^8 + 4x^6 + 2x^4 + 28x^2 + 1.$$

Observació 4.2.7. *Donada F/K algebraica i separable, tenim $F = K(\alpha)$ pel corol.lari 4.2.5. Per a trobar aquest α, fixem-nos que l'anterior idea via usant automorfismes del exemple anterior dóna una metodologia quan L/K Galois; no obstant quan no és F/K Galois també ens la dona, efectivament: la diferència serà tal sols que cal considerar una extensió finita L' de F on L'/K és Galois i pensar que les arrels del irreductible de l'element primitiu α per a F que busquem estaran en L' (no han de ser necessàreament a F) i ara segurament alguns automorfismes de $Gal(L'/K)$ portarà α al mateix α però hem de buscar que surtin exactament $[F : K]$ elements diferents per $\sigma(\alpha) \in L'$ on σ recorre $Gal(L'/K)$, aquestes $[F : K]$-arrels diferents seran les arrels de $Irr(\alpha, K)[x]$ en $L'[x]$ pel candidat a element primitiu α per a la extensió F sobre K, $F = K(\alpha)$.*

Exemple 4.2.8. *Sigui $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ una extensió finita entre cossos finits ($q = p^s$ on p primer, s natural positiu), és normal per ser cos descomposició i és separable (exercici), per tant és Galois, observeu que $Gal(\mathbb{F}_{q^\ell}/\mathbb{F}_q) =< Frob^s >$ cíclic d'ordre exactament ℓ on $Frob : K \to K$ és $Frob(x) = x^p$ (exercici). Estudieu els cossos intermedis que hi ha entre $\mathbb{F}_{q^\ell}$ i $\mathbb{F}_q$.*

Finalitzem el capítol amb una definició:

Definició 4.2.9. *Donat $p(x) \in K[x]$ sense arrels múltiples en els seus factors irreductibles en $K[x]$, diem $Gal(p(x)/K)$ al grup de Galois $Gal(E/K)$ on E és el cos de descomposició de $p(x)$ sobre K. (Recordeu que $Gal(p(x)/K)$ actua permutant les arrels del polinomi $p(x)$ i conèixer aquesta permutació determina aquest element unívocament dins del grup de Galois).*

Observació 4.2.10. *Maple sap calcular donat un $p(x) \in \mathbb{Q}[x]$ de grau no massa gran el grup $Gal(p(x)/\mathbb{Q})$, escriviu:*
> galois(polinomi);

Observació 4.2.11 (*)**.** *Si L/K Galois (no finita) vol dir normal i separable on normal (es pot demostrar que és equivalent a la condició de ser cos de descomposició d'una col.lecció de polinomis sobre el cos base K). Ara $Gal(L/K)$ no és un grup finit, la correspondència bijectiva de Galois (o l'apartat primer del teorema fonamental de la teoria de Galois) s'escriu en el cas no finit afirmant que hi ha una bijecció Φ de la forma següent:*

$$\Phi : \{subcossos\ entre\ L\ i\ K\} \to \{subgrups\ tancats\ de\ Gal(L/K)\},$$

$$F \mapsto Gal(L/F)$$

$$L^H \hookleftarrow H$$

I què són els subgrups tancats de $Gal(L/K)$? Amb quina topología en $Gal(L/K)$?

És la topología de Krull pel grup $Gal(L/K)$ definida de la forma següent: per a cada $\sigma \in Gal(L/K)$ definim el conjunt

$$\mathcal{B}_\sigma := \{\sigma Gal(L/K')|\ K'/K \text{ extensió Galois } finita\} \subseteq Gal(L/K)$$

i fixem-nos que $\sigma \in \mathcal{B}_\sigma$. Es demostra que $\mathcal{B}_\sigma$ és una base d'entorns de $\sigma \in Gal(L/K)$ $\forall \sigma \in Gal(L/K)$ i recordem que $U \subseteq Gal(L/K)$ és obert si $\forall \sigma \in U$ $\exists v \in \mathcal{B}_\sigma$ on $v \subset U$. Això defineix la topología de Krull en $Gal(L/K)$ que el converteix amb un grup topològic (grup topològic:=és un espai topològic que tés a més estructura de grup on les operacions de grup són continues). Els entorns bàsics $\sigma \cdot Gal(L/K')$ són oberts i tancats.

Capítol 5

Teoria de Galois d'equacions

El "aim" d'aquest capítol és demostrar que no tenim fórmula genèrica per polinomis de grau ≥ 5.

Per aquest capítol considerem que treballem amb cossos de característica zero.

Val a dir que per restriccions d'horari, (teoria de Galois té 30 hores en el grau) aquest capítol donarà les idees principals per a demostrar el teorema de resolubilitat §5.1 i la impossibilitat de la fórmula per radicals per a polinomis de grau ≥ 5 §5.2, i no crec que doni temps a fer a classe ni la demostració del teorema ni la caracterització de les extensions radicals que continguin arrels n-èssimes de 1(§5.3, i §5.4 respectivament).

Comentar-vos que les extensions radicals no tan sols tenen aplicació al resultat de Galois de resolubilitat d'equacions; Kummer va treballar amb elles tot introduint-hi arrels de l'unitat per atacar el teorema de Fermat i va demostrar el teorema de Fermat pel cas dels primers regulars. Aquestes extensions de Kummer també són importants per obtenir el teorema de Fermat per tot primer p, resultat d'Andrew Wiles. Més encara, els últims ICM, Kazuya Kato és sempre un expositor principal i sempre és referent a treballs per a atacar un dels problemes de l'Institut Clay: la conjectura de Birch-Swinnerton-Dyer i més en general la conjectura del nombre de Tamagawa (o de Bloch-Kato). Aquestes conjectures passen per a estudiar objectes a través d'aquestes extensions de Kummer, més concretament extensions ciclotòmiques. En la conjectura del nombre de Tamagawa també surt la funció zeta de Riemann i el seu valor en els enters, per exemple quan val

$$\zeta(2k+1) = \sum_{n=1}^{\infty} \frac{1}{n^{2k+1}}$$

amb $k \geq 1$, més fàcil: quins $\zeta(2k+1)$ són nombres irracionals? quants d'aquests són transcendents sobre $\mathbb{Q}$?. El cas $\zeta(2k)$ ho treballareu a anàlisi complexa, el nombre π amb potències seves ens soluciona les anteriors preguntes! per $\zeta(2k)$. Què succeeix per $\zeta(2k+1)$?

5.1 Resolubilitat per radicals. Grups resolubles

Recordem que a partir d'ara tots els cossos tenen característica zero.

Comencem a formalitzar que voldria dir que poguessim escriure les arrels d'un polinomi amb arrels n-èssimes, sumes, productes, e iteracions d'aquestes operacions.

Definició 5.1.1. *Una extensió F/K s'anomena radical si existeixen $\alpha \in F$ i $m \in \mathbb{N}_{\geq 1}$ on $F = K(\alpha)$ i $\alpha^m \in K$. (Quan $\alpha^m = 1$ parlarem d'extensió ciclotòmica).*

Definició 5.1.2. *Una torre finita d'extensions radicals és una cadena finita de cossos*

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\ell$$

on K_i/K_{i-1} és una extensió radical per $i = 1, \ldots, \ell$.

Definició 5.1.3. *Sigui K cos (sempre estem en car =0) i $p(x) \in K[x] \setminus K$. Diem que l'equació*

$$p(x) = 0$$

és resoluble per radicals sobre K si existeix una torre finita d'extensions radicals:

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\ell$$

on K_ℓ conté un cos de descomposició de $p(x)$ sobre K.

Observació 5.1.4. *Aquesta definició s'adiu a la problemàtica de buscar una fórmula mitjançant l'iteració d'arrels i sumes i productes, tal com s'obtenien les fórmules de grau 2, 3 i 4 (alguna d'elles vistes en el curs).*

Recordeu que tot i tenir una expressió en radicals per les arrels d'un polinomi a vegades tampoc és fàcil obtenir igualtats, ja que l'expressió en radicals no és única tot i que existeixi, i a més ja sabeu també que $\sqrt[n]{*}$ és una funció multivaluada. No obstant aquí no ens plantegem aquests problemes de les expressions radicals, tan sols si donat un polinomi és resoluble per radicals, on una resposta afirmativa vol dir (segons la definició anterior, penseu-ho una mica) que les arrels s'expressen en forma de radicals: és dir com iteració d'arrels n-èssimes, sumes i productes.

Exemple 5.1.5.

1. *L'extensió $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ és radical ja que $(e^{2\pi i/n})^n \in \mathbb{Q}$.*
2. *El polinomi $x^3 + 4 \in \mathbb{Q}[x]$ és resoluble per radicals, efectivament tenim la torre finita d'extensions radicals:*

$$\mathbb{Q} \subseteq \mathbb{Q}(-\sqrt[3]{4}) \subseteq \mathbb{Q}(-\sqrt[3]{4}, e^{2\pi i/3})$$

on $\mathbb{Q}(-\sqrt[3]{4}, e^{2\pi i/3})$ és un cos de descomposició de $p(x)$ sobre $\mathbb{Q}$.

Anem a explotar una mica la propietat de ser $p(x)$ resoluble per radicals, tenim en aquesta situació una torre finita d'extensions radicals $K \subseteq \ldots \subseteq K_\ell$. Si K_ℓ/K fos Galois, llavors d'aquesta torre de cossos obtindríem una cadena de subgrups de $Gal(K_\ell/K)$ usant el teorema fonamental de la teoria de Galois, fem la següent definició.

Definició 5.1.6. *Un grup finit G s'anomena resoluble si existeix una cadena de subgrups*

$$G = H_0 \geq H_1 \geq \ldots \geq H_\ell = \{id\}$$

complint que $H_i \trianglerighteq H_{i+1}$ per $i = 0, \ldots, \ell - 1$ i H_i/H_{i+1} és un grup abelià.

Observació 5.1.7. *Si G resoluble es pot refinar la cadena de forma que H_i/H_{i+1} és un grup cíclic.*

Un dels resultats principals de la teoria d'equacions de Galois és el següent:

Teorema 5.1.8 (de resolubilitat)**.** *[Galois i altres] Sigui K un cos de característica zero, i $p(x) \in K[x] - K$. Llavors:*
$p(x)$ és resoluble per radicals si i només si $Gal(p(x)/K)$ és un grup resoluble.

Exemple 5.1.9. *1. Tot grup abelià és resoluble,*

2. *S_3 és resoluble:*
$$\{id\} \leq A_3 \leq S_3$$

3. *S_4 és resoluble via la cadena:*
$$\{id\} \leq \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq A_4 \leq S_4$$

4. *S_n o A_n no és resoluble per a $n \geq 5$ (Galois)*

5. *Teorema Feit-Thomson: tot grup finit d'ordre senar és resoluble.(Molt difícil la demostració en aquest nivell).*

El fet que el polinomi de grau 3 i 4 tingui fórmula per radicals de les seves arrels prové del fet que $Gal(p(x)/K) \hookrightarrow S_3$ ó S_4 respectivament (recordeu que donat $p(x)$ un polinomi de grau n en $K[x]$ es té $Gal(p(x)/K) \hookrightarrow S_n$ ja que un automorfisme queda determinat en saber a on va cadascuna de les arrels del polinomi i les arrels del polinomi $p(x)$ han d'anar a arrels del mateix polinomi per un element de $Gal(p(x)/K)$) i per tant és un grup resoluble (recordeu que un subgrup d'un grup resoluble és resoluble, veieu appèndix C).

Anem ara a demostrar la implicació fàcil de l'anterior teorema 5.1.8, demostrar que $p(x)$ resoluble llavors el grup $Gal(p(x)/K)$ és un grup resoluble.

Considerem $p(x)$ és resoluble per radicals, i tenim una cadena finita d'extensions radicals:

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\ell \tag{5.1}$$

on un cos de descomposició de $p(x)$ és dins de K_ℓ i escrivim $K_i = K_{i-1}(a_i)$ on $a_i^{n_i} \in K_{i-1}$ per a cert $n_i \in \mathbb{N}_{\geq 1}$.

Fem la següent hipòtesi en el proper paràgraf per a aportar certa reflexió: Suposem per un moment i tan sols en aquest paràgraf que K_ℓ/K és Galois; llavors per la correspondència de Galois (el teorema fonamental de la teoria de Galois) de la cadena (5.1) obtenim la cadena de grups

$$Gal(K_\ell/K) \geq Gal(K_\ell/K_1) \geq \ldots \geq Gal(K_\ell/K_\ell) = \{id\} \tag{5.2}$$

però fixeu-vos que per donar una cadena semblant a la definició de grup resoluble necessitem la condició de normalitat. Si volem la condició de normalitat en la

cadena (5.2) necessitem $Gal(K_\ell/K_i) \trianglelefteq Gal(K_\ell/K_{i-1})$; i pel teorema fonamental de la teoria de Galois cal que K_i/K_{i-1} sigui una extensió de Galois i recordem que $K_i = K_{i-1}(a_i)$ amb $a_i^{n_i} \in K_{i-1}$, per tant necessitem que hi hagi les arrels de $x^{n_i} - 1$ en K_i per tal que en K_i hi hagi totes les arrels de $x^{n-i} - a_i^{n_i}$.

Els següents lemes volen caracteritzar les extensions radicals M/K on K hi té arrels de polinomis $x^N - 1$ i un lema tècnic de grups resolubles.

Definició 5.1.10. *Donat F un cos, una arrel n-èssima de la unitat és una arrel del polinomi $x^n - 1$ en F. Una arrel n-èssima de la unitat ξ s'anomena primitiva si el grup $< \xi >= \{\xi^j | j \in \mathbb{N}\}$ té ordre exactament n, en cas d'existir, anotarem també per una arrel n-èssima per ξ_n si volem fer explicit el seu ordre.*

Lema 5.1.11. *Considerem $\tilde{E}$ un cos de descomposició de $x^n - 1$ sobre K. Llavors $\tilde{E}$ té una arrel n-èssima primitiva de l'unitat ξ, la qual és element primitiu de l'extensió,(per tant $\tilde{E} = K(\xi)$) i $Gal(\tilde{E}/K) \cong H$ amb $H \leq (\mathbb{Z}/(n))^*$ on recordeu que $(\mathbb{Z}/(n))^*$ són els elements invertibles de l'anell $\mathbb{Z}/(n)$ amb el producte.*

Demostració. Considerem $\alpha_1, \ldots, \alpha_n = 1$ les n arrels de $x^n - 1$ en $\tilde{E}$ (totes diferents per separabilitat), $\tilde{E} = K(\alpha_1, \ldots, \alpha_n)$; és clar que $H := \{\alpha_1, \ldots, \alpha_n\} \leq \tilde{E}^*$ és un subgrup finit dels elements invertibles de $\tilde{E}$. Demostrem que H és cíclic d'ordre n i per tant un generador d'aquest grup és un arrel n-èssima primitiva de 1 i un element primitiu δ per $\tilde{E}$ (és dir $\tilde{E} = K(\delta)$. Anem doncs a demostrar-ho: si H no fos cíclic llavors per la classificació de grups abelians finits podem escriure $H \cong C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}$ amb $n = n_1 n_2 \cdot \ldots \cdot n_r$ i $n_1 | n_2 | \ldots | n_r$ per tant $mcm(n_1, n_2, \ldots, n_r) = n_r < n$ si $r > 1$, però llavors $\alpha_i^{n_r} = 1$ per tot i per tant el polinomi $x^{n_r} - 1$ té n arrels però té grau $n_r < n$ Impossible!! Per tant $r = 1$ i el grup H és cíclic.

Per acabar ens falta demostrar que $\sigma \in Gal(\tilde{E}/K)$ és un subgrup de $(\mathbb{Z}/(n))^*$. Escrivim $\tilde{E} = K(\xi)$

Sigui $\sigma \in Gal(K(\xi)/K)$, $\sigma(\xi)$ ha d'esser una arrel de $x^n - 1$ en $K(\xi)$ per tant de la forma ξ^r on podem pensar $r \in (\mathbb{Z}/(n))$. Com $Gal(K(\xi)/K)$ és un grup existeix $\tau = \sigma^{-1}$ i $\tau(\xi) = \xi^s$ com $\sigma\tau = id$ obtenim que $rs \equiv 1 (mod\ n)$ per tant $r, s \in (\mathbb{Z}/(n))^*$, definim doncs l'aplicació:

$$\psi : Gal(K(\xi_n)/K) \to (\mathbb{Z}/(n))^*$$

$$\sigma \mapsto r$$

és clar que és injectiva (penseu-ho un moment). Veiem que ψ és morfisme de grups:
per un costat tenim, $(\sigma_1\sigma_2)(\xi) = \xi^{\psi(\sigma_1\sigma_2)}$, per l'altre $(\sigma_1\sigma_2)(\xi) = \sigma_1(\xi^{\psi(\sigma_2)}) = \sigma_1(\xi)^{\psi(\sigma_2)} = (\xi^{\psi(\sigma_1)})^{\psi(\sigma_2)} = \xi^{\psi(\sigma_1)\psi(\sigma_2)}$, provant que via ψ $Gal(K(\xi)/K)$ el podem pensar com un subgrup de $(\mathbb{Z}/(n))^*$. □

Lema 5.1.12. *Suposem K conté una arrel n-èssima primitiva de 1, que anomenem ξ. Sigui $a \in K$, i α arrel del polinomi de $K[x]$ $x^n - a$ en un cos de descomposició de $x^n - a$ sobre K, llavors $K(\alpha)/K$ és una extensió de Galois amb grup de Galois un grup cíclic de grau d on $d|n$ i $\alpha^d \in K$.*

Demostració. Si $a = 0$ és clar, pensem $a \neq 0$, tenim $\xi^i\alpha$ amb $i = 1, \ldots, n$ són també arrels de $x^n - a$; com $\xi \in K$ per hipòtesi tenim $K(\alpha)$ és cos de descomposició pel polinomi $x^n - a$ i per tant Galois. Definim la següent aplicació:

$$h : Gal(K(\alpha)/K) \to \{w \in K | w^n = 1\}$$

$$\sigma \mapsto \frac{\sigma(\alpha)}{\alpha},$$

observem que

$$h(\sigma \circ \tau) = \frac{\sigma \circ \tau(\alpha)}{\alpha} = \frac{\sigma(\tau(\alpha))}{\sigma(\alpha)} \frac{\sigma(\alpha)}{\alpha} = \sigma(\frac{\tau(\alpha)}{\alpha}) \frac{\sigma(\alpha)}{\alpha} = \frac{\tau(\alpha)}{\alpha} \frac{\sigma(\alpha)}{\alpha} = h(\tau)h(\sigma)$$

on en la penúltima igualtat usem $\tau(\alpha)/\alpha \in K$; fixeu-vos que l'anterior igualtat demostra que h és morfisme de grups i clarament h és injectiva (σ queda determinada per la imatge de α ja que estem extensió simple amb element primitiu α), per tant

$$Gal(K(\alpha)/K) \cong \textit{subgrup de } C_n \cong C_d$$

on és un grup cíclic amb $d|n$. Sigui θ un generador de $Gal(K(\alpha)/K)$ tenim llavors:

$$(\frac{\theta(\alpha)}{\alpha})^d = 1$$

per tant $\theta(\alpha^d) = \alpha^d$ i també $\theta^j(\alpha^d) = \alpha^d$ per tant $\alpha^d \in K$ (useu $K(\alpha)^{Gal(K(\alpha)/K)} = K$), finalitzant la prova. □

Lema 5.1.13. *Sigui G un grup finit i que té una cadena de subgrups*

$$G = H_0 \geq H_1 \geq \ldots \geq H_n$$

amb $H_i \trianglerighteq H_{i+1}$ per $i = 0, \ldots, n-1$ amb H_i/H_{i+1} grup abelià, amb H_n no necessàreament el subgrup identitat. Suposem que tenim $H_n \leq H \leq G$ on $H \trianglelefteq G$. Llavors G/H és resoluble.

Demostració. Com $H \trianglelefteq G$ tenim la cadena de subgrups:

$$G = H_0H \geq H_1H \geq \ldots \geq H_nH$$

amb $H_iH \trianglerighteq H_{i+1}H$ per $i = 0, \ldots, n-1$. Com tenim que $H_n \leq H$ obtenim $H_nH = H$. Llavors podem formar la cadena:

$$\frac{G}{H} = \frac{H_0H}{H} \geq \frac{H_1H}{H} \geq \ldots \geq \frac{H_nH}{H} = 1$$

amb $\frac{H_iH}{H} \trianglerighteq \frac{H_{i+1}H}{H}$. Estem doncs a punt de justificar que $\frac{G}{H}$ és resoluble, ens falta veure que els quocients son grups abelians i usarem els teoremes de Noether que vau veure al taller teòric de grups, el primer taller. Efectivament, observem primer que

$$\frac{\frac{H_iH}{H}}{\frac{H_{i+1}H}{H}} \cong \frac{H_iH}{H_{i+1}H}$$

per $i = 0, \ldots, n-1$, i tenim

$$\frac{H_iH}{H_{i+1}H} \cong \frac{H_i}{H_i \cap H_{i+1}H} \cong \frac{\frac{H_i}{H_{i+1}}}{\frac{H_i \cap H_{i+1}H}{H_{i+1}}}$$

finalment com $\frac{H_i}{H_{i+1}}$ és abelià també ho és $\frac{H_iH}{H_{i+1}H}$, demostrant finalment que G/H és resoluble. □

Finalment ja estem en condicions de demostrar una implicació del teorema 5.1.8,

Demostració. [⇒ del teorema 5.1.8]
Sigui doncs una torre d'extensions radicals

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\ell$$

on K_ℓ conté E un cos de descomposició del polinomi $p(x)$ sobre K. Escrivim $K_i = K_{i-1}(a_i)$ amb $a_i^{n_i} \in K_{i-1}$ per $i = 1, \ldots, \ell$ (del fet que K_i/K_{i-1} és una extensió radical). Denotem per N al natural $n_1 \cdot \ldots \cdot n_\ell$ i considerem un cos de descomposicó del polinomi $x^N - 1$ sobre K_ℓ, podem escriure aquest cos usant el lemma 5.1.11 via $K_\ell(\xi_N)$ on ξ_N és una arrel N-èssima primitiva de 1. Considerem llavors la torre d'extensions

$$K \subseteq K(\xi_N) \subseteq K_1(\xi_N) \subseteq \ldots \subseteq K_\ell(\xi_N)$$

que fixem-nos que és una extensió de torres radical i observem ara que $K_i(\xi_N)/K_{i-1}(\xi_N)$ és una extensió radical que és de Galois amb grup de Galois un grup cíclic ja que $K_i(\xi_N)$ és cos de descomposició del polinomi $x^{n_i} - a_i^{n_i}$ sobre $K_{i-1}(\xi_N)$ (observeu ξ_N^{N/n_i} és una arrel n_i-èssima primitiva de 1) pel Lemma 5.1.12. Observem també que $K(\xi_N)/K$ és una extensió radical de Galois amb grup de Galois abelià pel 5.1.11. [1]

Considerem ara F un cos de descomposició per $x^N - 1$ i $Irr(a_i^{n_i}, K)[x]$. Fixem-nos que $K_\ell(\xi_N) \subseteq F$, F/K és Galois i tenim una cadena de grups:

$$Gal(F/K) \trianglerighteq Gal(F/K(\xi_N)) \trianglerighteq Gal(F/K_1(\xi_N)) \trianglerighteq \ldots \trianglerighteq Gal(F/K_{\ell-1}(\xi_N)) \trianglerighteq Gal(F/K_\ell(\xi_N));$$

on $G_a \trianglerighteq G_b$ en la cadena indica que G_b és un subgrup normal de G_a i aquesta normalitat s'obté del fet que $K_i(\xi_N)/K_{i-1}(\xi_N)$ i $K(\xi_N)/K$ són extensions de Galois i de la correspondència bijectiva de Galois obtenim aquesta normalitat. Observem que

$$Gal(F/K_{i-1}(\xi_N))/Gal(F/K_i(\xi_N)) \cong Gal(K_i(\xi_N)/K_{i-1}(\xi_N))$$

és abelià per $i = 1, \ldots, \ell$ where $K_0 = K$, i tenim també

$$Gal(F/K_0)/Gal(F/K_0(\xi_N)) \cong Gal(K(\xi_N)/K)$$

abelià, per tant apliquem ara el Lemma 5.1.13 amb $G = Gal(F/K)$ i $H = Gal(F/E)$ on recordem que E és el cos de descomposició de $p(x)$ que està dins K_ℓ, tenim $H \trianglelefteq G$ del fet que E/K és Galois (useu teorema principal de la teoria de Galois) i pel teorema principal de la teoria de Galois tenim $G/H \cong Gal(E/K)$, ara aplicant el Lemma 5.1.13 obtenim que $Gal(E/K)$ és un grup resoluble.

□

[1] Fixeu-vos que si $K_\ell(\xi_N)/K$ fos Galois tindríem quasi bé, usant la correspondència de Galois amb la torre radical contruïda entre K i $K_\ell(\xi_N)$, una cadena de subgrups que compleixen la condició de grup resoluble per al grup $G = Gal(K_\ell(\xi_N)/K)$; usant llavors Lema 5.1.13 obtindríem el resultat del teorema. Lamentablement no ha de perquè complir-se que $K_\ell(\xi_N)/K$ sigui Galois, per resoldre això seguiu la lectura de la demostració.

5.2 No hi fórmula per radicals per a polinomis de grau ≥ 5

Anem ara obtenir que com a conseqüència del teorema 5.1.8 podem demostrar la impossibilitat de fórmules per polinomis de grau ≥ 5.

Recordem primer els següents resultats de grups resolubles que es treballen a la classe de seminaris, veieu també appèndic C d'aquests apunts:

Exemple 5.2.1. *1. Tot grup abelià és resoluble,*

2. Tot subgrup d'un grup resoluble és resoluble.

3. S_3 és resoluble:

$$\{id\} \leq A_3 \leq S_3$$

4. S_4 és resoluble via la cadena:

$$\{id\} \leq \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq A_4 \leq S_4$$

5. S_n o A_n no és resoluble per a $n \geq 5$ (Galois)

6. Teorema Feit-Thomson: tot grup finit d'ordre senar és resoluble.(Molt difícil la demostració en aquest nivell).

El fet que el polinomi de grau 3 i 4 tingui fórmula per radicals de les seves arrels prové del fet que $Gal(p(x)/K) \hookrightarrow S_3$ o S_4 respectivament (recordeu que donat $p(x)$ un polinomi de grau n en $K[x]$ es té $Gal(p(x)/K) \hookrightarrow S_n$ ja que un automorfisme queda determinat en saber a on va cadascuna de les arrels del polinomi i les arrels del polinomi $p(x)$ han d'anar a arrels del mateix polinomi per un element de $Gal(p(x)/K)$) i per tant és un grup resoluble.

Teorema 5.2.2. *Un polinomi genèric de grau n sobre K que escrivim per $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K(a_0, \ldots, a_{n-1})[x]$ (pensant a_i com a variables) té grup de Galois S_n, és a dir $Gal(p(x)/K(a_0, \ldots, a_{n-1})) \cong S_n$.*

Abans de demostrar-ho anem a fer el següent resultat preparatori:

Teorema 5.2.3. *Considerem $K(X_1, \ldots, X_n)$ el cos de fraccions dels polinomis en n-variables a coeficients en K $K[X_1, \ldots, X_n]$. Fem actuar $\sigma \in S_n$ permutant les variables, és a dir $\sigma(X_i) := X_{\sigma(i)}$. Llavors:*

$$K(X_1, \ldots, X_n)^{S_n} = K(s_1, \ldots, s_n),$$

on s_i són els polinomis simètrics elementals en les variables X_i, recordeu per exemple $s_1 = X_1 + X_2 + \ldots + X_n$, $s_2 = \sum_{i<j} X_i X_j$, ...
En particular l'extensió $K(X_1, \ldots, X_n)/K(s_1, \ldots, s_n)$ és Galois amb grup de Galois isomorf a S_n.

Demostració. [teorema 5.2.3] Com $\sigma(s_i) = s_i^\sigma = s_i$ per $\sigma \in S_n$, és clar que

$$K(s_1, \ldots, s_n) \subseteq (K(X_1, \ldots, X_n))^{S_n} \subseteq K(X_1, \ldots, X_n).$$

Fixeu-vos que

$$p(x) = (x-X_1)(x-X_2)\cdot\ldots\cdot(x-X_n) = x^n - s_1x^{n-1} + \ldots + (-1)^n s_n \in K(s_1,\ldots,s_n)[x]$$

obtenim que $K(X_1,\ldots,X_n)$ és un cos de descomposició de $p(x)$ sobre $K(s_1,\ldots,s_n)$ i com té grau n obtenim (de la proposició 3.2.5):

$$[K(X_1,\ldots,X_n) : K(s_1,\ldots,s_n)] \leq n!,$$

per altra banda obtenim que $S_n \leq Gal(K(X_1,\ldots,X_n)/K(X_1,\ldots,X_n)^{S_n})$ per tant $[K(X_1,\ldots,X_n) : K(X_1,\ldots,X_n)^{S_n}] \geq n!$, obtenint $[K(X_1,\ldots,X_n)^{S_n} : K(s_1,\ldots,s_n)] = 1$.

Fixem-nos com $K(X_1,\ldots,X_n)/K(X_1,\ldots,X_n)^{S_n}$ és Galois pel teorema d'Artin amb grup de Galois S_n i observem que a més hem demostrat en la prova que $K(X_1,\ldots,X_n)$ és el cos de descomposició del polinomi $x^n - s_1x^{n-1} + \ldots + (-1)^n s_n$ sobre $K(s_1,\ldots,s_n)$. □

Demostració. [teorema 5.2.2] Sigui ara $f(x)$ un polinomi genèric de grau n que escrivim ara per,

$$f(x) = x^n - t_1x^{n-1} + \ldots + (-1)^n t_n \in K[t_1,\ldots,t_n][x]$$

on pensem t_i variables indeterminades (on $a_{n-i} = (-1)^i t_i$ i $K[t_1,\ldots,t_n] = K[a_1,\ldots,a_n]$), és a dir $K[t_1,\ldots,t_n]$ és l'anell de polinomis en n-variables a coeficients en K. Considerem el morfisme d'anells (K-lineal):

$$\phi : K[t_1,\ldots,t_n] \to K[s_1,\ldots,s_n]$$

$$t_i \mapsto s_i$$

clarament és epi, i veiem que és injectiu: efectivament si $P(s_1,\ldots,s_n) \in K[s_1,\ldots,s_n]$ vam demostrar al principi de curs que P era el polinomi zero, demostrant la injectivitat (Corol.lari 1.2.9). Per tant ϕ dona a un isomorfisme dels cossos $K(t_1,\ldots,t_n)$ a $K(s_1,\ldots,s_n)$ enviant $f(x)$ al polinomi $\underline{\phi}(f(x)) = x^n - s_1x^{n-1} + \ldots + (-1)^n s_n \in K(s_1,\ldots,s_n)[x]$. Per tant un cos de descomposició de $f(x)$ sobre $K(t_1,\ldots,t_n)$ és isomorf a un cos de descomposició de $\underline{\phi}(f(x))$ sobre $K(s_1,\ldots,s_n)$ i els grups de Galois coincideixen per tant té grup de Galois S_n. □

Corol·lari 5.2.4. *No hi ha una fórmula en radicals genèrica per les arrels d'un polinomi genèric arbitrari de grau n si $n \geq 5$.*

Demostració. Com $Gal(p(x)/K(a_1,\ldots,a_n)) \cong S_n$ del teorema 5.2.2 obtenim que no és resoluble per radicals per a $n \geq 5$ del fet que S_n no és un grup resoluble i usant ara el teorema de Galois 5.1.8. □

Observació 5.2.5. *Un voldria una afirmació de l'anterior resultat sobre $\mathbb{Q}$ en el sentit següent: que donat un polinomi qualsevol de grau n sobre $\mathbb{Q}$ no tenim fórmula per radicals en general, és a dir per un polinomi de grau n sobre $\mathbb{Q}$ hi ha infinits casos en que té grup de Galois S_n. Aquest fet és veritat com va demostrar Hilbert i que va donar peu a unes línies de recerca respecte al problema que plantejo tot seguit en aquesta observació.*

Un dels problemes més interessants en teoria de Galois és el següent (problema invers de la teoria de Galois): fixem un cos K i un grup finit G, existeix

una extensió de Galois d'aquest cos K amb grup de Galois G? Fixeu-vos que si el cos base no està fixa't la resposta és fàcil!(useu el teorema de Cayley per pensar aquest grup dins cert S_n i useu llavors el teorema d'Artin per a obtenir que $F(X_1,\ldots,X_n)^G$ és Galois sobre $F(X_1,\ldots,X_n)$ amb grup de Galois G on $F(X_1,\ldots,X_n)$ és el cos de fraccions de l'anell en n-variables $F[X_1,\ldots,X_n]$).

Acabem aquesta secció amb un resultat més numèric, donant explícitament una familia no finita de polinomis en que no podem expressar les seves arrels per radicals, Corol.lari 5.2.8!!

Lema 5.2.6. *Sigui p un primer i $H \leq S_p$ un subgrup que conté una transposició i un cicle d'ordre p. Llavors $H = S_p$.*

Demostració. Sense pèrdua de generalitat podem pensar (i,j) i $(1,2,\ldots,p)$ són elements de S_p. Si $p = 2$ és clar el resultat. Suposem $p > 2$. Observeu $(1,2,\ldots,p)^{j-i} = (i,j,a_3,\ldots,a_n)$, per tant podem suposar $(1,2)\ (1,2,\ldots,p) \in H$. De la igualtat:

$$(1,2,\ldots,p)^{\ell}(1,2)(1,2,\ldots,p)^{-\ell} = (1+\ell, 2+\ell)$$

per $\ell = 1,\ldots,p-2$; per tant $(1,2),(2,3),\ldots,(p-1,p) \in H$ i tenim:

$$(i,i+1)(1,i)(1,i+1) = (1,i+1)$$

per i entre 2 i $p-1$, començant per $(1,2)$ anem obtenint que $(1,2),(1,3),\ldots,(1,p) \in H$, i finalment observem

$$(m,n) = (1,n)(1,m)(1,n) \in H$$

per tant com tota transposició de S_p és en H i com tot element de S_p és producte de transposicions obtenim que $H = S_p$. □

Corol·lari 5.2.7. *Sigui $p(x) \in \mathbb{Q}[x]$ un polinomi irreductible de grau p primer amb exactament dos arrels complexes i no reals llavors $Gal(p(x)/\mathbb{Q}) \cong S_p$.*

Demostració. Sigui K el cos de descomposició de $p(x)$ sobre $\mathbb{Q}$ pensat dins els nombres complexos. Sabem $Rep : Gal(K/\mathbb{Q}) = Gal(p(x)/\mathbb{Q}) \hookrightarrow S_p$ pel fet de ser cos descomposició de $p(x) \in \mathbb{Q}[x]$ de grau p. Siguin $\{\alpha_1,\alpha_2,\alpha_3,\ldots,\alpha_p\}$ les p arrels diferents en $\mathbb{C}$ on $\alpha_1,\alpha_2 \in \mathbb{C}\setminus\mathbb{R}$. Considerem la conjugació complexa τ, s'obté $\tau(\alpha_1) = \alpha_2$, $\tau(\alpha_2) = \alpha_1$ i $\tau(\alpha_i) = \alpha_i$ per $i \geq 3$, via l'ordre triat de les arrels tenim $Rep(\tau) = (1,2)$ una transposició. Ara com $p|[K:\mathbb{Q}]$ ja que $p(x)$ irreductible, obtenim $p||Gal(K/\mathbb{Q})|$ doncs pel teorema de Cauchy de grups obtenim que $Gal(K/\mathbb{Q})$ té un element d'ordre exactament p, és a dir un cicle ordre p. Ara aplicant lema 5.2.6 obtenim $Gal(K/\mathbb{Q}) \cong S_p$. □

Corol·lari 5.2.8. *$Gal(x^5 - pnx + p/\mathbb{Q}) \cong S_5$ amb p primer i $n \geq 2$ natural. Per tant les arrels d'aquest polinomi $x^5 - npx + p$ no s'expressen per radicals.*

Demostració. Per Eisenstein $\ell(x) := x^5 - pnx + p$ és irreductible. Anem a demostrar que té exactament tres arrels reals. Calculem $\ell'(x) = 5x^4 - pn$ que té dues arrels reals diferents $\pm\sqrt[4]{\frac{np}{5}}$, per tant com a molt $\ell(x)$ té 3 arrels reals. Fixem-nos $\lim_{n\to+\infty}\ell(x) = +\infty$, $\ell(1) = 1 - np + p \leq 1 - p < 0$, $\ell(-1) = -1 + pn + p \geq p - 1 > 0$, $\lim_{n\to-\infty}\ell(x) = -\infty$, obtenim que $\ell(x)$ té una arrel < -1, una altra entre -1 i 1, i la tercera > 1, aplicant el resultat anterior obtenim que el seu grup de Galois és S_5 i usant el teorema de Galois de resolubiltat obtenim que el polinomi no és resoluble per radicals. □

5.3 Extensions ciclotòmiques. Extensions cícliques.

Per intentar demostrar la implicació contrària del teorema 5.1.8, cal caracteritzar les extensions amb grup abelià cíclic i si estan relacionades amb extensions radicals. Això és així si el cos base té les arrels de l'unitat, anem doncs a aprofundir amb les extensions obtingudes d'adjuntar-hi arrels unitats en aquesta secció.

Definició 5.3.1. *Sigui K un cos. Una extensió ciclotòmica de K és una extensió algebraica de la forma $K(\xi_n)$ on ξ_n és una arrel n-èssima primitiva de 1. Fixem-nos que $K(\xi_n)/K$ és Galois ja que és cos de descomposició del polinomi $x^n - 1 \in K[x]$ i és separable sota la hipòtesi del capítol de considerar K de caracteristica zero en aquest capítol.*

Definició 5.3.2. *Una extensió finita L/K radical amb $L = K(a)$ amb $a^n \in K$ s'anomena de Kummer si K conté una arrel n-èssima primitiva de 1.*

Hem vist com a conseqüència del Lemma 5.1.11 el següent resultat

Corol·lari 5.3.3. *$Gal(x^n - 1/K)$ és isomorf a un subgrup de $(\mathbb{Z}/(n))^*$.*

Introduïm ara els conceptes necessaris per a podem preparar la demostració de la implicació contrària del teorema 5.1.8, per això cal caracteritzar extensions finites galois amb grup de galois cíclic.

Definició 5.3.4. *Diem que una extensió finita F/K és cíclica si és una extensió de Galois i $Gal(F/K)$ és un grup cíclic.*

Proposició 5.3.5. *Sigui F/K una extensió de grau n on K conté una arrel n-èssima primitiva de 1. Suposem que F/K és una extensió cíclica. Llavors $\exists \alpha \in F$ on $F = K(\alpha)$ i α és arrel d'un polinomi de la forma $x^n - a$ amb $a \in K$ (és a dir F/K és una extensió radical).*

Abans d'iniciar la demostració, necessitem un lema referent a condicions lineals d'automorfismes

Lema 5.3.6 (de Dedekind)**.** *Sigui K i F dos cossos. Siguin $\sigma_i : K \hookrightarrow F$, morfismes de cossos diferents per $i = 1, \ldots, n$. Llavors $\sigma_1, \ldots, \sigma_n$ són linealment independents sobre F.*

Demostració. [Lema de Dedekind] Demostrem-ho per inducció respecte n. Per a $n = 1$, $\sigma_1 \neq 1$ perquè $\sigma_1(1) = 1 \neq 0$ obtenint el resultat.

Suposem $n > 1$ i que $\sigma_1, \ldots, \sigma_{n-1}$ són linealment independents sobre F. Considerem $a_i \in F$ satisfent:

$$a_1\sigma_1 + \ldots + a_n\sigma_n = 0. \tag{5.3}$$

S'obté doncs que $\forall s \in K$ tenim la igualtat:

$$a_1\sigma_1(s) + \ldots + a_n\sigma_n(s) = 0 \tag{5.4}$$

escrivim $s = xy$ fixant $y \in K$ i $\forall x \in K$ obtenim

$$a_1\sigma_1(xy) + \ldots + a_n\sigma_n(xy) = a_1\sigma_1(x)\sigma_1(y) + \ldots + a_n\sigma_n(x)\sigma_n(y) = 0 \tag{5.5}$$

si multipliquem per $\sigma_n(y)$ l'equació (5.4) fent $s = x$ obtenim que per tot $x \in K$:

$$a_1\sigma_1(x)\sigma_n(y) + \ldots + a_n\sigma_n(x)\sigma_n(y) = 0, \tag{5.6}$$

restant ara equació (5.5) amb equació (5.6) obtenim (que podem eliminar σ_n, efedctivament):

$$a_1(\sigma_1(y) - \sigma_n(y))\sigma_1(x) + \ldots a_{n-1}(\sigma_{n-1}(y) - \sigma_n(y))\sigma_{n-1}(x) = 0$$

per tot $x \in K$ per tant obtenim:

$$a_1(\sigma_1(y) - \sigma_n(y))\sigma_1 + \ldots a_{n-1}(\sigma_{n-1}(y) - \sigma_n(y))\sigma_{n-1} = 0$$

on $a_i(\sigma_i(y) - \sigma_n(y)) \in F$ i com $\sigma_1, \ldots, \sigma_{n-1}$ són F-linealment independents obtenim

$$a_i(\sigma_i(y) - \sigma_n(y)) = 0, \tag{5.7}$$

per a $i = 1, \ldots, n-1$ a més això és cert per a qualsevol $y \in K$ fixat. Usem ara que $\sigma_i \neq \sigma_n$ per $i = 1, \ldots, n-1$ per a concloure que $a_i = 0$ per a $i = 1, \ldots, n-1$ de l'equació (5.7). Per tant del sistema (5.3) obtenim $a_n\sigma_n = 0$ i com $\sigma_n \neq 0$ obtenim finalment que $a_n = 0$, és a dir obtenint que $\sigma_1, \ldots, \sigma_n$ són F-linealment independents. □

Demostració. [Proposició 5.3.5] Suposem F/K extensió cíclica de grau n, i escrivim $Gal(F/K) = \{id, \sigma, \ldots, \sigma^{n-1}\}$. Considereu $\alpha : F \to F$, amb $\alpha = id + \xi_n\sigma + \ldots + \xi_n^{n-1}\sigma^{n-1}$, pel Lema de Dedekind 5.3.6 $\exists\lambda \in F$ on $\alpha(\lambda) \neq 0$ (ja que $id, \sigma, \ldots, \sigma^{n-1}$ són F-linealment independents i per tant aquesta combinació lineal és no zero) , escrivim

$$\beta = \alpha(\lambda) = \lambda + \xi_n\sigma(\lambda) + \ldots + \xi_n^{n-1}\sigma(\lambda)^{n-1};$$

d'aquesta expressió obtenim que

$$\sigma(\beta) = \xi_n^{-1}\beta; \quad \sigma^k(\beta) = \xi_n^{-k}\beta$$

a més sabem que σ ha de permutar les arrels de $g(x) = Irr(\beta, K)[x]$ ja que $\beta \in F$ i F/K Galois, per tant $\xi_n^{-k}\beta$ són arrels també de $g(x)$, i per tant $[K(\beta) : K] = grau(g(x)) \geq n$ i com $[F : K] = n$ i tenim l'inclusió de cossos $K \subseteq K(\beta) \subseteq F$ obtenim que $F = K(\beta)$ i $\sigma(\beta^n) = (\xi_n^{-1}\beta)^n = \beta^n$ i per tant β^n és fix per tot $Gal(F/K)$ i per tant $\beta^n \in K$. □

Anem per acabar aquesta secció a estudiar en detall $Gal(x^n - 1/\mathbb{Q})$ i d'aquest càlcul podem caracteritzar el polígons regulars que són construïbles amb regle i compàs com una primera aplicació al que és l'estudi d'extensions ciclotòmiques sobre $\mathbb{Q}$.

5.3.1 Extensions ciclotòmiques sobre $\mathbb{Q}$

Sigui ξ_n una arrel n-èssima primitiva de 1 (la pensem dins $\overline{\mathbb{Q}}$, o dins $\mathbb{C}$ en aquesta subsecció), fixem-nos que ξ_n^k també és una arrel n-èssima primitiva de 1 si es compleix $mcd(k, n) = 1$.

Definició 5.3.7. *El n-èssim polinomi ciclotomic es defineix per*

$$\Phi_n(x) := \prod_{k\in(\mathbb{Z}/(n))^*}(x-\xi_n^k) = \prod_{1\leq d\leq n,(d,n)=1}(x-\xi_n^d).$$

Lema 5.3.8. *El polinomi $\Phi_n(x)$ és en $\mathbb{Q}[x]$.*

Demostració. Fixem-nos que $\forall\sigma\in Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ tenim $\underline{\sigma}(\Phi_n(x))=\Phi_n(x)$ per tant σ fixa els coeficients del polinomi $\Phi_n(x)$, i per tant aquests són en $\mathbb{Q}=\mathbb{Q}(\xi_n)^{Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})}$. □

Lema 5.3.9. *Per a $n\geq 1$ tenim la igualtat en $\mathbb{Q}[x]$*

$$x^n-1=\prod_{d|n}\Phi_d(x).$$

Demostració. És clar que $\Phi_d(x)|x^n-1$ per a $d|n$, i com $\Phi_d(x)$ té arrels diferents a $\Phi_{d'}(x)$ si $d\neq d'$ obtenim que

$$\prod_{d|n}\Phi_d(x)|x^n-1$$

però tota arrel de x^n-1 es troba en algún $\Phi_d(x)$ per $d|n$, per tant $\prod_{d|n}\Phi_d(x)$ i x^n-1 tenen el mateix grau i el coeficient de x^n és 1 en ambdos polinomis. □

Corol·lari 5.3.10. *Tenim que $\Phi_n(x)\in\mathbb{Z}[x]$.*

Demostració. Demostrem-ho per inducció en n, per $n=1$ tenim $\Phi_1(x)=x-1\in\mathbb{Z}[x]$. Suposem cert per $1\leq n\leq k$ i veiem que $\Phi_j(x)\in\mathbb{Z}[x]$ per $1\leq j\leq k+1$. Tenim que

$$\Phi_{k+1}(x)\ell(x)=x^{k+1}-1$$

on $x^{k+1}-1,\ell(x)=\prod_{d|k+1,d\neq k+1}\Phi_d(x)$ són en $\mathbb{Z}[x]$ i ambdos mònics, en aquesta situació i com $\mathbb{Z}$ és un domini amb $Q(\mathbb{Z})=\mathbb{Q}$ és fàcil demostrar (exercici al lector) que $\Phi_{k+1}(x)\in\mathbb{Z}[x]$ obtenint el resultat. □

Teorema 5.3.11. *El polinomi $\Phi_n(x)$ és un polinomi irreductible sobre $\mathbb{Q}[x]$, per tant $\Phi_n(x)=Irr(\xi_n,\mathbb{Q})[x]$, $[\mathbb{Q}(\xi_n):\mathbb{Q}]=grau(\Phi_n(x))=|(\mathbb{Z}/(n))^*|$.*

Demostració. L'únic que cal demostrar és que $\Phi_n(x)$ és irreductible en $\mathbb{Q}[x]$. Suposem que fos reductible, pel Lemma de Gauss podem escriure

$$\Phi_n(x)=f_1(x)f_2(x)$$

amb $f_i(x)\in\mathbb{Z}[x]$ mònics. Podem suposar sense pèrdua de generalitat que $\xi_n\in f_1(x)$, amb f_1 irreductible i demostrarem que ξ_n^k és arrel de $f_1(x)$ per tot k amb $mcd(k,n)=1$ i per tant $f_2=1$ obtenint que ha de ser irreductible.

Escrivim $k=pm$ amb p un nombre primer $p\nmid n$, es suficient demostrar que sempre que tenim ξ arrel de $f_1(x)$ llavors ξ^p és també arrel de $f_1(x)$ per a obtenir el resultat. Anem a demostrar això últim. Suposem que ξ^p fos arrel de $f_2(x)$. Escrivim $g(x)=f_2(x^p)$ on $g(\xi)=0$. Com f_1 irreductible tenim que $f_1(x)=Irr(\xi,\mathbb{Q})[x]$ per tant tenim que

$$g(x)=f_1(x)h(x)$$

amb algun $h(x) \in \mathbb{Z}[x]$ ja que $g, f_1 \in \mathbb{Z}[x]$ mònics. Fem ara reducció a $\mathbb{Z}/(p)[x]$ on escriurem una barra damunt a la reducció en $\mathbb{Z}/(p)[x]$. Tenim llavors

$$\overline{g}(x) = \overline{f}_2(x^p) = (\overline{f}_2(x))^p$$

per tant obtenim $\overline{f}_1(x)\overline{h}(x) = \overline{f}_2(x)^p$, prenem $\overline{q}(x)$ factor irreductible de $\overline{f}_1(X)$ tenim que $\overline{q}(x)|\overline{f}_2(x)^p$ per tant $\overline{q}(x)|\overline{f}_2(x)$ de ser irreductible, i obtenim que $\overline{q}(x)$ és factor irreductible per a $\overline{f}_1(x)$ i $\overline{f}_2(x)$ on $\overline{q}(x)^2|\overline{\Phi}_n(x)$, però $\overline{\Phi}_n(x)$ no té arrels múltiples en un cos de descomposició sobre $\mathbb{Z}/(p)$ ja que $x^n - 1$ no en té ($p \nmid n$), per tant aquesta situació no es pot donar, obtenint així la irreductibilitat per $\Phi_n(x)$. □

Corol·lari 5.3.12. *Es té* $Gal(x^n - 1/\mathbb{Q}) \cong (\mathbb{Z}/(n))^*$.

Anem a fer una aplicació del teorema anterior, i del teorema principal a la teoria de Galois finita per a construccions amb regle i compàs.

Definició 5.3.13. *Es defineix la funció φ d'Euler a la funció definida per $\varphi(n) := |(\mathbb{Z}/(n))^*|$ per a $n \in \mathbb{N}_{\geq 1}$.*

Anem a llistar algunes propietats de la funció φ d'Euler.

Lema 5.3.14. *La funció φ d'Euler satisfà:*

1. *$\varphi(nm) = \varphi(n)\varphi(m)$ si $n, m \in \mathbb{N}_{\geq 1}$ amb $mcd(n, m) = 1$,*
2. *$\varphi(p^n) = p^n(1 - \frac{1}{p})$ per a p primer.*

Demostració. Exercici al lector. □

Fixeu-vos que l'anterior lema permet el càlcul de $\varphi(n)$ un cop tenim la factorització de n en nombres primers.

Definició 5.3.15. *Un nombre primer (de $\mathbb{Q}$) s'anomena de Fermat si és de la forma $2^m - 1$. Diem $\mathcal{C}$ al conjunt de primers de Fermat.*

Fixeu-vos els primers de Fermat p satisfant que $\varphi(p)$ és una potència de 2.

Teorema 5.3.16 (Gauss-Wantzel)**.** *El polígon regular de n costats és construïble amb regle i compàs si i només si $n = 2^m \prod_{p \in \mathcal{C}} p$ on p recorre un subconjunt finit dins els nombres primers de Fermat.*

Demostració. Fixeu-vos primer que per tal de construir el polígon n-costats és suficient demostrar que $cos(2\pi i/n)$ és un nombre construïble, que pel teorema 2.4.8 és equivalent que hi hagi una cadena de cossos reals amb

$$K_0 := \mathbb{Q} \subseteq K_1 \subseteq \ldots \subseteq K_\ell$$

amb $cos(2\pi i/n) \in K_\ell$ i $[K_i : K_{i-1}] \leq 2$ per $i = 1, \ldots, \ell$. Observem que tenir l'anterior cadena és equivalent (exercici al lector) a tenir una cadena de cossos

$$L_0 := \mathbb{Q} \subseteq L_1 \subseteq \ldots L_m = \mathbb{Q}(e^{2\pi i/n}) \tag{5.8}$$

amb $[L_i : L_{i-1}] \leq 2$ per $i = 1, \ldots, m$.

Per tant estudiem per a quins n l'extensió de Galois $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ té una cadena com l'anterior (5.8).

Pel corol.lari 2.4.9 s'ha de complir que $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}]$ ha de ser una potència de 2, per tant usant el teorema 5.3.11 s'ha de complir que $\varphi(n) = 2^{natural}$, i per les propietats de la φ d'Euler n ha de tenir la factorització en primers de la forma $2^m \prod_{p\in\mathcal{C}} p$ on p recorre un subconjunt finit dins els nombres primers de Fermat. Anem ara a demostrar que si n té aquesta factorització tenim la cadena (5.8) demostrant el teorema. Efectivament, usem ara el teorema principal de la teoria de Galois finita. Com $Gal(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q})$ és un grup abelià d'ordre una potència de 2 (recordeu que estem impossant que n és $2^m \prod_{p\in\mathcal{C}} p$) podem construir una cadena de subgrups de $Gal(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q})$ d'index 2,

$$H_0 := Gal(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \geq H_1 \geq H_2 \geq \ldots \geq H_k = \{id\}$$

amb index entre H_i i H_{i+1} exactament 2 per $i = 0, \ldots, k-1$, per tant per la correspondència bijectiva de la teoria de Galois finita obtenim una cadena

$$M_0 := \mathbb{Q} \subseteq M_1 \subseteq \ldots M_k = \mathbb{Q}(e^{2\pi i/n})$$

amb $[M_i : M_{i-1}] = 2$. □

5.4 Demostració teorema resolubilitat radicals

Recordem que en la §5.1 van enunciar el teorema de resolubilitat de radicals, teorema 5.1.8 i vam fer la demostració que si $p(x)$ resoluble per radicals sobre K llavors $Gal(p(x)/K)$ és resoluble per radicals, anem a demostrar ara la implicació que ens falta.

Lema 5.4.1 (d'irracionalitats naturals)**.** *Sigui L/K una extensió i $p(x)$ un polinomi separable sobre el cos K. Siguin F_1, F_2 cossos de descomposició de $p(x)$ sobre K i L respectivament. Llavors F_1/K i F_2/L són extensions de Galois i $Gal(F_2/L)$ és isomorf a un subgrup de $Gal(F_1/K)$*

Demostració. És clar que $p(x)$ és també separable sobre L. Escrivim $\alpha_1, \ldots, \alpha_n$ les arrels de $p(x)$ és un cos de descomposició de $p(x)$ sobre L, podem pensar $F_1 = K(\alpha_1, \ldots, \alpha_n)$ i $F_2 = L(\alpha_1, \ldots, \alpha_n)$ amb $F_1 \subseteq F_2$. Definim el morfisme de grups (exercici a comprovar que és morfisme de grups) que és ben definit ja que F_1/L és una extensió normal:

$$h : Gal(F_2/L) \to Gal(F_1/K)$$

$h(\sigma) := \sigma_{|_{F_1}}$ és a dir la restricció de σ en el cos F_1. Fixeu-vos que si $\sigma \in Ker(h)$ tenim llavors que $\sigma(\alpha_i) = \alpha_i$ per $i = 1, \ldots, n$ i per tant $\sigma = id$ demostrant que

$$Gal(F_2/L) \cong Im(f) \leq Gal(F_1/K).$$

□

Ara usant el lema anterior i la proposició 5.3.5 podem demostrar que si $Gal(p(x)/K)$ és un grup resoluble llavors $p(x)$ és resoluble per radicals:

Demostració. [de $\Leftarrow$ del Teorema 5.1.8] Escrivim $n = |Gal(p(x)/K)|$. Com $Gal(p(x)/K)$ és un grup resoluble i $Gal(p(x)/K(\xi_n))$ és isomorf a un subgrup de l'anterior (via el lema d'irracionalitats naturals) per tant tenim que

$Gal(p(x)/K(\xi_n))$ és un grup resoluble. Escrivim E un cos de descomposició de $p(x)$ sobre $K(\xi_n)$. Tenim llavors la cadena de subgrups:

$$\{id\} \leq H_\ell \leq \ldots \leq H_0 = Gal(E/K(\xi_n))$$

amb $H_i \trianglelefteq H_{i-1}$ on H_{i-1}/H_i és un grup cíclic per tot $i = 1, \ldots, \ell$. Pel teorema principal de la teoria de Galois finita obtenim una torre de cossos:

$$K_0 := K(\xi_n) = E^{H_0} \subseteq K_1 = E^{H_1} \subseteq \ldots \subseteq K_\ell = E$$

complint a més K_i/K_{i-1} Galois amb $Gal(K_i/K_{i-1}) \cong H_{i-1}/H_i$ un grup cíclic d'ordre n_i dividint l'ordre del grup $Gal(E/K(\xi_n))$ en particular dividint n ($Gal(E/K(\xi_n)$ és un subgrup del grup $Gal(E/K)$ que té ordre n). Ara com K_{i-1} conté ξ_n una arrel n-èssima primitiva de 1, per la proposició 5.3.5 obtenim que existeix $\alpha_i \in K_i$ on $K_i = K_{i-1}(\alpha_i)$ i $\alpha_i^{n_i} \in K_{i-1}$ per $i = 1, \ldots, \ell$ i per tant K_i/K_{i-1} és una extensió radical. Observem ara la torre de cossos:

$$K \subseteq K_0 \subseteq \ldots \subseteq K_\ell = E$$

i sigui E' un cos de descomposició de $p(x)$ sobre K, és clar que podem triar un E' dins de E i com $K \subseteq K_0$ és una extensió radical, obtenim que la torre

$$K \subseteq K_0 \subseteq \ldots \subseteq K_\ell = E$$

és una torre formada per extensions radicals i conté un cos de descomposició de $p(x)$ sobre K, demostrant que $p(x)$ és resoluble per radicals sobre K. □

Per acabar aquesta secció i el capítol, donem un exemple per a observar la importància de les arrels de la unitat per a poder obtenir una fórmula en radicals d'un polinomi $p(x)$ quan és resoluble, en particular observarem un polinomi concret i específic el qual és resoluble per radicals i per a tota torre de cossos radical per a $p(x)$ sobre K (on en aquest exemple correspon a $K = \mathbb{Q}$):

$$K \subseteq \ldots \subseteq K_\ell$$

satisfà que el cos de descomposició de $p(x)$ sobre K no és cap dels cossos d'aquesta torre (justificant la definició 5.1.3) i observarem la importància de les arrels de la unitat per a construir la torre i donar una fórmula per radicals de les arrels.

Anem primer a fer una mica de teoria general per a polinomis.
Sigui $f(x) \in K[x]$ un polinomi de grau $n \geq 1$ en $K[x]$ amb $mcd(f, f') = 1$ i siguin $\alpha_1, \ldots, \alpha_n$ arrels de f en un cos de descomposició L de f sobre K, (són diferents aquestes arrels). Escrivim

$$\delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \neq 0.$$

Considereu $\sigma \in Gal(L/K)$ via el monomorfisme de grups $Rep : Gal(L/K) \hookrightarrow S_n$ (pensem S_n com permutacions de les arrels $\{\alpha_1, \ldots, \alpha_n\}$) poden pensar σ com un element de S_n, per tant obtenim

$$\sigma(\delta) = \prod_{1 \leq i < j \leq n} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{1 \leq i < j \leq n} (\alpha_{Rep(\sigma)(i)} - \alpha_{Rep(\sigma)(j)}) = sign(Rep(\sigma))\delta$$

on *sgn* denota la funció signe en S_n que val 1 si σ és permutació parell (és a dir de A_n el grup alternat) o -1 si σ és senar, és a dir de $S_n - A_n$.

Definició 5.4.2. *Donat un polinomi $f(x)$ de grau n sobre K sense arrels repetides en un cos de descomposició, es defineix el discriminant de $f(x)$ al nombre*

$$\Delta := \delta^2$$

Fixeu-vos $\Delta \in K$, ja que $\forall \sigma \in Gal(p(x)/K) = Gal(L/K)$ tenim $\sigma(\Delta) = \sigma(\delta)^2 = sgn(Rep(\sigma))^2\Delta = \Delta$ i pel fet de que L/K és Galois, $\Delta \in L^{Gal(L/K)} = K$. Per tant el discriminant és un element de K no zero (de no tenir arrels repetides f). Obtenim que hem justificat el següent resultat:

Proposició 5.4.3. *Donat $f(x) \in K[x]$ un polinomi de grau n sense arrels repetides en un cos de descomposició de f sobre K. Llavors es tés:*

1. *si Δ té una arrel quadrada en K llavors $Rep(Gal(p(x)/K)) \leq A_n$ (podem pensar $Gal(p(x)/K)$ com a subgrup del grup alternat);*

2. *si Δ no té arrel quadrada en K llavors $Rep(Gal(p(x)/K)) \subsetneq A_n$.*

Observem tot seguit que podem calcular fàcilment el discriminant Δ d'un polinomi. Efectivament, observeu que

$$\delta = \begin{vmatrix} 1 & 1 & \dots & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \dots & \alpha_n \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \dots & \alpha_n^{n-1} \end{vmatrix},$$

i reescrivint l'anterior via $\delta = |A|$ amb A una matriu $n \times n$ a coeficients en L obtenim

$$\Delta = |A \cdot A^t| = \begin{vmatrix} n & \lambda_1 & \dots & \dots & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & \dots & \dots & \lambda_n \\ \vdots & \vdots & & & \vdots \\ \lambda_{n-1} & \lambda n & \dots & \dots & \lambda_{2n-2} \end{vmatrix}$$

on $\lambda_j = \alpha_1^j + \ldots + \alpha_n^j$ i fixem-nos que λ_j és un polinomi simètric respecte les arrels i per tant és pot calcular a partir dels coeficients del polinomi gràcies al teorema 1.2.7 i podem calcular algoritmicament Δ (mètode de Waring). Anem a explicitar alguns exemples de discriminants.

Exemple 5.4.4. *El discriminant per a*

1. *un polinomi $f(x) = x^2 + bx + c \in K[x]$ de grau 2 amb $b, c \in K$ s'obté $\Delta = b^2 - 4c$,*

2. *un polinomi $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ de grau 3 amb $a_0, a_1, a_2 \in K$ és*

$$\Delta = -4a_2^3a_0 + a_2^2a_1^2 + 18a_2a_1a_0 - 4a_1^3 - 27a_0^2.$$

Exemple 5.4.5. *Anem a explicitar un exemple concret d'un polinomi resoluble per radicals però que cap cadena de cossos radical conté el cos de descomposició.*

Prenem $\ell(x) = x^3 - 15x + 5 \in \mathbb{Q}[x]$ *irreductible en* $\mathbb{Q}[x]$ *pel criteri d'Eisenstein, a més és fàcil demostrar que les tres arrels de* $\ell(x)$ *són reals. Siguin* $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ *les tres arrels ara de* $\ell(x)$ *(pensem el cos de descomposició de* $\ell(x)$ *sobre* $\mathbb{Q}$ *dins* $\mathbb{C}$*). Sigui* $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ *cos descomposició* $\ell(x)$ *sobre* $\mathbb{Q}$*, tenim* $[L : \mathbb{Q}] = |Gal(L/\mathbb{Q})|$ *de ser Galois, i recordeu* $Rep(Gal(L/\mathbb{Q})) \leq S_3$ *(sempre* $[L : \mathbb{Q}] \leq 3!$ *perquè és cos descomposició per un polinomi de grau 3). Calculem el discriminant per a* $\ell(x)$ *i obtenim:*

$$\Delta = -4(-15)^3 - 27(5)^2 = 3^3 5^2 (20 - 1)$$

i per tant $\delta = 15\sqrt{3 \cdot 19} \notin \mathbb{Q}$ *i sempre per construcció* $\delta \in L$ *per tant com* $\mathbb{Q} \subseteq \mathbb{Q}(\delta) \subseteq L$ *i* $[\mathbb{Q}(\delta) : \mathbb{Q}] = 2$*; i tenim* $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_i) \subseteq L$ *i* $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = grau(Irr(\alpha_i, \mathbb{Q})[x]) = grau(\ell(x)) = 3$ *obtenim que* $[L : \mathbb{Q}] = 6$ *i* $Gal(L/\mathbb{Q}) \cong S_3$*. Fixeu-vos que tenim 4 subgrups de* S_3*:* A_3*,* $< (1,2) >$*,*$< (1,3) >$*,*$< (2,3) >$*; que corresponen als cossos intermedis respectivament:* $\mathbb{Q}(\delta), \mathbb{Q}(\alpha_3), \mathbb{Q}(\alpha_2), \mathbb{Q}(\alpha_1)$*.*

Sabem pel teorema 5.1.8 que $\ell(x)$ *és resoluble per radicals (ja que* S_3 *és un grup resoluble), anem ara a demostrar que la torre formada per extensions radicals pel polinomi* $\ell(x)$ *no conté el cos de descomposició, ho fem per reducció a l'absurd, imaginem que Sí i demostrarem que no és possible. Com el teorema principal de la teoria de Galois ens dóna tots els cossos intermedis possibles entre* $L/\mathbb{Q}$*, si podem construir una torre radical on* L *apareix a la cadena ha de ser de la forma següent:*
A) $\mathbb{Q} \subseteq \mathbb{Q}(\delta) \subseteq L$
B) $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_i) \subseteq L$*, amb* $i \in \{1, 2, 3\}$*,*
C) $\mathbb{Q} \subseteq L$*.*
Observem primer que el cas C) no pot ser torre radical. Efectivament si $L/\mathbb{Q}$ *fos extensió radical, triem* $L = \mathbb{Q}(\theta)$ *on* $\theta^n \in \mathbb{Q}$ *cert* $n > 1$*, i pensem* $L \subseteq \mathbb{C}$*, llavors totes les arrels del polinomi* $x^n - \theta^n$ *són en* L *per ser* $L/\mathbb{Q}$ *normal, en particular* $\theta e^{2\pi i/n}/\theta$ *que és a* $\mathbb{C} - \mathbb{R}$ *però recordem que* $L \subset \mathbb{R}$*, contradicció.*
Veiem ara que el cas A) tampoc pot donar una torre radical. Efectivament, és clar que $\mathbb{Q} \subseteq \mathbb{Q}(\delta)$ *és extensió radical perquè és de grau 2. Veiem que* $L/\mathbb{Q}(\delta)$ *no és una extensió radical. Si ho fos, existiria* $\theta \in L$ *on* $L = \mathbb{Q}(\delta)(\theta)$ *on* $\theta^m = q' \in \mathbb{Q}(\delta)$ *per tant* $Irr(\theta, \mathbb{Q}(\delta))|\theta^m - q'$*, observem que* $grau(Irr(\theta, \mathbb{Q}(\delta))[x]) = 3 = [L : \mathbb{Q}(\delta)]$*. Com* L *és dins* $\mathbb{R}$ *les tres arrels de* $Irr(\theta, \mathbb{Q}(\delta))[x]$ *són reals, però el polinomi* $x^m - q'$ *tan sols té com a molt 2 arrels reals!!! per tant* $L/\mathbb{Q}(\delta)$ *no pot ser una extensió radical.*
Veiem ara que el cas B) tampoc pot donar una torre radical. És clar que $L/\mathbb{Q}(\alpha_i)$ *és radical perquè té grau 2. Veiem que* $\mathbb{Q}(\alpha_i)/\mathbb{Q}$ *no pot ser radical. Si* $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\eta)$ *on* $\eta^m = q \in \mathbb{Q}$ *tenim* $Irr(\eta, \mathbb{Q})[x]|x^m - q$ *però ara com* $L/\mathbb{Q}$ *normal tenim que en* L *hi ha d'haver totes les arrels de* $Irr(\eta, \mathbb{Q})[x]$ *que han de ser 3 i totes reals perquè* $L \subset \mathbb{R}$*, però* $x^m - q$ *tan sols té com a molt 2 arrels reals! provant que aquesta torre no pot ser radical.*

Per tant per $\ell(x)$ *sabem de forma teòrica usant el teorema 5.1.8 que és resoluble per radicals però en cap torre de cossos d'extensions radicals per a* $\ell(x)$ *hi apareix el cos de descomposició de* $\ell(x)$*, tan sols en un d'aquests cossos de una torre radical contindrà el cos de descomposició.*

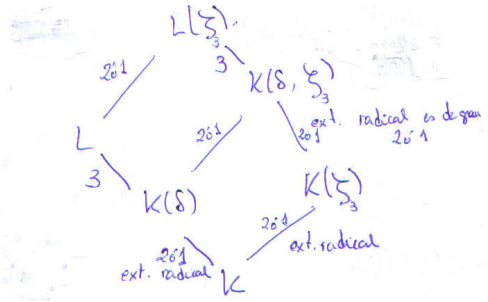
En l'exemple anterior hem explicat per un $\ell(x)$ concret que no obtenim una torre radical pensant en una cadena donada pel cos de descomposició. Com es soluciona per a trobar una torre radical i trobar una fórmula per les arrels en forma radical?

A la demostració del teorema 5.1.8 s'han donat idees per tal de trobar aquesta torre: introduir les arrels de la unitat. Referent a obtenir la fórmula per les arrels en radicals, és clau que si M/K radical, cal trobar un θ explicit on $M = K(\theta)$ amb $\theta^j \in K$ per cert natural j no zero: per a trobar θ el punt clau es troba en la demostració de la proposició 5.3.5. Anem a explicitar-ho per una equació d'una cúbica en general reobtenint la fórmula per radicals donada de forma ad-hoc en la §1.3.

Sigui ara i fins finalitzar aquesta secció $\ell(x) \in K[x]$ un polinomi de grau 3 que l'escrivim per

$$\ell(x) = x^3 + px + q,$$

observeu $\Delta = -4p^3 - 27q^2$ i δ una arrel quadrada de Δ. Sigui L un cos de descomposició de $\ell(x)$ sobre K i sigui ξ_3 una arrel 3-èssima primitiva de 1 que introduim sobre el cos L, llavors tenim la següent extensió de cossos on marquem les extensions que són sempre radicals:



Observeu que $L(\xi_3)/K(\delta, \xi_3)$ és Galois de grau 3 i per tant és cíclica. Per la proposició 5.3.5 és una extensió radical; per tant la cadena

$$K \subseteq K(\xi_3) \subseteq K(\delta, \xi_3) \subseteq L(\xi_3)$$

és una torre de cossos radicals que conté un cos de descomposició pel polinomi de grau 3 $\ell(x)$ i d'aquesta torre hem d'expressar les arrels del polinomi $\ell(x)$ en radicals, anem a buscar aquesta fórmula per radicals de les arrels.

Anem a buscar element θ on $L(\xi_3) = K(\xi_3, \delta)(\theta)$ on $\theta^3 \in K(\xi_3, \delta)$. És fàcil veure que $Gal(L(\xi_3)/K(\xi_3, \delta)) =< \sigma >$ on $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ i $\sigma(\alpha_3) = \alpha_1$. Usant ara la demostració de la proposició 5.3.5 el candidat a θ és (fixeu-vos ara que l'elecció que vam fer a la §1.3 per trobar la fórmula es

transforma amb una elecció natural a partir de la demostració de la proposició 5.3.5)

$$\theta := \alpha_1 + \xi_3\alpha_2 + \xi_3^2\alpha_3,$$

escrivim

$$\epsilon := \alpha_1 + \xi_3^2\alpha_2 + \xi_3\alpha_3.$$

Fixem-nos que tenim

$$\theta\epsilon = -3p,\ (\theta\epsilon)^3 = -27p^3;\quad \theta^3 + \epsilon^3 = -27q,$$

obtenim $(x-\theta^3)(x-\epsilon^3) = x^2 + 27qx - 27p^3$ i per tant obtenim que θ^3, ϵ^3 són els elements $\frac{27}{2}q \pm \frac{3}{2}(2\xi_3+1)\delta \in K(\xi_3, \delta)$, d'aquí i per construcció tenim

$$\alpha_1 = \frac{1}{3}(\theta + \epsilon)$$

$$\alpha_2 = \frac{1}{3}(\xi_3^2\theta + \xi_3\epsilon)$$

$$\alpha_3 = \frac{1}{3}(\xi_3\theta + \xi_3^2\epsilon);$$

obtenint les fórmules pel polinomi de grau 3 donades en §1.3 d'aquests apunts.

Appendix A

Els nombres complexos

A primer curs us van definir el nombres racionals $\mathbb{Q}$, els reals $\mathbb{R}$ i el nombres complexos $\mathbb{C}$. Recordeu que els nombres reals es defineixen per axiomes de completitud topològica via la topologia del valor absolut usual sobre $\mathbb{Q}$ (valor absolut arquimedià sobre $\mathbb{Q}$), veieu l'últim tema proposat d'aquest apèndix per diferents valors absoluts i diferents topologies.
Dins els nombres reals us parlàvem de nombres irracionals i nombres racionals, on n'hi ha dels primers un nombre no numerable i numerables pels racionals. A teoria de Galois $x \in \mathbb{C}$ (en particular en $\mathbb{R}$) parlem de nombres transcendents i d'algebraics, dels nombres irracionals n'hi ha d'algebraics sobre $\mathbb{Q}$ com $\sqrt{2}$, i $\sqrt[3]{2}$,... (nombres que són solució d'un polinomi en $\mathbb{Q}[x]$ i de nombres transcendents com π,... (nombres reals que no són arrels de cap polinomi a coeficients a $\mathbb{Q}[x]$). No obstant demostrar que un nombre real és transcendent no és una tasca fàcil (tampoc ho és demostrar que fos irracional, és dir que no pertany als nombres racionals!!!, per exemple: és sin(1) irracional? En cas afirmatiu, és transcendent o algebraic sobre $\mathbb{Q}$?).
Aquest appendix aprofundirà l'estructura de $\mathbb{C}$ com nombres algebraics i transcendents, estudiant-hi $Aut(\mathbb{C})$ (automorfisme com cos) i comentarem la transcendència sobre $\mathbb{Q}$ d'alguns nombres i referències per la demostració al lector interessat.

En aquest appendix suposem que coneixem que $\mathbb{C}$ és un cos algebraicament tancat, és a dir que tota extensió finita de $\mathbb{C}$ és $\mathbb{C}$ (equivalentment que tot polinomi no constant sobre $\mathbb{C}[x]$ té una (totes) arrel(s) a $\mathbb{C}$) i volem proposar diversos treballs per l'alumne interessat en aprofundir el temari del curs.

A.1 Primer treball: primers resultats de transcendència

La primera tasca d'aquest treball és voler presentar i demostrar el resultat de Lioville de l'any 1844 que afirma que un nombre algebraic està "allunyat" dels nombres racionals, anem a detallar que volem afirmar amb el terme "allunyat".

Teorema A.1.1 (Lioville, 1844)**.** *Per qualsevol nombre algebraic $\alpha \in \mathbb{C}$ amb $n = grau(Irr(\alpha, \mathbb{Q})[x]) > 1$, existeix una constant c (que sol depén d'α) com-*

plint

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n}$$

per tots els nombres racionals p/q amb $q > 0$ on el valor absolut és l'usual de $\mathbb{C}$ on $x + iy \in \mathbb{C}$ $x, y \in \mathbb{R}$ $|x + iy| = \sqrt{x^2 + y^2}$.

Després de fer la demostració, veureu amb un exemple com aquest resultat de Lioville permet demostrar transcendència de certs nombres expressats en sèries numèriques, efectivament:

$$\xi := \sum_{n=1}^{\infty} 10^{-n!}$$

és fàcil comprovar és convergent, trieu $p_j = 10^{j!} \sum_{n=1}^{j} 10^{-n!}$, $q_j = 10^{j!}$ i comproveu $|\xi - \frac{p_j}{q_j}| < q_j^{-j}$ i useu el teorema de Lioville anterior per observar que és transcendent.

Segonament el treball consisteix en presentar una demostració sobre la transcendència dels nombre π i del nombre e (potser acceptant algun resultat d'anàlisi complexa).

Fem primer una mica d'història. Euler l'any 1744 va demostrar la irracionalitat de e i l'any 1781 Lambert va demostrar la irracionalitat del nombre π. No fou fins 1873 que Hermite va demostrar la transcendència del nombre e. Aquest treball d'Hermite va aportar una nova línea de treball, la qual, una generalització va permetre a Lindemann demostrar el 1882 la transcendència de π. Aquests treballs van ser estudiats, simplificats i generalitzats per grans matemàtics com Weierstrass, Hilbert i Hurwitz.

Vosaltres en el seminari cal que doneu una demostració analítica, sense usar el teorema de Lindemann(-Weierstrauss) i/o la generalització de Baker (veieu el tercer treball per l'aplicació d'aquest resultat).

[Referencies: consulteu pp.1-5 del llibre Alan Baker "Transcendental number theory" Cambridge Mathematical Library.
També podeu consultar "Calculus" de Spivak per la prova e i π transcendent].

A.2 Segon treball: clausura algebraica d'un cos

Hem vist a classe que si $\alpha \in \mathbb{C}$ és algebraic sobre $\mathbb{Q}$ tenim que $\mathbb{Q}(\alpha)/\mathbb{Q}$ és una extensió algebraica sobre $\mathbb{Q}$, és a dir tot $\ell \in \mathbb{Q}(\alpha)$ és algebraic sobre $\mathbb{Q}$ és dir ℓ és solució d'un polinomi no zero sobre $\mathbb{Q}[x]$. Considerem ara $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} | \alpha \textit{ algebraic sobre } \mathbb{Q}\}$, demostrarem que és un subcos de $\mathbb{C}$ i que és algebraicament tancat, $\overline{\mathbb{Q}}$ s'anomena la clausura algebraica de $\mathbb{Q}$ dins de $\mathbb{C}$.
Per fer-ho, ho fareu en un context més general.
Comencem fent la següent definició,

Definició A.2.1. *Una extensió de cossos L/K (usualment de grau infinit) es diu una clausura algebraica de K si L/K és algebraica i L és algebraicament tancat.*

Fixeu-vos que $\mathbb{C}/\mathbb{Q}$ no és algebraica ja que $\pi \in \mathbb{C}$ no és algebraic.
Recordeu que $\mathbb{C}$ és un cos algebraicament tancat.

La primera feina d'aquest treball és enunciar i demostrar l'existència de la clausura algebraica per a un cos K arbitrari.

Teorema A.2.2. *Donat un cos K qualsevol, existeix una clausura algebraica L/K.*

La segona feina és demostrar la unicitat (llevat d'isomorfisme) de la clausura algebraica d'un cos K, anem-ho a detallar una mica.

Proposició A.2.3. *Sigui $\iota : K_1 \hookrightarrow K_2$ un monomorfisme amb K_i cossos, amb K_2 algebraicament tancat. Considerem L/K_1 una extensió algebraica llavors existeix $j : L \hookrightarrow K_2$ monomorfisme amb $j_{|K_1} = \iota$.*

I demostrar,

Teorema A.2.4. *Siguin L_1/K i L_2/K dos clausures algebraiques de K llavors existeix un automorfisme $\varphi : L_1 \to L_2$ amb $\varphi_{|K} = id$.*

Un cop demostrats els resultats anteriors, apliquem-los a $K = \mathbb{Q}$. És fàcil demostrar que $\overline{\mathbb{Q}}$ és una clausura algebraica de $\mathbb{Q}$ i és única entre les clausures algebraiques de $\mathbb{Q}$ dins $\mathbb{C}$. Demostreu que $\overline{\mathbb{Q}}$ és numerable, per tant hi ha un nombre no numerable de nombres no algebraics en $\mathbb{C}$.

[Referència: capítol 8 del llibre d'en Garling "A course in Galois theory", Cambridge University Press. Consulteu també el capítol 6 del llibre de'n Milne "Galois Theory".]

A.3 Tercer treball: més exemples de nombres transcendents mitjançant els teoremes de Lindermann(-Weierstrass) i Baker

Estudi de la transcendència de α^β.

El treball de Lindermann presentat en l'any 1882 (veieu també el primer treball pel primer resultat important d'aquesta memòria de Lindermann que demostrava la transcendència de π per primer cop) afirmava un altre resultat (una demostració completa va ser donada per Weierstrass alguns anys després), és,

Teorema A.3.1 (Lindermann-Weierstrass)**.** *Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$ que són $\mathbb{Q}$-linealment independents. Llavors les exponencials $e^{\alpha_1}, \ldots, e^{\alpha_n}$ compleixen que no hi ha cap polinomi no nul $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ complint $f(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$.*

Aquest teorema és equivalent al teorema

Teorema A.3.2 (Lindermann-Weierstrass)**.** *Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$ diferents. Llavors $e^{\alpha_1}, \ldots, e^{\alpha_n}$ són $\mathbb{Q}$-linealment independents.*

Després d'esboçar-ne la prova en la vostra expossició en el seminari, expliciteu tot demostrant-ho diferents conseqüències immediates del teorema de Lindermann-Weierstrass com són [1] [2]:

1. e^{α} amb α algebraic no zero és transcendent,
2. π i e transcendents (π:red.absurd i useu $e^{\pi i}=-1$ i $e^0=1$),
3. $\sin(\alpha), \cos(\alpha), \sec(u), \mathrm{cosec}(u), \tan(u), \mathrm{cotan}(u)$ amb u algebraic no nul són transcendents (useu expressions de e^{ix}, e^{-ix} amb $x \in \mathbb{R}$ per les anteriors funcions trigonomètriques)
4. $u \neq 1$ algebraic no zero i f una de les funcions trigonomètriques inverses, llavors $f(u)$ és transcendent sobre $\mathbb{Q}$,
5. si $u \neq 1$ algebraic llavors $log(u)$ és transcendent sobre $\mathbb{Q}$.

L'any 1900, Hilbert, dins el congrés internacional de matemàtiques (el ICM, que es celebra cada quatre anys, i recordeu que l'any 2006 el ICM va celebrar-se a Madrid) va presentar un conjunt de 23 problemes que van ser referència per tots els matemàtics en la seva recerca durant tot el segle XX, [per aprofundir en aquests problemes (cosa que no se us demana en aquest treball!!!) i els posteriors esforços animo a tot matemàtic interessat a llegir "El reto de Hilbert" de Jeremy J.Gray publicat en ed.Crítica].

El seté problema es referia a transcendència i preguntava:
Donats $\alpha, \beta \in \mathbb{C}$ algebraics sobre $\mathbb{Q}$ amb $\alpha \neq 0, 1$ que podem dir sobre transcendència o no del nombre complex α^{β} sobre $\mathbb{Q}$? per exemple és $2^{\sqrt{2}} (= e^{\sqrt{2} log(2)})$ transcendent sobre $\mathbb{Q}$?
La intuició de Hilbert va fallar aquí, ja que inicialment va considerar que la solució d'aquest problema vindria després de demostrar la hipòtesi de Riemann (que encara és un problema obert) i l'últim teorema de Fermant (demostrada per Wiles recentment, 1995-1998). Gelfond 1929 i Kuzmin 1930 van aportar resultats parcials fins arribar al resultat general que afirmava la transcendència de α^{β} usant una tècnica d'anàlisi d'una funció auxiliar, el resultat obtingut simultàneament per Gelfond i Schneider (de forma independent) és,

Teorema A.3.3 (Gelfond-Schneider, 1934)**.** *Siguin $\alpha_1, \alpha_2, \beta_1$ i β_2 nombres algebraics sobre $\mathbb{Q}$ no zero amb $log(\alpha_1), log(\alpha_2)$ $\mathbb{Q}$-linealment independents, llavors*

$$\beta_1 \log(\alpha_1) + \beta_2 \log(\alpha_2) \neq 0.$$

Demostreu que aquesta formulació d'aquest teorema implica el corol.lari següent,

[1] **Exponencial complexa i logaritme complex**. Coneixèu, les funcions de variable real $e : \mathbb{R} \to \{r \in \mathbb{R} | r > 0\}$ i $\log : \{r \in \mathbb{R} | r > 0\} \to \mathbb{R}$. Sabem que $e^{ir} = \cos(r) + i \sin(r)$ amb $r \in \mathbb{R}$ això permet definir una exponencial complexa amb la propietat $exp(A+B) = exp(A)exp(B)$ amb $A, B \in \mathbb{C}$ definida per $exp : \mathbb{C} \to \mathbb{C}^*$ $exp(r+is) := e(r)\cos(s) + ie(r)\sin(s)$ amb $r, s \in \mathbb{R}$.

[2] Fixem-vos que $exp(c + 2\pi ik) = exp(c)$ per $c \in \mathbb{C}$ amb $k \in \mathbb{Z}$, per tant la funció exp no és injectiva. No obstant podem plantejar-nos si existeix un logaritme, no obstant la falta d'aquesta injectivitat farà que s'han de restringir a una banda de nombres complexos, "determinació del logaritme", indicant que en aquesta banda no hi ha dos nombres complexos on la seva diferència sigui un múltiple enter de $2\pi i \in \mathbb{C}$. Usualment es tria el següent subconjunt $M_{-\pi,\pi} = \{c \in \mathbb{C} | -\pi \leq Im(c) < \pi\}$ i s'obté una funció logaritme $\log : \mathbb{C}^* \to M_{-\pi,\pi}$ complint $exp(\log(\alpha)) = \alpha \in \mathbb{C}$, fixeu-vos que es compleix $\log(exp(\alpha)) = \alpha'$ amb $\alpha - \alpha' = 2\pi ik'$ per a cert $k' \in \mathbb{Z}$.

Corol·lari A.3.4 (Gelfond-Schneider, 1934). *α, β algebraics sobre $\mathbb{Q}$ no zero amb $\alpha \neq 1$ i $\beta \notin \mathbb{Q}$ llavors α^β és transcendent sobre $\mathbb{Q}$.*

Aquí acaba la primera part del vostre treball. Deixeu-me completar una mica més la posterior evolució i algunes altres qüestions.

El teorema de Gelfond-Schneider de l'any 1934 es va plantejar si es podia generalitzar a una expressió amb n enlloc de 2 i es va observar que fer-ho aportaria resultats de transcendència per expressions de la forma $e^{\beta_0}\alpha_1^{\beta_1}\ldots\alpha_n^{\beta_n}$ amb β_i, α_i algebraics. Va ser Alan Baker l'any 1966 que obté aquesta generalització (comentar que a l'ICM 1970 Baker va rebre la medalla Fields per aquesta aportació):

Teorema A.3.5 (Baker, 1966). *Si $\alpha_1, \ldots, \alpha_n$ són nombres algebraics no zero complint que*

$$\log(\alpha_1), \ldots, \log(\alpha_n)$$

són $\mathbb{Q}$-linealment independents llavors $1, \log(\alpha_1), \ldots, \log(\alpha_n)$ són $\mathbb{Q}$-linealment independents.

Com a conseqüències s'obtenen els següents corol.laris

Teorema A.3.6 (Baker,1966). *Siguin $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ algebraics, amb $\alpha_i's$ no zero. Escrivim $\delta := \beta_1 \log(\alpha_1) + \ldots + \beta_n \log(\alpha_n)$. Si $\delta \neq 0$ llavors δ és transcendent sobre $\mathbb{Q}$.*

Teorema A.3.7 (Baker, 1966). *El nombre $e^{\beta_0}\alpha_1^{\beta_1}\ldots\alpha_n^{\beta_n}$ és transcendent sobre $\mathbb{Q}$ per qualsevol $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n$ algebraics no zero.*

Teorema A.3.8 (Baker, 1966). *El nombre $\alpha_1^{\beta_1}\ldots\alpha_n^{\beta_n}$ és transcendent sobre $\mathbb{Q}$ per qualsevol $\alpha_1, \ldots, \alpha_n$ algebraics no zero ni 1, i qualsevol nombres algebraics $\beta_1, \ldots, \beta_n$ complint que $1, \beta_1, \ldots, \beta_n$ $\mathbb{Q}$-linealment independents.*

Fins aquí, tan el primer treball d'aquest seminari com en aquest treball hem estudiat transcendència sobre $\mathbb{Q}$. Tot seguit, en el següent treball d'aquest seminari, parlarem de bases de transcendència i surt la pregunta natural (veieu proposició A.4.2) si un nombre transcendent sobre $\mathbb{Q}$ ho és encara sobre $\mathbb{Q}(\delta)$ on δ és un altre nombre transcendent, per exemple podem preguntar-nos: és π transcendent sobre $\mathbb{Q}(e)$?
Per respondre afirmativament caldria afirmar que no existeix $f(x, y) \in \mathbb{Q}[x, y]$ no zero complint $f(e, \pi) = 0$.
Hi ha molt pocs resultats en aquest sentit. Hi ha una conjectura de Schanuel que aportaria gran progrés en la matèria. Anem a explicar-la, no obstant hem d'introduir primer la següent definició.

Definició A.3.9. *Sigui F/K extensió de cossos. Siguin $a_1, \ldots, a_m \in F$. Diem que $a_1, \ldots, a_m$ són algebraicament independents sobre K si tota $f \in K[x_1, \ldots, x_m]$ complint $f(a_1, \ldots, a_m) = 0$ implica $f = 0$.*

Conjectura A.3.10 (Schanuel). *Si $y_1, \ldots, y_m$ nombres complexos $\mathbb{Q}$-linealment independents llavors hi ha com a mínim m dels nombres*

$$y_1, \ldots, y_m, e^{y_1}, \ldots, e^{y_m}$$

que són algebraicament independents sobre $\mathbb{Q}$.

Suposant certa la conjectura, considereu els dos nombres algebraics $\mathbb{Q}$-linealment independents $1, i\pi$, obtenim $1, i\pi, e^{i\pi} = -1, e$ almenys dos són algebraicament independents, per força han de ser $i\pi$ i e, d'aquí fàcilment s'obté:

Corol·lari A.3.11. *Si la conjectura de Schanuel anterior és certa llavors π és transcendent sobre $\mathbb{Q}(e)$ i e és transcendent sobre $\mathbb{Q}(\pi)$.*

[Referència (pel treball): P.Morandi, "Fields and Galois theory", Springer, GTM 167, p.135 i posteriors.
Altra referència: A. Baker, "Transcendental number theory", Cambridge, CML, capítols 1, 2.]

A.4 Quart treball: base de transcendència

Hem vist del segon treball que tenim

$$\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subset \mathbb{C}$$

on $\overline{\mathbb{Q}}$ és el cos que conté tots els nombres complexos que són algebraics sobre $\mathbb{Q}$ (a més és numerable), per tant $\mathbb{C} - \overline{\mathbb{Q}}$ està format per nombres transcendents (i és un conjunt no numerable). En el tercer treball hem demostrat que per exemple $e^{\sqrt{2}}$ i $e^{2\sqrt{2}}$ són transcendents, però és clar que ambdós tenen una relació algebraica entre ells. Volem un concepte de base de transcendència on no hi hagi relació algebraica entre aquests nombres, aquest problema s'ha plantejat ja anteriorment; efectivament hem preguntat en el treball anterior si e és transcendent sobre $\mathbb{Q}(\pi)$ o no. La noció de base de transcendència sobre un cos $F \subseteq \mathbb{C}$ refereix a triar un conjunt maximal de nombres de $\mathbb{C}$ que són algebraicament independents sobre el cos base F (veieu definició A.3.9 d'algebraicament independents en el treball anterior).

El treball consisteix en presentar la noció de base de transcendència i obtenirne la seva existència i propietats bàsiques, i com aplicació observar que $\mathbb{C}/\overline{\mathbb{Q}}$ té una base de transcendència (format per nombres transcendents sobre $\overline{\mathbb{Q}}$ i en particular sobre $\mathbb{Q}$) no numerable $\{t_i\}_{i\in I}$ on $\mathbb{C}/\overline{\mathbb{Q}}(\{t_i\}_{i\in I})$ és una extensió algebraica ($\mathbb{C}$ és una extensió algebraica sobre $\overline{\mathbb{Q}}(\{t_i\}_{i\in I})$.

El treball consisteix en exposar §18.1 i §18.2 del llibre de'n Garling, veieu referència.
Anem a detallar el treball, comencem fent la següent definició:

Definició A.4.1. *Un subconjunt S de L és algebraicament independent sobre K (L/K extensió de cossos) si per cadascún dels subconjunts finits T de S, els elements de T són algebraicament independents respecte la definició A.3.9.*

Per agafar intuició enuncieu aquest resultat sense demostrar-ho,

Proposició A.4.2. *Sigui L/K extensió i $\delta_1, \ldots, \delta_n$ elements diferents de L. Denotem $K_0 = K$, $K_i := K(\delta_1, \ldots, \delta_i)$ per $i = 1, \ldots, n$. Llavors $\{\delta_1, \ldots, \delta_n\}$ són algebraicament independents sobre K si i només si δ_i és transcendent sobre K_{i-1} per $i = 1, \ldots, n$.*

Denotem per $\mathcal{L}_{L/K} := \{S \subset L | S \text{ algebraicament independent}\}$ ordenem aquest conjunt per inclusió, un element $S \in \mathcal{L}_{L/K}$ maximal respecte inclusió s'anomena una base de transcendència de L sobre K.
Observareu la propietat següent (demostrant-la o no)

Proposició A.4.3. *Sigui L/K una extensió i S subconjunt de S. Llavors S és una base de transcendència de L sobre K si i nomes si $S \in \mathcal{L}_{L/K}$ i $L/K(S)$ és una extensió algebraica.*

I demostrareu

Teorema A.4.4. *Sigui L/K extensió, i A un subconjunt de L on $L/K(A)$ és algebraic i C un subconjunt de A que és algebraicament independent sobre K. Llavors existeix una base de transcendència B de L sobre K amb $C \subseteq B \subseteq A$.*

Un cop demostrat aplicarem a demostrar que $\mathbb{C}$ té una base de transcendència S sobre $\mathbb{Q}$ o sobre $\overline{\mathbb{Q}}$ on S és un conjunt no numerable (useu el fet que tota extensió algebraica finita o no d'un cos numerable és numerable).

[Referencia: el llibre Garling "A course in Galois Theory" de la Cambridge, capítol 18.]

A.5 Cinqué Treball: $Aut_{\mathbb{Q}}(\mathbb{C})$

Aquest treball intenta donar idees de cossos isomorfs a $\mathbb{R}$ que es troben dins de $\mathbb{C}$, (penseu que cal que mantingui l'operació producte i la idea "ximple" de rectes dins $\mathbb{C}$ passant per l'origen, que són $\mathbb{Q}$-espais vectorials, no donen cossos: el producte de dos nombres surt d'aquesta recta), i de com és de gran $Aut_{\mathbb{Q}}(\mathbb{C})$. La dificultat d'aquest treball radica en donar-ne una referència, anem doncs a indicar el treball en forma d'exercicis e indicacions per poder-los fer.

Sempre aquest treball $Aut(K)$ es refereix a automorfismes de cossos del cos K en ell mateix, i $Aut_M(K)$ els automorfismes del cos K deixant fix el cos M. El primer que farem és demostrar el següent resultat

Proposició A.5.1. $Aut(\mathbb{R}) = \{id\}$.

Indicació: es fácil demostrar que fixa $\mathbb{Q}$. Després demostreu que envia nombres reals positius a positius i preserva ordre, obtenint

$$\{r \in \mathbb{Q} | a < r\} = \{r \in \mathbb{Q} | \alpha(a) < r\}$$

per $\alpha \in Aut(\mathbb{R})$, usant la propietat de suprem en conjunts en $\mathbb{R}$ obteniu el resultat.

De l'anterior proposició observem que tenim molt pocs automorfismes del cos dels nombres reals, tan sols un!!!

Anem tot seguit a estudiar $Aut(\mathbb{C})$ els automorfisme de cossos de $\mathbb{C}$ en ell mateix. És fàcil demostrar que $Aut_{\mathbb{Q}}(\mathbb{C}) = Aut(\mathbb{C})$.
Del treball anterior tenim que $\mathbb{C}$ és una extensió algebraica de $\overline{\mathbb{Q}}(S)$ on S és una base de transcendència de $\overline{\mathbb{Q}}$ a $\mathbb{C}$ on S és un conjunt no numerable. Observeu:

Lema A.5.2. *Hi ha una infinitud no numerable de $Aut_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}(S))$.*

Per fer-ne la demostració observeu que qualsevol bijecció del conjunt S dóna un automorfisme de $\overline{\mathbb{Q}}(S)$ fixant $\overline{\mathbb{Q}}$ i recordeu que S és un conjunt no numerable. Tot seguit demostreu:

Proposició A.5.3. *Tot $\phi \in Aut_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}(S))$ s'extén a un element del grup $Aut_{\overline{\mathbb{Q}}}(\mathbb{C})$ i en particular dóna elements del grup $Aut_{\mathbb{Q}}(\mathbb{C})$, i $Aut_{\mathbb{Q}}(\mathbb{C})$ és un grup amb un nombre no numerable d'elements.*

Per demostrar-ho, considereu $\phi \in Aut_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}(S))$, podem pensar-ho com $\phi : \overline{\mathbb{Q}}(S) \to \mathbb{C}$, i demostreu primer que ϕ s'estén a un monomorfisme $\tilde{\phi} : \mathbb{C} \to \mathbb{C}$ (useu lema de Zorn, recordeu $\mathbb{C}/\overline{\mathbb{Q}}(S)$ és una extensió algebraica). Tot seguit, demostreu que $\tilde{\phi}$ és automorfisme, és a dir un element de $Aut_{\overline{\mathbb{Q}}}(\mathbb{C})$, per fer-ho observeu $\tilde{\phi}(\mathbb{C}) \cong \mathbb{C}$ i $\mathbb{C}/\tilde{\phi}(\mathbb{C})$ és una extensió algebraica de com està construït ϕ, observeu que $\tilde{\phi}(\mathbb{C})$ és algebraicament tancat i intenteu concloure.

Un podria preocupar-se per $Aut_{\mathbb{Q}}(\mathbb{C})$ enlloc d'estudiar $Aut_{\overline{\mathbb{Q}}}(\mathbb{C})$ on en aquest últim l'automorfisme fixa tots els nombres algebraics sobre $\mathbb{Q}$, però per les nostres qüestions aquí és suficient. Fixeu-vos que un nombre algebraic sobre $\mathbb{Q}$ ha d'anar un algebraic sobre $\mathbb{Q}$ per un automorfisme de $Aut_{\mathbb{Q}}(\mathbb{C})$; per tant un grup clau a estudiar és $Aut_{\mathbb{Q}}(\overline{\mathbb{Q}})$ (un automorfisme de $Aut_{\mathbb{Q}}(\overline{\mathbb{Q}})$ podem pujar-lo a $\overline{\mathbb{Q}}(S)$, hi ha una infinitud no numerable d'automorfismes de pujar-los i cadascun d'aquests automorfisme a $\overline{\mathbb{Q}}(S)$ heu demostrat en la prova sugerida per la proposició anterior que poden pujar-se a $\mathbb{C}$, és a dir a elements de $Aut_{\mathbb{Q}}(\mathbb{C})$ on aquest última pas el nombre d'aixecaments d'un automorfisme en $\overline{\mathbb{Q}}(S)$ a $\mathbb{C}$ és un conjunt numerable, ja que és $\mathbb{C}/\overline{\mathbb{Q}}(S)$ extensió algebraica) aquest és el grup més important pels teoristes de nombres i geòmetres aritmètics, una millor comprensió permetria un millor atac a problemes d'aquests camps matemàtics.

Centrem-nos amb algunes conseqüències dels nostres resultats, heu de demostrar,

Corol·lari A.5.4. $\mathbb{C}$ *conté infinits cossos isomorfs a* $\mathbb{R}$ *que contenen a* $\mathbb{Q}$.

Per fer la demostració observeu que si $\sigma_1, \sigma_2 \in Aut_{\mathbb{Q}}(\mathbb{C})$ tenim que $\sigma_2^{-1}\sigma_1 \in Aut_{\mathbb{Q}}(\mathbb{R})$ i per tant σ_1, σ_2 són iguals si es restringeixen a $\mathbb{R}$.
Tot seguit, definiu la relació d'equivalència $\sigma_1 \sim \sigma_2 \Leftrightarrow \sigma_1(\mathbb{R}) = \sigma_2(\mathbb{R})$. Veieu que en cada classe sol hi ha dos elements de $Aut_{\mathbb{Q}}(\mathbb{C})$, useu la infinitud dels $Aut_{\mathbb{Q}}(\mathbb{C})$ per a concloure.

Finalment demostreu el següent resultat:

Proposició A.5.5. *Sigui $K \subseteq \mathbb{C}$ un cos diferent dels $\mathbb{R}$ però isomorf a $\mathbb{R}$. Demostreu que K és dens en $\mathbb{C}$ amb la topologia del mòdul en variable complexa $|z = a + bi| = \sqrt{a^2 + b^2}$.*

Per la prova si $\beta : \mathbb{R} \to K$ és l'isomorfisme de cossos, és fàcil demostrar que s'extén a un automorfisme dels complexos $\tilde{\beta} : \mathbb{C} \to \mathbb{C}$. Heu de demostrar que donat $x + iy \in \mathbb{C}$ arbitrari i per a tot $\varepsilon > 0$ existeix elements del cos K, diem-lo η complint $|x + iy - \eta| < \varepsilon$. Per fer això trieu $a + bi \in K$ arbitrari amb $b \neq 0$ i si $q_1, q_2 \in \mathbb{Q}$ observeu $q_1(a + bi) + q_2 = (q_1 a + q_2) + q_1 b_1 \in K$, per qualsevol racionals q_1, q_2. Ara trieu q_1, q_2 amb els propòsits buscats usant que la clausura del valor absolut usual (arquimedià) de $\mathbb{Q}$ és $\mathbb{R}$.

A.6 Sisè Treball: Inmersions i topologies

Considerem el cos $K := \mathbb{Q}[x]/(x^2 - 2)$, fixem-nos que la clase de x representa un número on el seu quadrat és 2, dins dels nombres complexos hi ha dues

possibilitats per aquest valor $\pm\sqrt{2}$ i podem definir els següents isomorfismes de cossos (inmersions de K en $\mathbb{C}$),

$$\sigma_1 : K \to \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{C}, \sigma_2 : K \to \mathbb{Q}[-\sqrt{2}] \subseteq \mathbb{C}$$

via $\sigma_1([x]) = \sqrt{2}$ i $\sigma_2([x]) = -\sqrt{2}$. A $\mathbb{C}$ tenim el valor absolut usual $|z = a + bi| = \sqrt{a^2 + b^2}$ definint-hi una topologia. Anem a estudiar com σ_i donen valors absoluts diferents en K i per tant topologies diferents. Ho farem en general per un cos K no necessàreament extensió de grau 2 sobre $\mathbb{Q}$, sinó de grau n. Anem a detallar el treball, es un treball que combina anàlisi, topologia i àlgebra.

Definició A.6.1. *Sigui K un cos qualsevol. Un valor absolut de K és una aplicació $|\ | : K \to \mathbb{R}$ tal que $\forall x, y \in K$ satisfà els axiomes següents:*

1. $|x| \geq 0$,
2. $|x| = 0 \Leftrightarrow x = 0$,
3. $|xy| = |x||y|$; *i*
4. *desigualtat triangular:* $|x + y| \leq |x| + |y|$.
   Si a més satisfà un axioma més fort que la desigualtat triangular:

(d') *desigualtat ultramètrica:* $|x + y| \leq max(|x|, |y|)$

es diu que el valor absolut és no arquimedià o ultramètric, en altre cas el valor absolut s'anomena arquimedià.

Recordeu que donar un valor absolut en K, defineix una topologia donat per la $distancia(x, y) = |x - y|$.

Observeu que tot l'anàlisi que us han explicat es arquimedià, però hi ha tot un altre anàlisi no arquimedià que no se us explica. Perquè és útil l'anàlisi no arquimedià? És molt útil per teoria de nombres per exemple, recordeu la reina de les matemàtiques segons Gauss ja que és una disciplina que usa tant anàlisi, geometria, àlgebra i topologia. Anem a donar un conjunt de valors absoluts a $\mathbb{Q}$ per tenir idea de diferents valors absoluts.

Exemple A.6.2. Valors absoluts en $\mathbb{Q}$. *A $\mathbb{Q}$, hi ha el valor absolut arquimedià usual $|x| := max(x, -x)$. D'altra banda per cada nombre primer p de $\mathbb{Q}$ definirem un valor absolut (no arquimedià) mitjançant $|x|_p := p^{-v_p(x)}$ on $v_p(x)$ és l'enter definit de la forma següent: escrivim $x \in \mathbb{Q}$ com $x = \frac{n}{m}$ amb n, m enters coprimers, sigui ℓ_1 la potència de p que divideix n i ℓ_2 la potència de p que divideix m llavors $v_p(x) = \ell_1 - \ell_2$. Per exemple $|24|_2 = \frac{1}{2^3}$, $|24|_3 = \frac{1}{3}$ i $|24|_p = 1$ per a $p \geq 5$, fixeu-vos que el valor $|x|_p$ ens permet saber com el primer p apareix en x, propietat aritmètica.*

És pot demostrar que aquests valors absoluts que acabem de presentar són tots els valors absoluts a $\mathbb{Q}$ que defineixen topologies diferents, tot seguit ho detallem un mica amb més generalitat.

Definició A.6.3. *Dos valors absoluts d'un mateix cos K, $|\ |_1, |\ |_2$ s'anomenen equivalents quan defineixen la mateixa topologia, recordeu que la topologia donada per un valor absolut $|\ |$ és via la funció distàcia $distancia(x, y) = |x - y|$.*

Es pot demostrar,

Proposició A.6.4. *Dos valors absoluts no trivials d'un cos K $|\ |_1, |\ |_2$ són equivalents si i només si existeix un nombre real $r > 0$ tal que per a tot $x \in K$ $|x|_2 = |x|_1^r$.*

Recordem que $\mathbb{R}$ és un cos complet respecte el valor absolut usual arquimedià, i $\mathbb{R}$ s'obté de completar $\mathbb{Q}$ amb el valor absolut arquimedià. També hi ha completacions de $\mathbb{Q}$ pels valors absoluts no arquimedians de l'exemple A.6.2, aquesta completació dóna altres cossos que no treballarem en aquest curs, cossos p-àdics que s'anoten per $\mathbb{Q}_p$.

Anem avui a parlar de cossos respecte un valor absolut arquimedià.

Teorema A.6.5 (Ostrowski)**.** *Sigui K un cos complet respecte d'un valor absolut arquimedià $|\ |$. Llavors K és isomorf al cos $\mathbb{R}$ o bé al cos $\mathbb{C}$ i el valor absolut $|\ |$ és equivalent al valor absolut usual (i.e. l'isomorfisme de cossos és també un morfisme continu amb les topologies donades pels valors absoluts).*

Anem després d'aquesta introducció a detallar el que heu de treballar en aquest treball del seminari, fins ara tan sols era a nivell divulgatiu.

Considereu K una extensió finita de $\mathbb{Q}$, tenim $[K : \mathbb{Q}] = n$, veurem a teoria que K és simple i per tant $K = \mathbb{Q}(\alpha)$ on $grau(Irr(\alpha, \mathbb{Q})[x]) = n$, per cert $\alpha \in K$. Per a cada arrel $\delta_i \in \mathbb{C}$ del polinomi $Irr(\alpha, \mathbb{Q})[x]$ podem definir monomorfisme,

$$\sigma_{\delta_i} : K \hookrightarrow \mathbb{C}$$

via $\sigma_{\delta_i}(\alpha) := \delta_i$ i $\mathbb{Q}$-lineal. Aquest morfisme que anomenem immersió defineix un valor absolut en K (i per tant una topologia en K) definit per:

$$|x|_{\sigma_{\delta_i}} := \sqrt{\sigma_{\delta_i}(x)\overline{\sigma_{\delta_i}(x)}}$$

on donat $\gamma = a + bi \in \mathbb{C}$ amb $a, b \in \mathbb{R}$, $\overline{\gamma} = a - bi$ és el conjugat complex.
Ordenem les n arrels de $Irr(\alpha, \mathbb{Q})[x]$ de la forma: $\alpha_1, \ldots, \alpha_{r_1} \in \mathbb{R}$ les arrels reals i

$$\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \ldots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$$

, les arrels complexes i no reals (recordeu que si γ és arrel d'un polinomi a $\mathbb{Q}[x]$ també $\overline{\gamma}$ és arrel d'aquest polinomi). Considerem les diferents immersions:

$$\sigma_{\alpha_i} : K \hookrightarrow \mathbb{C}$$

definides per $\sigma_{\alpha_i}(\alpha) = \alpha_i$ i $\mathbb{Q}$-lineals, observeu que les r_1 primeres la imatge és real, i les $2r_2$ segones la imatge no és dins els nombres reals.
El teorema a estudiar i a demostrar és

Teorema A.6.6. *Sigui K una extensió de grau n. Siguin r_1, r_2 com abans. Tot valor absolut arquimedià de K és equivalent a un dels valors absoluts $|x|_{\sigma_{\alpha_i}}$ amb $i \in \{1, \ldots, n\}$, a més si $\alpha_{i+1} = \overline{\alpha_i}$ el valor absolut $|x|_{\sigma_{\alpha_{i+1}}}$ és igual a $|x|_{\sigma_{\alpha_i}}$ i llevat d'aquestes identificacions tots els valors absoluts anteriors són no equivalents, i per tant hi ha en K exactament r_1+r_2 valors absoluts arquimedians no equivalents.*

[Referència: J. Neukirch "Algebraic Number Theory", cap.II §3,Springer]

Appendix B

Aprofundint amb construccions geomètriques usant teoria de galois

Hem vist a classe de teoria que un punt $x \in \mathbb{R}$ és construïble amb regle i compàs si i només si existeixen una torre de cossos $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m$ amb $x \in K_m$ i $[K_i : K_{i-1}] \leq 2$ per $i = 1, \ldots, m$.

En aquest apendix expossarem diversos treballs per l'alumne interessat a ampliar resultats sobre construccions amb regle i compàs de certs punts i un segon bloc de treballs referent a construccions possibles amb origami, és a dir distàncies que poden fer-se amb plecs en un paper (via certs axiomes). En tècniques d'origami s'obté un resultat anàleg a l'anterior però amb $[K_i : K_{i-1}] \leq 3$, per tant la construcció en origami permet fer més construccions que amb regle i compàs.

B.1 Construcció del polígons regulars amb regle i compàs.

En aquests treballs volem estudiar per a quins $n \in \mathbb{N}$ $cos(\frac{2\pi}{n})$ i $sin(\frac{2\pi}{n})$ són construïbles amb regle i compàs, ja que si ho són ens permet construir el punt $P = (\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$. Considereu el cos $\mathbb{Q}(e^{\frac{2\pi i}{n}})$, on recordeu $e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n}) \in \mathbb{C}$. És fàcil demostrar que el polígon regular d' n-costats és construïble amb regle i compàs si i només si $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ té una cadena de subcossos $\mathbb{Q} = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r$ amb $\mathbb{Q}(e^{\frac{2\pi i}{n}}) \subseteq L_r$ i $[L_i : L_{i-1}] \leq 2$ si i només si $\mathbb{Q}(\cos(\frac{2\pi i}{n}))$ té una cadena de subcossos $\mathbb{Q} = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_s$ amb $\mathbb{Q}(\cos(\frac{2\pi i}{n})) \subseteq M_s$ amb $[M_i : M_{i-1}] \leq 2$.

(Tr1) **Treball 1: Un petit estudi del cos $\mathbb{Q}(e^{\frac{2\pi i}{n}})$.**
En aquest treball heu de calcular $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}]$ i $P_n(x) := Irr(e^{\frac{2\pi i}{n}}, \mathbb{Q})[x]$. És clar que $e^{\frac{2\pi i}{n}}$ és una arrel de $x^n - 1$ i és clar que $x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1)$. Per a $n \geq 2$ tenim $P_n | x^{n-1} + \ldots + x + 1$. Observeu que si $m|n$

(amb $m \neq n$, $m \geq 2$) les arrels no 1 de $x^m - 1$ són de $x^n - 1$ i per tant s'obté $P_m | x^{n-1} + \ldots + x + 1$. Definim ara una arrel n-èssima primitiva $\xi_n \in \mathbb{C}$ com un arrel de $x^n - 1$ però que no és arrel de $x^m - 1$ quan $m|n$ amb $m \neq n$. Definiu el polinomi

$$\Phi_n(x) := \prod_{\xi_n} (x - \xi_n).$$

I definim $\varphi(n) := grau(\Phi_n)$.

El treball consisteix en:
1) demostrar $\Phi_n(x) \in \mathbb{Q}[x]$,
2) Demostreu $\varphi(n) = \#\{\ell \in \mathbb{N}_{\geq 1} | mcd(\ell, n) = 1, \ell \leq n\}$. Si escrivim $n = \prod_{i=1}^{n} p_i^{n_i}$ amb p_i primers, demostreu llavors que $\varphi(n) = \prod_{i=1}^{n} p_i^{n_i - 1}(p_i - 1)$.
3) Proveu que $P_n(x) = \Phi_n(x)$ i per tant $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}] = \varphi(n)$.

[Referència: llibre de Matemàtica discreta de'n Rifà i altres autors, Materials UAB, i/o algún llibre de Teoria de Galois (en aquest últim cas vigileu a no utilitzar tècniques no donades encara en el curs)].

(Tr2) **Treball 2: Polígons construïbles amb regle i compàs. Primers de Fermat.**
El treball consisteix principalment en demostrar el següent teorema de Gauss (usant el resultats del treball 1 d'aquest seminari):

Teorema B.1.1 (Gauss, 1796)**.** *Si el polígon d'n-costats és construïble amb regle i compàs llavors n és de la forma següent* $n = 2^s$ *o bé* $2^s p_1 \cdot \ldots \cdot p_r$ *on* p_i *són primers diferents de Fermat, amb* $s \in \mathbb{N}$.

Falta dir que és un primer de Fermat: un primer s'anomena de Fermat si és de la forma $p = 2^r + 1$ amb $r \in \mathbb{N}$.
Usant el petit teorema de Fermat és fàcil demostrar que els possibles primers de Fermat han de ser de la forma $2^{2^j} + 1$ (efectivament $2^r \equiv -1 (mod\ p)$ per tant $2r|p-1$).
Fermat va conjecturar l'any 1650 que tots els nombres naturals de la forma $2^{2^j} + 1$ són primers, aquesta conjectura és errònea i va ser Euler l'any 1732 que va donar el primer contraexemple.

El treball consisteix primer en demostrar l'anterior teorema de Gauss, i tot seguit explicitar els primers de Fermat més petits que són primers i observar que la conjectura de Fermat és errònea, és a dir donar el contraexemple d'Euler.

[Referència: qualsevol llibre de teoria de Galois, per exemple el Garling].

Comentar, a caire informatiu, que més endavant en el curs veurem que $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ té la bona propietat d'extensió d'automorfismes sobre $\mathbb{Q}$, dita "extensió de Galois sobre $\mathbb{Q}$" amb cert grup (grup d'automorfismes) que anomenarem grup de Galois, i el coneixement dels subgrups d'aquest grup (que en el cas $\mathbb{Q}(e^{2\pi i/n})$ és un grup abelià i per tant molt fàcil calcular-hi tots els subgrups) permet construir tota la torre de subcossos (correspondència de Galois) i per tant si tenim una torre de subcossos amb grau 2 obtindrem que és construïble, això permet demostrar usant teoria de Galois el recíproc de l'anterior resultat de forma molt senzilla.

Referent a aquest recíproc a l'anterior teorema de Gauss, cal comentar que Gauss va afirmar-lo, però la primera demostració va ser presentada l'any 1836 per Wantzel:

Teorema B.1.2 (Wantzel, 1836). *Si $n = 2^s$ o bé $2^s p_1 \cdot \ldots \cdot p_r$ on p_i són primers diferents de Fermat, amb $s \in \mathbb{N}$, llavors el polígon regular de n-costars és construïble amb regle i compàs.*

(Tr3) **Treball 3: Construcció del polígon regular de 17 costats**

Gauss tenia dues passions, les matemàtiques i la filologia. Va esser (segons una llegenda) trobar la següent expressió als dinou anys d'edat, (1796):

$$16cos(\frac{2\pi}{17}) = -1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}, \tag{B.1}$$

que va fer-lo decidir a dedicar-se a les matemàtiques completament. Observeu que la igualtat (B.1) dóna la construcció algebraica del punt necessari per a construir el polígon regular de 17 costats que Gauss sabia que era construïble pel teorema de Gauss que hem intrduït en el treball 2 d'aquest seminari.

Aquesta expressió (B.1) com l'argument general de construcció de polígons regulars (el teorema de Gauss explicat en el treball 2 d'aquest seminari) es troben a §365,366 del llibre "Disquisions Aritmètiques", llibre de C.F. Gauss dedicat a la que ell considera la reina de les matemàtiques: "la teoria de nombres".(Hi ha la versió en català d'aquest llibre de Gauss per Griselda Pasqual, editat per la Societat Catalana de Matemàtiques)

Cal dir que Gauss no va explicitar la construcció amb regle i compàs del polígon regular en 17 costats. El primer en explicitar-ho va esser Erchinger al voltant de l'any 1800. Una altra de les històries diuen que Gauss en observar la construcció va demanar que la construcció del polígon regular amb regle i compàs fos reproduïda en la seva làpida.

El vostre treball consisteix en:
1) trobar $Irr(cos(\frac{2\pi}{17}), \mathbb{Q})[x]$, i obtenir l'expressió de Gauss per $cos(\frac{2\pi}{17})$ de l'equació (B.1),
2) trobar extensions de cossos M_i amb $[M_i : M_{i-1}] = 2$ que justifiquin que és construïble amb regle i compàs el polígon regular de 17 costats,
3) i usar aquestes extensions de grau 2 per a donar una construcció amb regle i compàs per a la construcció del heptadecàgon regular.

[Referències: Per a obtenir l'expressió donada per Gauss, i calcular $Irr(cos(2\pi/17), \mathbb{Q})[X]$ consulteu per exemple:
"Constructibility of Regular Polygons", Eric T. Eekhoff, Iowa State University, pages 9-13.

Després d'haver obtingut l'expressió de Gauss donada per la fórmula (B.1), per a la construcció de cossos intermedis de grau 2 i una construcció amb

regle i compàs, suggerim la construcció següent donada per Linn Smith (1920):
Denotem per $z_1 = 2cos(2\pi/17)$, és l'arrel més gran (ambdues són a $\mathbb{R}$) de l'equació:

$$Z^2 - y_1 Z + y_4 = 0$$

on y_1 és l'arrel més gran de l'equació (ambdues arrels són reals):

$$Y^2 - x_1 Y - 1 = 0$$

i y_4 és l'arrel més gran de l'equació:

$$Y^2 - x_2 Y - 1 = 0;$$

on x_1 i x_2 són arrels reals amb $x_1 > x_2$ de l'equació:

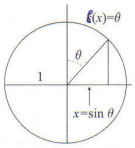
$$X^2 + X - 4 = 0.$$

Un cop comprovat, fixeu-vos que les arrels de $W^2 - aW + b = 0$ d'un polinomi de grau 2 s'obtenen intersecant l'eix OX amb la circumferència construïda de la forma següent: tenim els punts que hem de suposar construïbles (a, b) i $(0, 1)$, considereu $P = (a/2, (b+1)/2)$, la circumferència buscada és la que té centre P i que passa per (a, b) i $(0, 1)$. Si necessiteu més detalls consulteu: "A construction of the regular polygon of seventeen sides" de L.Lynn Smith, Amer. Math. Monthly 27 (1920), no. 7-9, pp. 322-323.]

La lemniscata de Bernouilli.
Aquest apartat és totalment divulgatiu i tan sols de caire informatiu.

Comencem parlant primer de la circumferència.

Considerem $x^2 + y^2 = 1$ i sigui $l_{OX}(x)$ la longitud de l'arc del primer quadrant de la circumferència que s'obté de recorre de 0 fins x amb $x \in [0, 1]$ (és a dir la longitud de la circumferència d'anar del punt $(0, 1)$ al punt $(x, \sqrt{1-x^2})$), igualment $l_{angle}(\theta)$ la longitud de l'arc d'un angle θ format a partir del punt $(0, 1)$ en el sentit de les agulles del rellotge, és a dir entre el punt $(0, 1)$ a $(\sin(\theta), \cos(\theta)) = (x, \sqrt{1-x^2})$ amb θ angle expressat en radiants sobre la circumferència (fixeu-vos que aquesta no és la noció estàndard de definició del sinus i cosinus).



Recordeu $l_{angle}(1) = 1$ (aquesta és la definició de radiant) i per tant $l_{angle}(\theta) = \theta$.

Anem a fer una mica d'anàlisi i geometria diferencial, anem a trobar $l_{OX}(x)$. La fórmula per la diferencial d'arc és $dl^2 = dx^2 + dy^2$ i per la circumferència d'equació $x^2 + y^2 = 1$ obtenim $dl = \frac{dx}{\sqrt{1-x^2}}$, d'on

$$l_{OX}(x) = \int_0^x \frac{dt}{\sqrt{1-t^2}},$$

és monòtona creixent en l'interval $[0,1]$, per tant té una funció inversa φ on

$$\alpha = \int_0^{\varphi(\alpha)} \frac{dt}{\sqrt{1-t^2}},$$

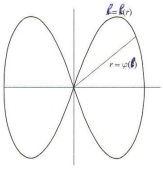
fixeu-vos però que aquesta φ és la funció sin, efectivament, $l_{OX}(x) = \theta$ on θ és l'angle en radiants recorregut entre el punt $(0,1)$ a $(x, \sqrt{1-x^2})$, per tant $x = \sin(\theta)$, d'on obtenim:

$$\theta = \int_0^{\sin(\theta)} \frac{dt}{\sqrt{1-t^2}}.$$

Observem que $l_{OX}(1) = \pi/2 = \int_0^1 \frac{dt}{\sqrt{1-t^2}}$, és la longitud de l'arc de la circumferència en el primer quadrant i és un nombre transcendent.
Per a construir l'$n-$àgon regular en la circumferència, hem de calcular el $\sin(\frac{2\pi}{n})$, volem una longitud d'arc de magnitud $2\pi/n$. Aquest resultat equival a estudiar el cos $\mathbb{Q}(e^{2\pi i/n})$ on $e^{2\pi i/n}$ són elements de torsió de $\mathbb{C}^*$, i usant teoria de Galois estudiar el grup $Aut_{\mathbb{Q}}(\mathbb{Q}(e^{2\pi i/n}))$ que és abelià.

Anem a la lemniscata. L'equació de la lemniscata presentada per Jacob Bernouilli té per equació:

$$(x^2+y^2)^2 = x^2 - y^2$$



En coordenades polars $x = r\cos(\theta)$, $y = r\sin(\theta)$ l'equació $(x^2+y^2)^2 = x^2-y^2$ s'escriu per $r^2 = \cos(2\theta)$.

Sigui $l_{OX}(x)$ la longitud de l'arc en el pètal de la dreta i part superior de la lemniscata entre 0 fins x amb $x \leq 1$. La fórmula de diferencial d'arc és:

$$dl^2 = dx^2 + dy^2 = dr^2 + r^2 d\theta^2 = \frac{dr^2}{1-r^4}$$

obtenint

$$l(r) = \int_0^r \frac{dt}{\sqrt{1-t^4}}$$

on $l(r)$ és la longitut d'arc de la lemniscata començant a (0,0) fins el punt de la fulla de la dreta i superior de la lemniscata que és troba a distància r del $(0,0)$. Com $r^2 = cos(2\theta)$ tenim $0 \leq r \leq 1$.

Denotem ara per ω la longitud d'un pètal de la lemniscata (pel cas de la circumferència aquest valor és π), obtenim:

$$\frac{\omega}{2} = \int_0^1 \frac{dt}{\sqrt{1-t^4}},$$

es pot demostrar que ω és un nombre trascendent, demostrat primerament per Theodor Schneider (1937).

Qüestió: Volem construir longituds d'arc $2\omega/n$ (de forma similar com en el cas de la circumferència amb $2\pi/n$, però ara amb l'arc donat per la lemniscata). Per a quins n és possible?

Observem primer que $l(r)$ és monòtona creixent a l'interval $[0,1]$ i per tant es pot invertir, diem $r=\varphi(l)$ la seva inversa obtenim:

$$s=\int_0^{\varphi(s)}\frac{dt}{\sqrt{1-t^4}}$$

aquesta φ s'anomena el sinus lemniscàtic.
Denotem per $\varphi=\text{sinlem}$ ara. Hem d'estudiar la construcció amb regle i compàs per $\text{sinlem}\,(2\omega/n)$.
Per fer això necessitem anàlisi en variable complexa: sinlem s'estén a una tipus de funció en variable complexa $\text{sinlem}:\mathbb{C}\to\mathbb{C}$ i destaquem que és periòdica amb ret $\Lambda=<(1+i)\omega,(1-i)\omega>$, és a dir $\text{sinlem}\,(\alpha+\gamma)=\text{sinlem}\,(\alpha)$ per $\gamma\in\Lambda$. Aquest fet és relaciona amb el que es diu corbes el.líptiques: $\mathbb{C}/\Lambda$, que topològicament és un donut, i la construcció del sinus lemniscàtic $2\omega/n$ es trasllada a l'estudi de punts de torsió de la corba el.líptica $\mathbb{C}/\Lambda$. Aquests punts de torsió donen extensions abelianes (extensions amb grups d'automorfismes un grup abelià, les quals són més fàcil el seu estudi) sobre un cos provinent d'una certa extensió d'un cos quadratic imaginari ($\mathbb{Q}(\sqrt{D})$ amb $D<0$ són els cossos quadratics imaginaris) si la corba el.líptica és molt particular "multiplicació complexa" però la corba el.líptica que surt per la lemniscata de la xarxa Λ és de "multiplicació complexa", això permet obtenir per Abel(1828)

Teorema B.1.3 (Abel, 1828)**.** *Si n és una potència de 2 per primers de Fermat diferents la lemniscata es pot dividir en n parts iguals.*

I finalment el fet que entenen molt bé les extensions abelianes sobre un cos quadràtic imaginari en Rosen l'any 1981 va demostrar el recíproc:

Teorema B.1.4 (Rosen, 1981)**.** *La lemniscata es pot dividir en n parts iguals si i només si n és una potència de 2 per primers de Fermat diferents.*

Comentar per completitud el següents resultats

Teorema B.1.5 (Weber)**.** *Tota extensió finita L de $\mathbb{Q}$ on L és cos de descomposició d'un polinomi sobre Q amb $Aut_{\mathbb{Q}}(L)$ un grup abelià es té que $L\subseteq\mathbb{Q}(e^{2\pi i/n})$ per a cert n.*

Teorema B.1.6. *Tota extensió finita L de K on L és cos de descomposició d'un polinomi sobre K amb $K=\mathbb{Q}(\sqrt{D})$ amb $D<0$ lliure de quadrats amb $Aut_K(L)$ un grup abelià llavors existeix una corba el.líptica E amb multiplicació complexa on $L\subseteq K(j,torsio(E))$ on j és un invariant modular de la corba el.líptica i del cos K i $torsio(E)$ són punts de torsió de la corba el.líptica.*

[Referència: per un article més detallat consulteu: "Gauss i els polígons" de Joan Carles Lario, membre del Seminari de Teoria de Nombres UAB-UB-UPC. Comentar que per una millor comprensió cal saber una mica sobre corbes el.líptiques i geometria algebraica, "la" referència és: J.Silverman "The Arithmetic of Elliptic Curves", GTM 106, Springer.]

B.2 Construcció usant plecs en paper: origami

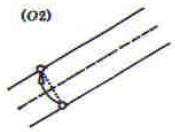
Anem a explicitar certes operacions que podem fer sobre un plà (pensarem també un paper quadrat) que ens permeten construir longituds reals, longituds que direm que són construïbles amb origami (corresponen a la longitud entre dos punts construïbles amb origami).

L'axiomàtica per la construcció de punts construïbles amb origami és la següent: partim de dos punts 0 i 1 (o millor diem-los $(0,0)$ i $(1,0)$, i construïm els següents per iteració dels següents axiomes:

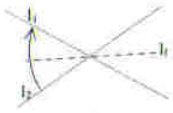
(i) la recta que es forma unint dos punts construïbles direm que és una recta construïble (en origami),

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

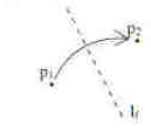
(iii) donades dos rectes paral.leles construïbles, podem construir la recta paral.lela ambdues i equidistant amb elles,



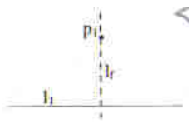
(iv) donades dues rectes construïbles, defineixen un angle, aquest angle es pot biseccionar, és dir podem construir la recta que bisecciona l'angle,



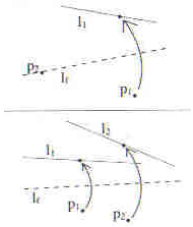
(v) donats dos punts construïbles P i Q diferents, podem construir la recta perpendicular a la recta formada pels dos punts P i Q de manera que el punt de tall d'ambdues rectes és el punt mig del segment PQ,



(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 (possiblement iguals) i dos punts construïbles P_1 i P_2 (possiblement iguals) un pot construir la recta que simultàniament reflexa P_1 en l_1 i P_2 en l_2,



(observeu 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, repasseu propietats de la paràbola).

Per parlar de nombres reals construïbles en origami, volem dir els punts construïbles en origami en l'eix OX, és dir de la forma $(\alpha, 0)$. Per fer-ho acceptarem aquests dos axiomes:

a) donat un segment entre dos punts construíbles 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,

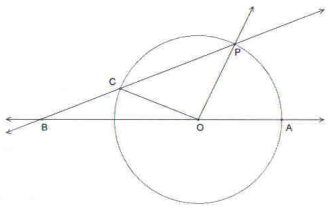
b) podem portar un angle a qualsevol punt P construïble on hi tenim una recta construïble pel punt P.

Denotarem per $\mathcal{M}$ el conjunt de tots els nombres reals construïbles amb origami. Es demostra que és un cos, i es caracteritza de forma similar al cas de construcció amb regle i compàs amb $[K_i : K_{i-1}] \leq 3$ enlloc de 2. Veieu treballs 5 i 6.

(Tr4) **Treball 4** Dos dels problemes clàssics de l'antiga civilització grega van ser: la duplicació del cub (també anomenat problema de Delion), i la trisecció de l'angle. És a dir construcció amb regle i compàs la longitud $\sqrt[3]{2}$ i el $\cos(\theta/3)$ (recordeu la fórmula de les raons trigonomètriques de l'angle triple en funció de les raons trigonomètrics de l'angle).
La primera feina és demostrar que és impossible la duplicació del cub i la trisecció de l'angle amb regle i compàs.

[Referèencia: qualsevol llibre de Teoria de Galois, per exemple el llibre de'n Garling "Galois Theory", que teniu a la bibliografia de l'assignatura.]

Arquimedes, va trobar una construcció per la trisecció d'un angle de la



forma següent:

inscriguem θ dins una circumferència de radi ℓ on θ l'angle que forma OP i OA, tenim que $\theta/3$ és l'angle format per BC i BO on BC és construït de forma que té longitud ℓ.

La segona feina d'aquest treball és: expliciteu aquesta construcció a classe, justificant la construcció, i veieu que no és una construcció amb regle i compàs.

[Observació: necessiteu un regle marcat!! Si teniu interés per construccions amb compàs i regle marcat, us aconsellem la lectura del següent treball: Arthur Baragar, "Constructions using a compass and twice-notched straightedge" en The American Mathematical Monthly, vol. 109, No.2, (Feb.2002), pp.151-164.]

Considerem finalment construccions amb els axiomes d'origami descrits anteriorment.
La tercera feina és exposar construccions geomètriques (gràfiques) en origami per tal de fer la duplicació del cub i la trisecció de l'angle en plecs de paper, justificant el resultat.

[Referència: Robert J. Lang, "Origami and geometric constructions", el trobeu en
http://www.langorigami.com/]

(Tr5) **Treball 5(*)** En l'article "Euclidean constructions and the geometry of Origami" el professor Geretschläger demostra en el teorema 1 d'aquest article que totes les construccions amb regle i compàs són construïbles en origami, acceptem aquest resultat pel que segueix. El vostre treball consisteix en demostrar de forma algebraica que amb origami un pot construir una arrel de qualsevol polinomi de grau 3 definit sobre un cos format per elements construïbles amb origami i aquest grau 3 és el màxim possible que podeu aconseguir per l'axiomàtica en origami en fer-ne un pas dels axiomes en la construcció d'un punt d'origami a partir d'uns de ja construïts via origami.

[Referència: capítol 6 i 7 de l'article de'n Geretschläger "Euclidean constructions and the geometry of origamy", Mathematics Magazine, vol.68, No.5, (Dec.1995), pp.357-371.]

(Tr6) **Treball 6** En l'anterior treball ja teniu els preliminars (useu el treball 5) per a demostrar seguint la demostració de teoria feta per construccions amb regle i compàs del següent resultat:

Teorema B.2.1 (Geretschläger-Emert-Meeks-Nelson)**.** *Un punt $x \in \mathbb{R}$ és construïble en origami si i només si existeixen una torre de cossos $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ amb $x \in K_n$ i $[K_i : K_{i-1}] \leq 3$*

Finalment useu el treball 1 per tal de demostrar un anàleg del teorema de Gauss per a polígons regulars usant origami:

Teorema B.2.2 (Emert-Meeks-Nelson)**.** *Si el polígon regular d'n costats és construïble amb origami llavors $n = 2^s 3^r$ o bé $n = 2^s 3^r \tilde{p}_1 \cdot \ldots \tilde{p}_\ell$ on $s, r \in \mathbb{N}$ i $\tilde{p}_i$ són primers de Pierpont diferents.*

Recordem que un primer és de Pierpont si és un primer de la forma $2^\mu 3^\alpha + 1$ amb $\mu, \alpha \in \mathbb{N}$. Per tant en origami si que podem fer la construcció exacta del heptagon regular!!!!

[Referències: Robert Geretschläger: "Euclidean constructions and the geometry of origamy", Mathematics Magazine, vol.68, No.5, (Dec.1995), pp.357-371.
John W. Emert, Kay I. Meeks, Roger B. Nelson:"Reflections on Mira", The American Mathematical Monthly, vol.101, No.6, (Jun-Jul, 1994), pp.544-549.
Roger C. Alperin, "A mathematical theory of origami constructions and numbers".]

Appendix C

Nocions en Teoria de grups

En aquest apendix expossarem alguns resultats bàsics de teoria de grups algun d'ells potser ja expossats en cursos anteriors. Comencem recordant algunes nocions preliminars de grups ja conegudes;

Definició C.0.3. *Un grup és un conjunt G, no buit, junt amb una operació $*$ complint la propietat associativa, l'existència de l'element neutre (anomenem-lo e) i l'existència de l'element invers per l'operació $*$, (donat $g \in G$ anomenem aquest invers per g^{-1}, ja que fàcilment es demostra la unicitat de l'invers).*
Si a més $*$ compleix la propietat commutativa, diem que $(G, *)$ és un grup abelià o commutatiu.

Alguns exemples de grups són $(\mathbb{Z}, +)$ i $(S_n, \circ)$ les permutacions; recordem que S_n denota les aplicacions bijectives del conjunt $\{1, \ldots, n\}$.

Definició C.0.4. *Un subgrup d'un grup $(G, *)$ és un subconjunt H de G tal que $(H, *)$ és un grup, en particular $h_1 * h_2 \in H$ $\forall h_i \in H$.*

És fàcil demostrar

Lema C.0.5. *Sigui $(G, *)$ un grup i H un subconjunt de G. Llavors són equivalents:*

1. *H és un subgrup de G*
2. *es compleix $e \in H$, $\forall g \in H \Rightarrow g^{-1} \in H$, i $\forall g_1, g_2 \in H \Rightarrow g_1 * g_2 \in H$*
3. *$H \neq \emptyset$ i $\forall g_1, g_2 \in H \Rightarrow g_1 * g_2^{-1} \in H$.*

Normalment quan $*$ se sobreenten escriurem G enlloc de $(G, *)$. Igualment per H un subgrup de G ho escriurem per $H \leq G$. Donat $H \leq G$ i $g, g_2 \in G$ denotem per Hg,gH i g_2Hg els següents subconjunts de G: $Hg := \{h*g | h \in H\}$, $gH := \{g * h | h \in H\}$ i $g_2Hg := \{g_2 * h * g | h \in H\}$. Si $H_1, H_2 \leq G$ sigui $H_1H_2 := \{h_1 * h_2 | h_i \in H_i\}$ que és un subconjunt de G que conté H_1 i H_2.

Lema C.0.6. *G un grup i $H \leq G$. Les relacions binàries següents:*

1. *$g_1 \sim_d g_2$ si i només si $g_1 * g_2^{-1} \in H$*
2. *$g_1 \sim_e g_2$ si i només si $g_2^{-1} * g_1 \in H$*

són d'equivalència. Les $\sim_d$-classes d'equivalència són $Hg = \{h * g \in G | h \in H\}$ anomenades classes a la dreta de G mòdul H. Les $\sim_e$–classes d'equivalència són $gH = \{g * h \in G | h \in H\}$ anomenades classes a l'esquerra de G mòdul H. (Recordeu que dues classes laterals esquerra o bé són disjuntes o la mateixa, i G és unió de classes laterals esquerra, similarment per la dreta).

Definició C.0.7. *Sigui N un subgrup de G, $N \leq G$. Diem que N és un subgrup normal de si $g^{-1} * n * g \in N$ $\forall g \in G$ i $\forall n \in N$. En aquesta situació escriurem també $N \lhd G$.*

Recordem que tot subgrup d'un grup commutatiu és normal. És fàcil demostrar:

Lema C.0.8. *Un subgrup N de G és normal si i només si $gN = Ng$ $\forall g \in G$, on recordeu $gN := \{g * n | n \in N\}$ i $Ng := \{n * g | n \in N\}$.*

Lema C.0.9. *Si $N \lhd G$, definim $G/N := \{gN | g \in G\}$. Definim l'operació $g_1N \cdot g_2N := (g_1 * g_2)N$ $\forall g_1, g_2 \in G$, la qual està ben definida. Llavors $(G/N, \cdot)$ és un grup que anotarem per abús de notació G/N.*

Donat un grup $(G, *)$ i un element $g \in G$ denotem per $< g >_{\geq 1} := \{g^n | n \in \mathbb{N}_{geq1}\} \cup \{e\}$ on $g^2 = g * g$, $g^3 = g * g * g$,... És fàcil veure que si existeix $n \geq 1$ on $g^n = e$ llavors $< g >_{\geq 1} \leq G$ i el natural positiu més petit complint $g^n = e$ s'anomena l'**ordre de g en G**, aquest natural sempre existeix quan G és un grup finit. Altrament denotem

$$< g > := \{g^n | n \in \mathbb{Z} \setminus \{0\}\} \cup \{e\} \leq G$$

i si g té ordre tenim $< g > = < g >_{\geq 1}$.
Diem que G és un grup **cíclic** si existeix $g \in G$ on $G = < g >$.

Definició C.0.10. *Donats dos grups $(G_1, *)$ i $(G_2, \cdot)$, una aplicació $f : G_1 \to G_2$ diem que és un homomorfisme o morfisme de grups si conserva l'operació de grup, és a dir*

$$\forall \ell_1, \ell_2 \in G_1, \ f(\ell_1 * \ell_2) = f(\ell_1) \cdot f(\ell_2).$$

Un morfisme de grups es diu monomorfisme si és injectiu; epimorfisme, si és exhaustiu, i isomorfisme, si és bijectiu. Un morfisme d'un grup $(G, *)$ amb ell mateix s'anomena endomorfisme de $(G, *)$. Un endomorfisme bijectiu s'anomena automorfisme.

Donem un parell d'exemples de morfismes de grups:
(1) Si $H \leq G$ l'inclusió $\iota : H \to G$ donada per $\iota(h) = h$ $\forall h \in H$, és monomorfisme.
(2) Si $N \lhd G$, la projecció $proj : G \to G/N$ definida per $proj(g) = gN$ és epimorfisme.

Lema C.0.11. *Sigui $f : G_1 \to G_2$ un morfisme de grups. Llavors,*

1. *$Im(f) := \{f(g_1) | g_1 \in G_1\}$ és un subgrup de G_2, on $Img(f)$ s'anomena la imatge de f.*
2. *$Ker(f) := \{g_1 \in G_1 | f(g_1) = e\} \lhd G_1$, on $ker(f)$ s'anomena el nucli de f.*

Recordem que tenim el següent resultat,

Teorema C.0.12 (d'isomorfisme)**.** *Sigui $f : G_1 \to G_2$ morfisme de grups. Llavors existeix un isomorfisme overline$f : G_1/Ker(f) \to Im(f)$ mitjançant $\overline{f}(gKer(f)) := f(g)$ $\forall g \in G_1$ (després de comprovar que està ben definit).*

Definició C.0.13. *Diem que dos grups $(G_1, *)$ $(G_2, \cdot)$ són isomorfs si existeix un isomorfisme entre ells. Escriurem $(G_1, *) \cong (G_2, \cdot)$ o bé $G_1 \cong G_2$ si les operacions són conegudes en el context que treballem.*

Volem fer un estudi de classificació de grups.

Definició C.0.14. *Sigui G un grup. Denotem per $|G|$ el nombre d'elements d'aquest grup en cas de ser finit i pel simbol ∞ en cas contrari; $|G|$ l'anomenarem l'ordre del grup G.*

Ens preguntem: quants grups d'ordre 6 hi ha, identificant els grups isomorfs entre ells? Igualment per a qualsevol $n \in \mathbb{N}$ podem preguntar-nos quants grups hi ha llevat d'isomorfisme d'ordre exactament n? Aquesta pregunta la treballareu per grups d'ordre petit en aquest seminari.

Fixeu-vos que dos grups isomorfs G_1, G_2 via un isomorfisme $f : G_1 \to G_2$ porta subgrups de G_1 a subgrups G_2, i porta subgrups l'ordre α a subgrups d'ordre α.

És fàcil demostrar que si G és finit G té un nombre finit de subgrups diferents (recordeu que tot conjunt finit tan sols té un nombre finit de subconjunts).

Definició C.0.15. *Sigui G un grup finit. Sigui $\mathcal{C} := \{H_0 = \{e\}, H_1, \ldots, H_s = G\}$ la llista (finita) de tots els subgrups diferents de G. Dibuixem el següent graf, per a cada subgrup li fem correspondre un punt, i si tenim $H_i \leq H_j$ amb $i \neq j$ i a més exigim que no existeix cap $k \neq j$ complint $H_i \leq H_k \leq H_j$ dibuixen una aresta del punt corresponent a H_i al H_j. Usualment dibuixarem el graf possant de baix a dalt els subgrups de menor a major ordre. Aquest graf l'anomenarem el reticle del grup G.*

Dibuixem el reticle del grup S_3. És un exercici demostrar que els únics subgrups són $\{\{id\}, S_3, < (1,2) >, < (1,3) >, < (2,3) >, < (1,2,3) >\}$ i tenim el següent reticle:

2cm

Observació: recordeu que la notació $(a_1, \ldots, a_j)$ d'un element de S_n, és l'apliació $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ on $f(a_i) = a_{i+1}$ per a $i \leq j-1$, $f(a_j) = a_1$ i $f(b) = b$ $\forall b \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_j\}$.

C.1 Primer Treball: propietats bàsiques, grups abelians, reticles grups d'ordre petit i abelians.

Primer consisteix en demostrar els teoremes de Noether següents:

Teorema C.1.1 (Noether)**.** *Sigui G un grup, $N_1 \lhd G$, $N_2 \lhd G$ amb $N_1 \subseteq N_2$. Llavors,*

$$(G/N_1)/(N_2/N_1) \cong G/N_2.$$

Definició C.1.2. *Sigui $H \leq G$, definim el normalitzador de H en G per*

$$N_G(H) := \{g \in G | g^{-1}Hg = H\}.$$

Comproveu que $N_G(H) \leq G$ i $H \lhd N_G(H)$.

Teorema C.1.3 (Noether)**.** *Sigui G grup, $H_1 \leq G$, $H_2 \leq G$ amb $H_1 \subseteq N_G(H_2)$. Llavors $H_1H_2 = H_2H_1$ és un subgrup de G, $H_2 \lhd H_1$, $H_1 \cap H_2 \lhd H_1$ i a més*

$$(H_1H_2)/H_2 \cong H_1/(H_1 \cap H_2).$$

Tot seguit recordarem

Teorema C.1.4 (de Lagrange)**.** *Sigui H un subgrup d'un grup finit G. Llavors $|H|$ divideix $|G|$,*

(repaseu la demostració, tot i que no cal expossar-la en públic) i recordeu la definició d'índex,

Definició C.1.5. *Sigui G un grup finit, $H \leq G$, l' índex de H en G denotat per $(G : H)$ és el nombre natural $|G|/|H|$.*

Volem estudiar per indexs petits quan els subgrups són normals o no.

Definició C.1.6. *Definim el cor normal d'un subgrup H de G per $cor_G(H) := \cap_{g \in G} g^{-1}Hg$.*

Demostreu,

Proposició C.1.7. *Donat H un subgrup d'un grup G, tenim les següents propietats:*

1. *$cor_G(H) \lhd G$ i $cor_G(H) \leq H$.*
2. *Si G finit amb $(G : H) = n$ es té $(G : cor_G(H))|n!$.* [*1].
3. *Si G és finit i p és el primer més petit que divideix $|G|$ llavors tot subgrup d'índex p de G és un subgrup normal de G.*

Observeu que com a corol.lari immediat de la proposició tenim que tot subgrup d'índex 2 d'un grup finit G és un subgrup normal.

Recordem la noció de finit generat,

Definició C.1.8. *Un grup G s'anomena finit generat (f.g. per simplificar) si existeixen un nombre finit d'elements $g_1, \ldots, g_k \in G$ complint que qualsevol $g \in G$ s'escriu com un producte finit de $\{g_1, \ldots, g_k\} \cup \{g_1^{-1}, \ldots, g_k^{-1}\}$ i en cas afirmatiu escriurem $G =< g_1, \ldots, g_k >$.*

Els cursos anteriors de la titulació de Matemàtiques heu demostrat un teorema de classificació de grups abelians finit generats, mòdul d'isomorfisme de grups.
Heu de recordar-ho en la vostra expossició en el seminari (i si teniu temps donar alguna idea de com us el van demostrar),

[1] Indicació per la prova: definiu un morfisme de G en S_n on penseu S_n aquí com les aplicacions bijectives del conjunt $\{H, a_1H, \ldots, a_{n-1}H\}$ de les classes laterals de H en G

Teorema C.1.9 (de classificació de grups abelians f.g.). *Sigui G un grup abelià f.g. Llavors existeixen naturals r, t i naturals $n_i > 1$ amb $n_1|n_2|\ldots|n_t$ complint*

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{t} \mathbb{Z}/(n_i\mathbb{Z}),$$

a més aquests enters r, t, n_i són únics complint aquestes propietats.

Definició C.1.10. *El número r del teorema previ s'anomena el rang del grup abelià G, i els n_i són els factors invariants.*

Podem construir quan $gcd(m, n) = 1$ un isomorfisme,

$$f : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

donat per $[z]_{mn} \mapsto ([z]_m, [z]_n)$ on $[a]_i$ denota la classe de a en $\mathbb{Z}/(i)$. Llavors es pot escriure el teorema anterior mitjançant,

Teorema C.1.11 (de classificació de grups abelians f.g.). *Sigui G un grup abelià f.g. Llavors existeixen naturals r, s, nombres primers diferents $p_1, \ldots, p_s$ i naturals $m_{i,j} \geq 1$ amb $n_1|n_2|\ldots|n_t$ complint*

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \prod_{j=1}^{k_i} \mathbb{Z}/(p_i^{m_{i,j}}\mathbb{Z}),$$

a més aquesta descomposició és única llevat d'ordre dels factors, els nombres $p_i^{m_i}$ s'anomenen divisors elementals de G.

Cal dir que hi ha grups abelians que no són finit generats. Doneu els exemples: $\mathbb{Q}$ i $\mathbb{Q}/\mathbb{Z}$ tot justificant-ho.

Finalment heu de donar el reticles de grups abelians d'ordre ≤ 20, explicitant la metodogia que heu fet servir.

[Bibliografia: qualsevol llibre d'Àlgebra amb un capítol de teoria de grups, i/o qualsevol llibre de Teoria de grups.]

C.2 Segon Treball: grups de permutació, teorema de Cayley. Grups simples. A_n és simple per $n \geq 5$

.

Recordarem diferents notacions per elements del grup de permutacions S_n. Cal introduir cicles de longitud r, noció de cicles disjunts, noció de transposició, i demostrar que tota permutació $\sigma \in S_n$ és producte de cicles disjunts dos a dos i demostrar que aquesta descomposició en cicles disjunts és única llevat ordre dels factors.

Definiu el signe d'una permutació $\sigma \in S_n$ i recordarem el morfisme de grups signe

$$signe : S_n \to \{1, -1\}$$

on el nucli s'anomena el grup alternat de grau n que denotarem per A_n, subgrup d'´índex 2 amb S_n i per tant $A_n \lhd S_n$. Doneu un petit criteri de càlcul de $signe(\sigma)$ quan σ és producte de cicles disjunts i de transposicions.

Sigui G un grup finit demostreu el teorema de Cayley:

Teorema C.2.1 (Cayley)**.** *Donat un grup finit G d'ordre n sempre existeix un monomorfisme de grups $G \to S_n$, per tant tot grup G és un subgrup d'un grup de permutacions.*

Definició C.2.2. *Un grup G és simple si $G \neq \{e\}$ i els únics subgrups normals de G són $\{e\}$ i G.*

Si G és abelià i finit, per tal de ser simple ha de ser cíclic d'ordre pimer.

Feu el reticle de grups per a S_3, A_3, S_4 i A_4.

La feina principal d'aquest treball consiteix en demostrar:

Teorema C.2.3. *El grup A_n és simple per a $n \geq 5$.*

Per a demostrar-ho heu de treballar molt bé amb els elements del grup A_n en particular un sistema de generadors i que significa que existis un subgrup normal a A_n.

Bibliografia: Pel teorema anterior, qualsevol llibre de Teoria de Galois, per exemple el Garling. Pels altres resultats, veieu apunts de cursos d'Àlgebra d'altres anys o bé consulteu qualsevol llibre d'Àlgebra bàsica.

C.3 Tercer Treball: Teoremes de Sylow

Aquest treball consisteix en demostrar el teorema de Sylow, on en l'expossició oral pot reduir-se tan sols a demostrar-ne el primer apartat. També demostrar el teorema de Cauchy i una aplicació a grups de cert ordre. Anem a detallar-ho,

Definició C.3.1. *Sigui G un grup finit. Sigui p un primer on $|G| = p^k m$ amb $mcd(k, m) = 1$. Un p-subgrup de Sylow de G és un subgrup H de G d'ordre exactament p^k.*

Teorema C.3.2 (de Sylow)**.** *Sigui G un grup finit d'ordre $p^k m$ amb $mcd(m, p) = 1$. Llavors:*

1. *existeix un p-subgrup de Sylow de G*
2. *tot subgrup de G d'ordre p^r amb $0 \leq r \leq k$ està inclòs en un p-subgrup de Sylow de G,*
3. *els p-subgrups de Sylow de G són conjugats, és a dir, si H_1, H_2 són dos p-subgrups de Sylow de G, llavors $\exists g \in G$ complint $H_1 = gH_2g^{-1}$,*
4. *si n_p designa al nombre total de p-subgrups de Sylow de G, es té $n_p \equiv 1(mod\ p)$ i $n_p | m$.*

després de demostrar-ho com a aplicacions demostrareu,

Corol·lari C.3.3 (Teorema de Cauchy)**.** *Sigui G un grup finit, i p primer complint $p||G|$. Llavors G té algun element d'ordre p.*

i també demostreu de forma teòrica (usant els teoremes de Sylow) que tot grup d'ordre 15 és abelià i cíclic, i que un grup d'ordre 42 no pot ser simple (veieu definició de grup simple en el treball anterior).

[Bibliografia: qualsevol llibre d'Àlgebra amb un capítol complert de teoria de grups, o qualsevol llibre inicial de Teoria de grups.]

C.4 Quart Treball: p-groups, grups resolubles

En aquest treball estudiarem la noció de resolubilitat (introduida la seva idea per Galois en demostrar la impossibilitat de l'equació genèrica per un polinomi de grau ≥ 5, com veurem a classe de teoria molt més endavant). Treballarem en dos tipus de grups que compleixen la propietat de resolubilitat: p-grups i grups nilpotents.

G sempre és un grup finit en aquest treball d'aquest seminari.

Definició C.4.1. *Donat un grup finit G, diem que G és un p-grup si i només si el seu ordre és una potència de p.*

El primer a demostrar és el següent resultat,

Lema C.4.2. *Donat G llavors el centre de G: $Z(G) := \{h \in G | h*g = g*h, \forall g \in G\}$ és un subgrup normal de G. Si G és un p-grup es té que $p||Z(G)|$, és a dir el centre d'un p-grup té elements diferents de l'element neutre del grup G.*

Calculeu explícitamet el centre, per tots els grups d'ordre 8 elements (llevat d'isomorfisme), i observeu que si G és abelià és clar que $Z(G) = G$.
Demostreu tot seguit,

Lema C.4.3. *Sigui G un p-grup G (finit) d'ordre p^n. Llavors G té subgrups normal d'ordre p^i per a qualsevol natural i complint $0 \leq i \leq n$, en particular G té un subgrup normal d'índex p.*

(Com indicació de la prova: observeu $Z(G)$ és abelià, i $G/Z(G)$ és un p-grup i podem calcular-hi de nou el centre ara al grup $G/Z(G)$).
Com una aplicació a classificació de grups, demostreu:

Lema C.4.4. *Tot grup finit G d'ordre p^2 és abelià.*

En particular els grups finits d'ordre 25 tan sols són isomorfs a $\mathbb{Z}/(5) \times \mathbb{Z}/(5)$ o bé a $\mathbb{Z}/(25)$.
Definirem tot seguit una noció introduïda per Galois (tot i que amb un altre llenguatge) inspirada de la bijecció entre extensions de cossos (de tipus Galois) i la seva analogia en teoria de grups (grup d'automorfisme d'un cos deixant un subcos fix), és la noció de grup resoluble:

Definició C.4.5. *Un grup finit G s'anomena resoluble si existeix una cadena de subgrups H_i de G amb $0 \leq i \leq n$ complint:*

1. *$H_0 = \{e\}$ i $H_n = G$,*

2. $H_i \lhd H_{i+1}$ *per* $i = 0, \ldots, n-1$,

3. H_{i+1}/H_i *és un grup abelià per* $i = 0, \ldots, n-1$.

La cadena $H_0 \leq H_1 \leq \ldots \leq H_n = G$ *direm que és una cadena resoluble per a* G.

Demostreu en el seminari que A_n i S_n per $n \geq 5$ no són resolubles (podeu usar que el grup del segon treball d'aquest seminari ha demostrat que A_n és simple per $n \geq 5$). Doneu una cadena resoluble per a S_4 i S_3.
Demostreu que la condició d'abelià en l'anterior definició de grup resoluble pot ser substituïda per cíclic, és a dir, demostreu:

Lema C.4.6. *G és resoluble si i només si una cadena de subgrups H_i de G amb $0 \leq i \leq m$ complint:*

1. $H_0 = \{e\}$ *i* $H_m = G$,

2. $H_i \lhd H_{i+1}$ *per* $i = 0, \ldots, m-1$,

3. H_{i+1}/H_i *és un grup cíclic per* $i = 0, \ldots, m-1$.

Finalment demostreu,

Proposició C.4.7. *Tot p-grup G és resoluble.*

(Indicació: useu la propietat del centre no trivial per anar obtenint la cadena resoluble, observeu primer $Z(G) \leq G$, si $G/Z(G)$ no és abelià té centre no trivial, useu per tal d'obtenir subgrups entre $Z(G)$ i G que permeten obtenir una cadena resoluble).

[Bibliografia: per a p-grups: Leedham-Green, Cr.R. and McKay, S. (2002) The structure of groups of prime power order, vol. 27, London Mathematical Society Monographs, Oxford Univ. Press. També un llibre de Teoria de grups que treballi el concepte de p-grups.]

C.5 Cinqué Treball: Reticle de grups no commutatius d'ordre 6 a 25

.

Hem vist diferents nocions que ens ajuden a estudiar els grups de cert ordre fixat. Inicialment és omplir una taula de mida $n \times n$ per a un grup d'ordre n, usant les propietats de grup, per veure-les mireu la bibliografia. D'aquesta forma podem dibuixar el reticle. Potser usant els teoremes de Sylow, resultats en p-grups, i altres podem ajudar-nos a simplificar-ho en alguns casos.

En aquest treball heu de donar reticles de grups pels grups d'ordre n amb $7 \leq n \leq 25$ via isomorfisme (els d'ordre menor o igual a 6 ja s'ha fet en el primer treball de seminari).
En la expossició doneu alguns exemples destacats de com ho heu calculat.
[Bibliografia: Atlas of finite groups: 20-A-27,20-A-11,20-A-29.]

C.6 Sissé apartat: Presentació de grups: generadors i relacions

Aquest apartat és divulgatiu, i tan sols s'expossa per a completitut del seminari en teoria de grups i segurament pot ser útil en altres assignatures com Topologia, o potser realitzant algun dels treballs anteriors trobeu aquesta noció en treballar en certs grups específics.

Una metodologia per a definir un grup és per una *presentació*. Anem a detallar-ho una mica.

Definició C.6.1. *Un grup lliure en un conjunt S és un grup on cada element no trivial g del grup s'escriu de forma única com un producte*

$$g = s_1^{a_1} s_2^{a_2} \dots s_j^{a_j}$$

amb j finit, on cada $s_i \in S$ $s_i \neq s_{i+1}$ amb $a_i \in \mathbb{Z} - \{0\}$ on l'element neutre és representa com triar cap element del conjunt S, equivalentment g s'escriu com a producte finit dels elements de S de forma única llevat de cancelacions consecutives d'un element de S pel seu invers. Denotem per F_S el grup lliure donat per S.

Per exemple si $|S| = 1$, $S = \{a\}$ tenim $F_{\{a\}} = \{a^n | n \in \mathbb{Z} - \{0\}\} \cup \{e = aa^{-1}\}$ que és isomorf a $(\mathbb{Z}, +)$.
Per exemple el grup cíclic $\mathbb{Z}/(n)$ no és lliure ja que $n[1] = [0] = [e]$.
Observeu que si $|S| \geq 2$ F_S és no abelià.

Definició C.6.2. *Donat un conjunt S les expressions $s_1^{b_1} s_2^{b_2} \dots s_j^{b_j}$ amb $s_i \in S$ i $b_j \in \mathbb{Z} - \{0\}$ les anomenarem paraules del conjunt S. Clarament tot element de F_S és una paraula en el conjunt S.*

Destaquem algunes propietats de grups lliures:

Teorema C.6.3. *Considerem S i T dos conjunts finits. $F_S \cong F_T$ si i només si S i T tenen el mateix cardinal.*

Teorema C.6.4 (Nielsen-Schreier)**.** *Tot subgrup d'un grup lliure és lliure.*

Comentar que el rank no ha de baixar del subgrup lliure d'un de lliure. Per a molta més informació: primer capítol Groups acting on graphs de Warren Dicks, M.J. Dunwoody (Dicks és professor del departament).
Anem ara a treballar el cas d'un grup G arbitrari. Denotem per

$$\psi : F_G \to G$$

definit en les paraules d'un element en F_G per $\psi(g) = g$. És fàcil demostrar que és un morfisme de grups exhaustiu. Pel teorema d'isomorfia tenim que $F_G/Ker(\psi) \cong G$, i és clar que els elements de $Ker(\psi)$ està format per paraules de F_G, denotem per R a un conjunt de paraules de F_G que pertanyen a $ker(\psi)$ de forma que generen $Ker(\psi)$ (aquest conjunt R podria tenir un nombre no finit d'elements), llavors escriurem

$$F_G/Ker(\psi) =< G|R >$$

i direm que $< G|R >$ és una presentació pel grup G.

Definició C.6.5. *Donat G un grup, una presentació de G és donar un conjunt S i un subconjunt R de les paraules de F_S anomenades relacions on $G \cong F_S/N$ on N és el subgrup normal més petit de F_S que conté R. Denotem aquesta presentació de G per $< S|R >$. (No confongueu aquesta notació amb la notació de subgrup generat per certs elements!!! tot i que s'anoten de la mateixa forma).*

Hem vist abans que qualsevol grup admet una presentació amb $S = G$, i si G és finit podem triar S un conjunt finit i R un conjunt finit per a donar-ne una presentació.

Donem tot seguit exemples de presentacions de certs grups:

F_S	$< S\|\emptyset >$
$\mathbb{Z}/n$	$< a\|a^n >$
D_{2n}, diedral ordre 2n	$< a, b\|a^n, b^2, (ab)^2 = abab >$
$\mathbb{Z} \times \mathbb{Z}$	$< a, b\|ab = ba >$
$\mathbb{Z}/m \times \mathbb{Z}/n$	$< a, b\|a^m, b^n, ab = ba >$
S_n	$< a_1, \ldots, a_{n-1}\|a_i^2, a_i a_j = a_j a_i \forall j \neq i \pm 1, (a_i a_{i+1})^3 >$