Equacions algebraiques
Curs 2025-2026

UNIVERSITAT DE BARCELONA

Darrera Iliçó

Artur Travesa

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona
28 de maig de 2026

Acabem un curs

De què ha anat aquest curs?

Acabem un curs

De què ha anat aquest curs?

En una primera aproximació, podem dir que aquest curs d'Equacions algebraiques ha estat un curs de Teoria de Galois;

Acabem un curs

De què ha anat aquest curs?

En una primera aproximació, podem dir que aquest curs d'Equacions algebraiques ha estat un curs de Teoria de Galois;

i això, per a molts, vol dir un curs sobre cossos i sobre grups,

Acabem un curs

De què ha anat aquest curs?

En una primera aproximació, podem dir que aquest curs d'Equacions algebraiques ha estat un curs de Teoria de Galois;

i això, per a molts, vol dir un curs sobre cossos i sobre grups,

però també sobre polinomis, anells, ...

Acabem un curs

De què ha anat aquest curs?

En una primera aproximació, podem dir que aquest curs d'Equacions algebraiques ha estat un curs de Teoria de Galois;

i això, per a molts, vol dir un curs sobre cossos i sobre grups,

però també sobre polinomis, anells, ...

Doncs, podríem dir que ha estat un curs d'Àlgebra.

Acabem un curs

De què ha anat aquest curs?

En una primera aproximació, podem dir que aquest curs d'Equacions algebraiques ha estat un curs de Teoria de Galois;

i això, per a molts, vol dir un curs sobre cossos i sobre grups,

però també sobre polinomis, anells, ...

Doncs, podríem dir que ha estat un curs d'Àlgebra.

Però, precisem una mica més?

Acabem un curs (cont.)

També hem fet servir resultats i tècniques que sovint s'associen a altres branques de la Matemàtica.

Acabem un curs (cont.)

També hem fet servir resultats i tècniques que sovint s'associen a altres branques de la Matemàtica.
Per exemple, per a la demostració del *teorema fonamental de l'Àlgebra* hem fet servir el teorema de Bolzano, que sovint s'associa a l'Anàlisi matemàtica.

Acabem un curs (cont.)

També hem fet servir resultats i tècniques que sovint s'associen a altres branques de la Matemàtica.
Per exemple, per a la demostració del *teorema fonamental de l'Àlgebra* hem fet servir el teorema de Bolzano, que sovint s'associa a l'Anàlisi matemàtica.
O per a provar que *tot cos és subcòs d'un cos algebraicament tancat*,

Acabem un curs (cont.)

També hem fet servir resultats i tècniques que sovint s'associen a altres branques de la Matemàtica.
Per exemple, per a la demostració del *teorema fonamental de l'Àlgebra* hem fet servir el teorema de Bolzano, que sovint s'associa a l'Anàlisi matemàtica.
O per a provar que *tot cos és subcòs d'un cos algebraicament tancat*, o que *tota immersió d'un cos en un cos algebraicament tancat es pot estendre a qualsevol extensió algebraica*,

Acabem un curs (cont.)

També hem fet servir resultats i tècniques que sovint s'associen a altres branques de la Matemàtica.
Per exemple, per a la demostració del *teorema fonamental de l'Àlgebra* hem fet servir el teorema de Bolzano, que sovint s'associa a l'Anàlisi matemàtica.
O per a provar que *tot cos és subcòs d'un cos algebraicament tancat*, o que *tota immersió d'un cos en un cos algebraicament tancat es pot estendre a qualsevol extensió algebraica*, o que *qualsevol extensió de cossos té un grau* (*ben determinat*), . . . ,

Acabem un curs (cont.)

També hem fet servir resultats i tècniques que sovint s'associen a altres branques de la Matemàtica.
Per exemple, per a la demostració del *teorema fonamental de l'Àlgebra* hem fet servir el teorema de Bolzano, que sovint s'associa a l'Anàlisi matemàtica.
O per a provar que *tot cos és subcòs d'un cos algebraicament tancat*, o que *tota immersió d'un cos en un cos algebraicament tancat es pot estendre a qualsevol extensió algebraica*, o que *qualsevol extensió de cossos té un grau* (*ben determinat*), . . . , hem fet servir el lema de Zorn (o si es vol, l'axiona de l'elecció), que correspon a Fonaments, o Lògica matemàtica.

Acabem un curs (cont.)

Per al càlcul en extensions de cossos, hem utilitzat bases del cos extensió pensat com a espai vectorial, tema que correspon a l'Àlgebra lineal, i l'algoritme d'Euclides per a polinomis, que correspon a l'Aritmètica.

Acabem un curs (cont.)

Per al càlcul en extensions de cossos, hem utilitzat bases del cos extensió pensat com a espai vectorial, tema que correspon a l'Àlgebra lineal, i l'algoritme d'Euclides per a polinomis, que correspon a l'Aritmètica.
Per a la descripció de les subextensions, hem usat reticles, que podríem encabir en Teoria de conjunts o en teoria de Grafs; i també el Teorema xinès del residu, d'Aritmètica o d'Estructures algebraiques.

Acabem un curs (cont.)

Per al càlcul en extensions de cossos, hem utilitzat bases del cos extensió pensat com a espai vectorial, tema que correspon a l'Àlgebra lineal, i l'algoritme d'Euclides per a polinomis, que correspon a l'Aritmètica.
Per a la descripció de les subextensions, hem usat reticles, que podríem encabir en Teoria de conjunts o en teoria de Grafs; i també el Teorema xinès del residu, d'Aritmètica o d'Estructures algebraiques.
Per a l'estudi de les construccions amb regle i compàs hem fet servir nocions bàsiques de Geometria euclidiana.

Acabem un curs (cont.)

Per al càlcul en extensions de cossos, hem utilitzat bases del cos extensió pensat com a espai vectorial, tema que correspon a l'Àlgebra lineal, i l'algoritme d'Euclides per a polinomis, que correspon a l'Aritmètica.
Per a la descripció de les subextensions, hem usat reticles, que podríem encabir en Teoria de conjunts o en teoria de Grafs; i també el Teorema xinès del residu, d'Aritmètica o d'Estructures algebraiques.
Per a l'estudi de les construccions amb regle i compàs hem fet servir nocions bàsiques de Geometria euclidiana.
I en la prova de la transcendència de π, hem usat eines d'Anàlisi complexa o de Càlcul integral.

Acabem un curs (cont.)

És a dir, el curs no només ha estat un curs d'Àlgebra, sinó que he procurat que fos un curs de Matemàtiques.

Acabem un curs (cont.)

És a dir, el curs no només ha estat un curs d'Àlgebra, sinó que he procurat que fos un curs de Matemàtiques.

Hi ha alguna altra àrea de la Matemàtica que, en aquesta introducció, ha quedat oblidada?

Acabem un curs (cont.)

És a dir, el curs no només ha estat un curs d'Àlgebra, sinó que he procurat que fos un curs de Matemàtiques.

Hi ha alguna altra àrea de la Matemàtica que, en aquesta introducció, ha quedat oblidada? Sí,

Acabem un curs (cont.)

És a dir, el curs no només ha estat un curs d'Àlgebra, sinó que he procurat que fos un curs de Matemàtiques.

Hi ha alguna altra àrea de la Matemàtica que, en aquesta introducció, ha quedat oblidada? Sí, i intentaré desvelar-ne, una mica, alguna.

Acabem un curs (cont.)

És a dir, el curs no només ha estat un curs d'Àlgebra, sinó que he procurat que fos un curs de Matemàtiques.

Hi ha alguna altra àrea de la Matemàtica que, en aquesta introducció, ha quedat oblidada? Sí, i intentaré desvelar-ne, una mica, alguna.

Em fixaré en un exemple.

L'automorfisme de Frobenius

Recordem que *si* $\mathbb{F}$ *és un cos finit, disposem de l'automorfisme de Frobenius de* $\mathbb{F}$ *(sobre* $\mathbb{F}_p$*)*

$$\varphi_p : \mathbb{F} \longrightarrow \mathbb{F}, \qquad \alpha \mapsto \alpha^p,$$

on $p > 0$ *és la característica de* $\mathbb{F}$*.*

L'automorfisme de Frobenius

Recordem que *si $\mathbb{F}$ és un cos finit, disposem de l'automorfisme de Frobenius de $\mathbb{F}$ (sobre $\mathbb{F}_p$)*

$$\varphi_p : \mathbb{F} \longrightarrow \mathbb{F}, \qquad \alpha \mapsto \alpha^p,$$

on $p > 0$ és la característica de $\mathbb{F}$.

Això es pot pensar, de nou, com una qüestió aritmètica, perquè p divideix els nombres combinatoris $\binom{p}{k}$, per a $1 \leq k \leq p$, de manera que, per a la suma, la fórmula per a la potència d'un binomi proporciona que $(\alpha + \beta)^p = \alpha^p + \beta^p$, mentre que per al producte és evident que $(\alpha\beta)^p = \alpha^p\beta^p$, per a l'element unitat tenim que $1^p = 1$, i per als inversos tenim que si $\alpha \neq 0$, llavors $(\alpha^{-1})^p = (\alpha^p)^{-1}$.

L'automorfisme de Frobenius

Recordem que *si $\mathbb{F}$ és un cos finit, disposem de l'automorfisme de Frobenius de $\mathbb{F}$ (sobre $\mathbb{F}_p$)*

$$\varphi_p : \mathbb{F} \longrightarrow \mathbb{F}, \qquad \alpha \mapsto \alpha^p,$$

on $p > 0$ és la característica de $\mathbb{F}$.

Això es pot pensar, de nou, com una qüestió aritmètica, perquè p divideix els nombres combinatoris $\binom{p}{k}$, per a $1 \leq k \leq p$, de manera que, per a la suma, la fórmula per a la potència d'un binomi proporciona que $(\alpha + \beta)^p = \alpha^p + \beta^p$, mentre que per al producte és evident que $(\alpha\beta)^p = \alpha^p\beta^p$, per a l'element unitat tenim que $1^p = 1$, i per als inversos tenim que si $\alpha \neq 0$, llavors $(\alpha^{-1})^p = (\alpha^p)^{-1}$.

Així, φ_p és un morfisme de cossos de $\mathbb{F}$ en $\mathbb{F}$; per tant, injectiu i, com que $\mathbb{F}$ és finit, exhaustiu. $\square$

L'automorfisme de Frobenius (cont.)

Ara, recordem que el cos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ és un subcòs de $\mathbb{F}$ i que, de fet, *és el subcòs format pels elements de* $\mathbb{F}$ *fixos per a l'acció de* φ_p.

L'automorfisme de Frobenius (cont.)

Ara, recordem que el cos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ és un subcòs de $\mathbb{F}$ i que, de fet, *és el subcòs format pels elements de* $\mathbb{F}$ *fixos per a l'acció de* φ_p.

Notem que, aquí, la inclusió de $\mathbb{F}_p$ en el cos fix la proporciona el petit teorema de Fermat: *per a tot nombre enter* α, $\alpha^p \equiv \alpha \pmod{p}$; és a dir, per a tot $\alpha \in \mathbb{F}_p$, és $\varphi_p(\alpha) = \alpha$.

L'automorfisme de Frobenius (cont.)

Ara, recordem que el cos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ és un subcòs de $\mathbb{F}$ i que, de fet, *és el subcòs format pels elements de* $\mathbb{F}$ *fixos per a l'acció de* φ_p.

Notem que, aquí, la inclusió de $\mathbb{F}_p$ en el cos fix la proporciona el petit teorema de Fermat: *per a tot nombre enter* α, $\alpha^p \equiv \alpha \pmod{p}$; és a dir, per a tot $\alpha \in \mathbb{F}_p$, és $\varphi_p(\alpha) = \alpha$.
Però, a més a més, com que un polinomi no pot tenir més arrels que el seu grau, no hi ha cap més element de $\mathbb{F}$ que sigui fix per φ_p.

És a dir, $\mathbb{F}_p$ és exactament el subcòs format pels elements fixos. $\square$

L'automorfisme de Frobenius (cont.)

Ara, recordem que el cos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ és un subcòs de $\mathbb{F}$ i que, de fet, *és el subcòs format pels elements de* $\mathbb{F}$ *fixos per a l'acció de* φ_p.

Notem que, aquí, la inclusió de $\mathbb{F}_p$ en el cos fix la proporciona el petit teorema de Fermat: *per a tot nombre enter* α, $\alpha^p \equiv \alpha \pmod{p}$; és a dir, per a tot $\alpha \in \mathbb{F}_p$, és $\varphi_p(\alpha) = \alpha$.
Però, a més a més, com que un polinomi no pot tenir més arrels que el seu grau, no hi ha cap més element de $\mathbb{F}$ que sigui fix per φ_p.

És a dir, $\mathbb{F}_p$ és exactament el subcòs format pels elements fixos. $\square$

Dit d'una altra manera, *el grup de Galois* $\mathrm{Gal}(\mathbb{F}|\mathbb{F}_p)$ (automorfismes de $\mathbb{F}$ que restringits a $\mathbb{F}_p$ són la identitat) *conté l'automorfisme de Frobenius* φ_p.

El grup de Galois sobre un cos finit

Més generalment, hem vist que *tota extensió de cossos finits* $L|k$ *és de Galois, i que el seu grup de Galois,* $\mathrm{Gal}(L|k)$*, és cíclic, generat per l'automorfisme de Frobenius (sobre* k*)* $\varphi_q : L \longrightarrow L$*, donat per* $\alpha \mapsto \alpha^q$*, on* $q = p^f$ *és el cardinal de* k*.*

Notem que φ_q és la potència f-èsima de l'automorfisme de Frobenius (sobre $\mathbb{F}_p$) de L, $\varphi_q = \varphi_p^f$, però que la restricció de φ_p^n a k només és la identitat si n és múltiple de f; és a dir, $\varphi_q = \varphi_p^f \in \mathrm{Gal}(L|k)$, però $\varphi_p^d \notin \mathrm{Gal}(L|k)$, si $1 \leq d \leq f-1$. (*Petit teorema de Fermat sobre* k*.*)

El grup de Galois sobre un cos finit (cont.)

Anem més enllà. Notem que *si K és un cos de característica $p > 0$, l'aplicació $\varphi_p : K \longrightarrow K$ és un morfisme injectiu de cossos de K en K; i si l'extensió $K|\mathbb{F}_p$ és algebraica, llavors φ_p és exhaustiu.*

El grup de Galois sobre un cos finit (cont.)

Anem més enllà. Notem que *si K és un cos de característica $p > 0$, l'aplicació $\varphi_p : K \longrightarrow K$ és un morfisme injectiu de cossos de K en K; i si l'extensió $K|\mathbb{F}_p$ és algebraica, llavors φ_p és exhaustiu.*

En efecte, cada element $\alpha \in K$ és algebraic sobre $\mathbb{F}_p$, de manera que genera un subcòs $\mathbb{F}_p(\alpha) \subseteq K$, i l'extensió $\mathbb{F}_p(\alpha)|\mathbb{F}_p$ és finita; per tant, $\mathbb{F}_p(\alpha)$ és un cos finit, i $\varphi_p : \mathbb{F}_p(\alpha) \longrightarrow \mathbb{F}_p(\alpha)$ és exhaustiva; per tant, tot element $\alpha \in K$ té una antiimatge per φ_p en $\mathbb{F}_p(\alpha) \subseteq K$. $\square$

El grup de Galois sobre un cos finit (cont.)

Anem més enllà. Notem que *si K és un cos de característica $p > 0$, l'aplicació $\varphi_p : K \longrightarrow K$ és un morfisme injectiu de cossos de K en K; i si l'extensió $K|\mathbb{F}_p$ és algebraica, llavors φ_p és exhaustiu.*

En efecte, cada element $\alpha \in K$ és algebraic sobre $\mathbb{F}_p$, de manera que genera un subcòs $\mathbb{F}_p(\alpha) \subseteq K$, i l'extensió $\mathbb{F}_p(\alpha)|\mathbb{F}_p$ és finita; per tant, $\mathbb{F}_p(\alpha)$ és un cos finit, i $\varphi_p : \mathbb{F}_p(\alpha) \longrightarrow \mathbb{F}_p(\alpha)$ és exhaustiva; per tant, tot element $\alpha \in K$ té una antiimatge per φ_p en $\mathbb{F}_p(\alpha) \subseteq K$. $\square$

És a dir, si $K|\mathbb{F}_p$ és una extensió algebraica, no necessàriament finita, disposem, també, de l'automorfisme de Frobenius, $\varphi_p \in \mathrm{Gal}(K|\mathbb{F}_p)$.

El grup de Galois sobre un cos finit (cont.)

I podem canviar el cos $\mathbb{F}_p$ per qualsevol cos finit $\mathbb{F}_q$, on $q = p^f$ és una potència de p.

El grup de Galois sobre un cos finit (cont.)

I podem canviar el cos $\mathbb{F}_p$ per qualsevol cos finit $\mathbb{F}_q$, on $q = p^f$ és una potència de p.

Si $K|\mathbb{F}_q$ és una extensió algebraica, l'automorfisme de Frobenius (sobre $\mathbb{F}_q$) $\varphi_q : K \longrightarrow K$, donat per $\alpha \mapsto \alpha^q$, és un element del grup de Galois $\mathrm{Gal}(K|\mathbb{F}_q)$.

El grup de Galois sobre un cos finit (cont.)

I podem canviar el cos $\mathbb{F}_p$ per qualsevol cos finit $\mathbb{F}_q$, on $q = p^f$ és una potència de p.

Si $K|\mathbb{F}_q$ és una extensió algebraica, l'automorfisme de Frobenius (sobre $\mathbb{F}_q$) $\varphi_q : K \longrightarrow K$, donat per $\alpha \mapsto \alpha^q$, és un element del grup de Galois $\mathrm{Gal}(K|\mathbb{F}_q)$.

Per exemple, podem escriure un cos clausura algebraica de $\mathbb{F}_q$ com la reunió $\overline{\mathbb{F}}_q = \bigcup_{f \geq 1} \mathbb{F}_{q^f}$, i l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$ no és finita, perquè, per a cada $f \geq 1$, conté una subextensió $\mathbb{F}_{q^f}|\mathbb{F}_q$ de grau f.

El grup de Galois sobre un cos finit (cont.)

I podem canviar el cos $\mathbb{F}_p$ per qualsevol cos finit $\mathbb{F}_q$, on $q = p^f$ és una potència de p.

Si $K|\mathbb{F}_q$ és una extensió algebraica, l'automorfisme de Frobenius (sobre $\mathbb{F}_q$) $\varphi_q : K \longrightarrow K$, donat per $\alpha \mapsto \alpha^q$, és un element del grup de Galois $\mathrm{Gal}(K|\mathbb{F}_q)$.

Per exemple, podem escriure un cos clausura algebraica de $\mathbb{F}_q$ com la reunió $\overline{\mathbb{F}}_q = \bigcup_{f \geq 1} \mathbb{F}_{q^f}$, i l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$ no és finita, perquè, per a cada $f \geq 1$, conté una subextensió $\mathbb{F}_{q^f}|\mathbb{F}_q$ de grau f.

Doncs, $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ conté l'automorfisme de Frobenius φ_q, que és d'ordre infinit; és a dir, *el grup de Galois absolut d'un cos finit conté un subrup cíclic infinit.*

El grup de Galois sobre un cos finit (cont.)

Fins aquí, res que no haguem vist durant el curs.

El grup de Galois sobre un cos finit (cont.)

Fins aquí, res que no haguem vist durant el curs.

Notem que l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$ és numerable (de grau numerable), i que $\overline{\mathbb{F}}_q$ és un cos numerable, reunió numerable de cossos finits.

El grup de Galois sobre un cos finit (cont.)

Fins aquí, res que no haguem vist durant el curs.

Notem que l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$ és numerable (de grau numerable), i que $\overline{\mathbb{F}}_q$ és un cos numerable, reunió numerable de cossos finits.

I també, que el grup de Galois absolut, $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$, conté un subgrup numerable, $\langle\varphi_q\rangle$.

El grup de Galois sobre un cos finit (cont.)

Fins aquí, res que no haguem vist durant el curs.

Notem que l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$ és numerable (de grau numerable), i que $\overline{\mathbb{F}}_q$ és un cos numerable, reunió numerable de cossos finits.

I també, que el grup de Galois absolut, $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$, conté un subgrup numerable, $\langle\varphi_q\rangle$.

Però el grup de Galois absolut no és numerable!

El grup de Galois sobre un cos finit (cont.)

Fins aquí, res que no haguem vist durant el curs.

Notem que l'extensió $\overline{\mathbb{F}}_q|\mathbb{F}_q$ és numerable (de grau numerable), i que $\overline{\mathbb{F}}_q$ és un cos numerable, reunió numerable de cossos finits.

I també, que el grup de Galois absolut, $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$, conté un subgrup numerable, $\langle\varphi_q\rangle$.

Però el grup de Galois absolut no és numerable!

Abans de veure això, però, limitem-nos a veure que el grup de Galois $\mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$ conté un element diferent de totes les potències de l'automorfisme de Frobenius; és a dir, que $\langle\varphi_p\rangle \subsetneq \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$.

El grup de Galois absolut d'un cos finit

Se satisfà el resultat següent, que es troba a la primera pàgina del primer capítol del llibre de Neukirch, **[Ne 1986]**.

El grup de Galois absolut d'un cos finit

Se satisfà el resultat següent, que es troba a la primera pàgina del primer capítol del llibre de Neukirch, **[Ne 1986]**.

Proposició

Existeix una successió de nombres enters, $\{a_n\}_{n\geq 1}$*, tal que*

- *per a tot* $n \geq 1$ *i tot divisor* $m \geq 1$ *de* n*, és* $a_n \equiv a_m \pmod{m}$,
- *i no existeix cap nombre enter* a *tal que per a tot* $n \geq 1$ *sigui* $a_n \equiv a \pmod{n}$.

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$.

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$;

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$; per tant, $a_n = n' x_n \equiv 0 \equiv m' x_m = a_m \pmod{m'}$,

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$; per tant, $a_n = n' x_n \equiv 0 \equiv m' x_m = a_m \pmod{m'}$, i també $a_n = 1 - p^{v_p(n)} y_n \equiv 1 \equiv 1 - p^{v_p(m)} y_m = a_m \pmod{p^{v_p(m)}}$;

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$; per tant, $a_n = n' x_n \equiv 0 \equiv m' x_m = a_m \pmod{m'}$, i també $a_n = 1 - p^{v_p(n)} y_n \equiv 1 \equiv 1 - p^{v_p(m)} y_m = a_m \pmod{p^{v_p(m)}}$; pel teorema xinès del residu, obtenim que $a_n \equiv a_m \pmod{m}$.

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$; per tant, $a_n = n' x_n \equiv 0 \equiv m' x_m = a_m \pmod{m'}$, i també $a_n = 1 - p^{v_p(n)} y_n \equiv 1 \equiv 1 - p^{v_p(m)} y_m = a_m \pmod{p^{v_p(m)}}$; pel teorema xinès del residu, obtenim que $a_n \equiv a_m \pmod{m}$.
Ara, si hi hagués algun nombre enter a tal que, per a tot m, fos $a \equiv a_m \pmod{m}$, tindríem que $a \equiv 0 \pmod{m'}$, per a tot m';

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$; per tant, $a_n = n' x_n \equiv 0 \equiv m' x_m = a_m \pmod{m'}$, i també $a_n = 1 - p^{v_p(n)} y_n \equiv 1 \equiv 1 - p^{v_p(m)} y_m = a_m \pmod{p^{v_p(m)}}$; pel teorema xinès del residu, obtenim que $a_n \equiv a_m \pmod{m}$.
Ara, si hi hagués algun nombre enter a tal que, per a tot m, fos $a \equiv a_m \pmod{m}$, tindríem que $a \equiv 0 \pmod{m'}$, per a tot m'; és a dir, a seria múltiple d'una infinitat de nombres enters, de manera que hauria de ser $a = 0$;

El grup de Galois absolut d'un cos finit (cont.)

Demostració

Escrivim tot nombre natural $n \geq 1$ en la forma $n = n' p^{v_p(n)}$, amb $v_p(n) \geq 0$ i n' no divisible per p.
Com que $\mathrm{mcd}(p, n') = 1$, existeixen nombres enters x_n, y_n tals que $1 = n' x_n + p^{v_p(n)} y_n$. Definim $a_n := n' x_n = 1 - p^{v_p(n)} y_n$.
Si m divideix n, llavors m' divideix n' i $v_p(m) \leq v_p(n)$; per tant, $a_n = n' x_n \equiv 0 \equiv m' x_m = a_m \pmod{m'}$, i també $a_n = 1 - p^{v_p(n)} y_n \equiv 1 \equiv 1 - p^{v_p(m)} y_m = a_m \pmod{p^{v_p(m)}}$; pel teorema xinès del residu, obtenim que $a_n \equiv a_m \pmod{m}$.
Ara, si hi hagués algun nombre enter a tal que, per a tot m, fos $a \equiv a_m \pmod{m}$, tindríem que $a \equiv 0 \pmod{m'}$, per a tot m'; és a dir, a seria múltiple d'una infinitat de nombres enters, de manera que hauria de ser $a = 0$; però això no pot ser, perquè també seria $a \equiv 1 \pmod{p^{v_p(m)}}$, per a tot m. $\square$

El grup de Galois absolut d'un cos finit (cont.)

Corol·lari

Per a tot nombre primer p, $\langle \varphi_p \rangle \subsetneq \mathsf{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$.

El grup de Galois absolut d'un cos finit (cont.)

Corol·lari

Per a tot nombre primer p, $\langle \varphi_p \rangle \subsetneq \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$.

Demostració

Considerem qualsevol successió $\{a_n\}_{n\geq 1}$ que satisfaci les propietats de la proposició; i, per a tot $n \geq 1$, considerem l'automorfisme $\psi_n := \varphi_p^{a_n} \in \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$, potència a_n-èsima de l'automorfisme de Frobenius φ_p.

El grup de Galois absolut d'un cos finit (cont.)

Corol·lari

Per a tot nombre primer p, $\langle \varphi_p \rangle \subsetneq \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$.

Demostració

Considerem qualsevol successió $\{a_n\}_{n\geq 1}$ que satisfaci les propietats de la proposició; i, per a tot $n \geq 1$, considerem l'automorfisme $\psi_n := \varphi_p^{a_n} \in \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$, potència a_n-èsima de l'automorfisme de Frobenius φ_p.
Notem que φ_p és la restricció a $\mathbb{F}_{p^n}$ de l'automorfisme de Frobenius φ_p de $\overline{\mathbb{F}}_p$; i, també, que ψ_n és la restricció a $\mathbb{F}_{p^n}$ de l'automorfisme $\varphi_p^{a_n}$ de $\overline{\mathbb{F}}_p$.

El grup de Galois absolut d'un cos finit (cont.)

Corol·lari

Per a tot nombre primer p, $\langle \varphi_p \rangle \subsetneq \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$.

Demostració

Considerem qualsevol successió $\{a_n\}_{n\geq 1}$ que satisfaci les propietats de la proposició; i, per a tot $n \geq 1$, considerem l'automorfisme $\psi_n := \varphi_p^{a_n} \in \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$, potència a_n-èsima de l'automorfisme de Frobenius φ_p.
Notem que φ_p és la restricció a $\mathbb{F}_{p^n}$ de l'automorfisme de Frobenius φ_p de $\overline{\mathbb{F}}_p$; i, també, que ψ_n és la restricció a $\mathbb{F}_{p^n}$ de l'automorfisme $\varphi_p^{a_n}$ de $\overline{\mathbb{F}}_p$.
Disposem, doncs, d'una successió d'automorfimes, ψ_n, cadascun d'un cos diferent, $\mathbb{F}_{p^n}$.

El grup de Galois absolut d'un cos finit (cont.)

Corol·lari

Per a tot nombre primer p, $\langle \varphi_p \rangle \subsetneq \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$.

Demostració

Considerem qualsevol successió $\{a_n\}_{n\geq 1}$ que satisfaci les propietats de la proposició; i, per a tot $n \geq 1$, considerem l'automorfisme $\psi_n := \varphi_p^{a_n} \in \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p)$, potència a_n-èsima de l'automorfisme de Frobenius φ_p.
Notem que φ_p és la restricció a $\mathbb{F}_{p^n}$ de l'automorfisme de Frobenius φ_p de $\overline{\mathbb{F}}_p$; i, també, que ψ_n és la restricció a $\mathbb{F}_{p^n}$ de l'automorfisme $\varphi_p^{a_n}$ de $\overline{\mathbb{F}}_p$.
Disposem, doncs, d'una successió d'automorfimes, ψ_n, cadascun d'un cos diferent, $\mathbb{F}_{p^n}$. O, si es vol, d'una successió d'automorfismes $\varphi_p^{a_n}$ de $\overline{\mathbb{F}}_p$.

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n.

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n. És a dir, donat $\alpha \in \overline{\mathbb{F}}_p$, definim $\psi(\alpha) := \psi_n(\alpha)$, per a qualsevol $n \geq 1$ tal que $\alpha \in \mathbb{F}_{p^n}$.

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n. És a dir, donat $\alpha \in \overline{\mathbb{F}}_p$, definim $\psi(\alpha) := \psi_n(\alpha)$, per a qualsevol $n \geq 1$ tal que $\alpha \in \mathbb{F}_{p^n}$. Però cal veure que això no depèn del valor n que fem servir.

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n. És a dir, donat $\alpha \in \overline{\mathbb{F}}_p$, definim $\psi(\alpha) := \psi_n(\alpha)$, per a qualsevol $n \geq 1$ tal que $\alpha \in \mathbb{F}_{p^n}$. Però cal veure que això no depèn del valor n que fem servir.

Donat $\alpha \in \overline{\mathbb{F}}_p$, si m és el menor nombre natural tal que $\alpha \in \mathbb{F}_{p^m}$, llavors α només pertany als cossos $\mathbb{F}_{p^n}$ tals que n és múltiple de m; i cal veure que $\psi_n(\alpha) = \psi_m(\alpha)$.

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n. És a dir, donat $\alpha \in \overline{\mathbb{F}}_p$, definim $\psi(\alpha) := \psi_n(\alpha)$, per a qualsevol $n \geq 1$ tal que $\alpha \in \mathbb{F}_{p^n}$. Però cal veure que això no depèn del valor n que fem servir.

Donat $\alpha \in \overline{\mathbb{F}}_p$, si m és el menor nombre natural tal que $\alpha \in \mathbb{F}_{p^m}$, llavors α només pertany als cossos $\mathbb{F}_{p^n}$ tals que n és múltiple de m; i cal veure que $\psi_n(\alpha) = \psi_m(\alpha)$.

Ara bé, per a tot múltiple n de m, el fet que sigui $a_n \equiv a_m \pmod{m}$ diu que existeix $\lambda \in \mathbb{Z}$ tal que $a_n = a_m + m\lambda$;

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n. És a dir, donat $\alpha \in \overline{\mathbb{F}}_p$, definim $\psi(\alpha) := \psi_n(\alpha)$, per a qualsevol $n \geq 1$ tal que $\alpha \in \mathbb{F}_{p^n}$. Però cal veure que això no depèn del valor n que fem servir.

Donat $\alpha \in \overline{\mathbb{F}}_p$, si m és el menor nombre natural tal que $\alpha \in \mathbb{F}_{p^m}$, llavors α només pertany als cossos $\mathbb{F}_{p^n}$ tals que n és múltiple de m; i cal veure que $\psi_n(\alpha) = \psi_m(\alpha)$.

Ara bé, per a tot múltiple n de m, el fet que sigui $a_n \equiv a_m \pmod{m}$ diu que existeix $\lambda \in \mathbb{Z}$ tal que $a_n = a_m + m\lambda$; per tant, en $\mathbb{F}_{p^m}$, tenim que $\varphi_p^{a_n} = \varphi_p^{a_m+m\lambda} = \varphi_p^{a_m} \circ \varphi_p^{m\lambda} = \varphi_p^{a_m}$, perquè φ_p^m (i, per tant, també $\varphi_p^{m\lambda}$) és la identitat en $\mathbb{F}_{p^m}$.

El grup de Galois absolut d'un cos finit (cont.)

Definim un automorfisme ψ de $\overline{\mathbb{F}}_p = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$ de manera que la restricció a cada cos $\mathbb{F}_{p^n}$ sigui ψ_n. És a dir, donat $\alpha \in \overline{\mathbb{F}}_p$, definim $\psi(\alpha) := \psi_n(\alpha)$, per a qualsevol $n \geq 1$ tal que $\alpha \in \mathbb{F}_{p^n}$. Però cal veure que això no depèn del valor n que fem servir.

Donat $\alpha \in \overline{\mathbb{F}}_p$, si m és el menor nombre natural tal que $\alpha \in \mathbb{F}_{p^m}$, llavors α només pertany als cossos $\mathbb{F}_{p^n}$ tals que n és múltiple de m; i cal veure que $\psi_n(\alpha) = \psi_m(\alpha)$.

Ara bé, per a tot múltiple n de m, el fet que sigui $a_n \equiv a_m \pmod{m}$ diu que existeix $\lambda \in \mathbb{Z}$ tal que $a_n = a_m + m\lambda$; per tant, en $\mathbb{F}_{p^m}$, tenim que $\varphi_p^{a_n} = \varphi_p^{a_m + m\lambda} = \varphi_p^{a_m} \circ \varphi_p^{m\lambda} = \varphi_p^{a_m}$, perquè φ_p^m (i, per tant, també $\varphi_p^{m\lambda}$) és la identitat en $\mathbb{F}_{p^m}$.

Doncs, $\psi_n(\alpha) = \varphi_p^{a_n}(\alpha) = \varphi_p^{a_m}(\alpha) = \psi_m(\alpha)$, com calia veure.

El grup de Galois absolut d'un cos finit (cont.)

Acabem de construir un element $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$; si veiem que $\psi \notin \langle \varphi_p \rangle$, haurem acabat.

El grup de Galois absolut d'un cos finit (cont.)

Acabem de construir un element $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$; si veiem que $\psi \notin \langle \varphi_p \rangle$, haurem acabat.

Però això és senzill, perquè si per a algun nombre enter a fos $\psi = \varphi_p^a$, en restringir a $\mathbb{F}_{p^n}$ tindríem que, en $\mathbb{F}_{p^n}$, seria $\varphi_p^{a_n} = \psi_n = \varphi_p^a$ i, com que φ_p és d'ordre n en $\mathbb{F}_{p^n}$, seria $a_n \equiv a \pmod{n}$.

El grup de Galois absolut d'un cos finit (cont.)

Acabem de construir un element $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$; si veiem que $\psi \notin \langle \varphi_p \rangle$, haurem acabat.

Però això és senzill, perquè si per a algun nombre enter a fos $\psi = \varphi_p^a$, en restringir a $\mathbb{F}_{p^n}$ tindríem que, en $\mathbb{F}_{p^n}$, seria $\varphi_p^{a_n} = \psi_n = \varphi_p^a$ i, com que φ_p és d'ordre n en $\mathbb{F}_{p^n}$, seria $a_n \equiv a \pmod{n}$. I això contradiu les propietats de la successió $\{a_n\}_{n\geq 1}$. $\square$

El grup de Galois absolut d'un cos finit (cont.)

Què hem fet?

El grup de Galois absolut d'un cos finit (cont.)

Què hem fet?

Màgia?

El grup de Galois absolut d'un cos finit (cont.)

Què hem fet?

Màgia?

No!

El grup de Galois absolut d'un cos finit (cont.)

Què hem fet?

Màgia?

No!

Topologia!

El grup de Galois absolut d'un cos finit (cont.)

Què hem fet?

Màgia?

No!

Topologia!

De fet, hem construït un límit de la successió $\varphi_p^{a_n}$.

Límits projectius

Fixem-nos que la successió $\{a_n\}_{n\geq 1}$ és, de fet, un element del (grup abelià) producte cartesià $Z := \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$, element per al qual se satisfan algunes propietats especials.

Límits projectius

Fixem-nos que la successió $\{a_n\}_{n\geq 1}$ és, de fet, un element del (grup abelià) producte cartesià $Z := \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$, element per al qual se satisfan algunes propietats especials.
De fet, aquest producte cartesià, Z, també és un anell, i de característica zero, perquè l'aplicació $\mathbb{Z} \longrightarrow \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$ donada per $a \mapsto \{a \pmod n\}_{n\geq 1}$ és un morfisme injectiu d'anells

Límits projectius

Fixem-nos que la successió $\{a_n\}_{n\geq 1}$ és, de fet, un element del (grup abelià) producte cartesià $Z := \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$, element per al qual se satisfan algunes propietats especials.
De fet, aquest producte cartesià, Z, també és un anell, i de característica zero, perquè l'aplicació $\mathbb{Z} \longrightarrow \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$ donada per $a \mapsto \{a \pmod n\}_{n\geq 1}$ és un morfisme injectiu d'anells (notem que 1 s'aplica en l'element unitat, la suma en la suma, el producte en el producte, i que l'únic nombre enter tal que $a \equiv 0 \pmod n$ per a tot $n \geq 1$ és $a = 0$)

Límits projectius

Fixem-nos que la successió $\{a_n\}_{n\geq 1}$ és, de fet, un element del (grup abelià) producte cartesià $Z := \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$, element per al qual se satisfan algunes propietats especials.
De fet, aquest producte cartesià, Z, també és un anell, i de característica zero, perquè l'aplicació $\mathbb{Z} \longrightarrow \prod_{n\geq 1}(\mathbb{Z}/n\mathbb{Z})$ donada per $a \mapsto \{a \pmod n\}_{n\geq 1}$ és un morfisme injectiu d'anells (notem que 1 s'aplica en l'element unitat, la suma en la suma, el producte en el producte, i que l'únic nombre enter tal que $a \equiv 0 \pmod n$ per a tot $n \geq 1$ és $a = 0$), de manera que Z conté un subanell isomorf a $\mathbb{Z}$.

Límits projectius (cont.)

Ara, posem $\hat{\mathbb{Z}}$ per al subconjunt de Z format per les successions $\{a_n\}_{n\geq 1}$ tals que per a tota parella de nombres enters (n, m) tals que m divideix n se satisfà que $a_n \equiv a_m \pmod{m}$ (s'anomenen les successions coherents per a la relació d'ordre donada per divisibilitat).

Límits projectius (cont.)

Ara, posem $\hat{\mathbb{Z}}$ per al subconjunt de Z format per les successions $\{a_n\}_{n\geq 1}$ tals que per a tota parella de nombres enters (n, m) tals que m divideix n se satisfà que $a_n \equiv a_m \pmod{m}$ (s'anomenen les successions coherents per a la relació d'ordre donada per divisibilitat). Notem que aquesta és la primera condició que hem demanat a la successió $\{a_n\}_{n\geq 1}$ anterior.

Límits projectius (cont.)

Ara, posem $\hat{\mathbb{Z}}$ per al subconjunt de Z format per les successions $\{a_n\}_{n\geq 1}$ tals que per a tota parella de nombres enters (n, m) tals que m divideix n se satisfà que $a_n \equiv a_m \pmod{m}$ (s'anomenen les successions coherents per a la relació d'ordre donada per divisibilitat). Notem que aquesta és la primera condició que hem demanat a la successió $\{a_n\}_{n\geq 1}$ anterior. En particular, doncs, $\hat{\mathbb{Z}}$ és no buit, és un subanell, i, de fet, conté $\mathbb{Z}$ (de fet, la imatge de $\mathbb{Z}$ pel morfisme de més amunt).

Límits projectius (cont.)

Ara, posem $\hat{\mathbb{Z}}$ per al subconjunt de Z format per les successions $\{a_n\}_{n\geq 1}$ tals que per a tota parella de nombres enters (n, m) tals que m divideix n se satisfà que $a_n \equiv a_m \pmod{m}$ (s'anomenen les successions coherents per a la relació d'ordre donada per divisibilitat). Notem que aquesta és la primera condició que hem demanat a la successió $\{a_n\}_{n\geq 1}$ anterior. En particular, doncs, $\hat{\mathbb{Z}}$ és no buit, és un subanell, i, de fet, conté $\mathbb{Z}$ (de fet, la imatge de $\mathbb{Z}$ pel morfisme de més amunt). S'anomena l'anell de Prüfer

Límits projectius (cont.)

Ara, posem $\hat{\mathbb{Z}}$ per al subconjunt de Z format per les successions $\{a_n\}_{n\geq 1}$ tals que per a tota parella de nombres enters (n, m) tals que m divideix n se satisfà que $a_n \equiv a_m \pmod{m}$ (s'anomenen les successions coherents per a la relació d'ordre donada per divisibilitat). Notem que aquesta és la primera condició que hem demanat a la successió $\{a_n\}_{n\geq 1}$ anterior. En particular, doncs, $\hat{\mathbb{Z}}$ és no buit, és un subanell, i, de fet, conté $\mathbb{Z}$ (de fet, la imatge de $\mathbb{Z}$ pel morfisme de més amunt). S'anomena l'anell de Prüfer (tot i que aquí, de moment, només ens interessi l'estructura de grup abelià additiu).

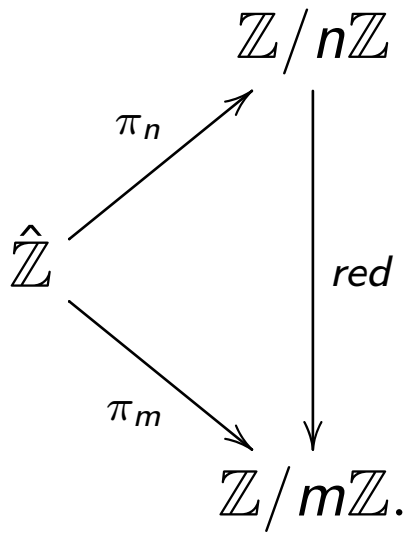
Límits projectius (cont.)

Ara, posem $\hat{\mathbb{Z}}$ per al subconjunt de Z format per les successions $\{a_n\}_{n\geq 1}$ tals que per a tota parella de nombres enters (n, m) tals que m divideix n se satisfà que $a_n \equiv a_m \pmod{m}$ (s'anomenen les successions coherents per a la relació d'ordre donada per divisibilitat). Notem que aquesta és la primera condició que hem demanat a la successió $\{a_n\}_{n\geq 1}$ anterior. En particular, doncs, $\hat{\mathbb{Z}}$ és no buit, és un subanell, i, de fet, conté $\mathbb{Z}$ (de fet, la imatge de $\mathbb{Z}$ pel morfisme de més amunt). S'anomena l'anell de Prüfer (tot i que aquí, de moment, només ens interessi l'estructura de grup abelià additiu).

L'anell $\hat{\mathbb{Z}}$ de les successions coherents, és el límit projectiu de la família de morfismes $\{(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/m\mathbb{Z}) : m|n\}$, i s'escriu $\hat{\mathbb{Z}} = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$, perquè se sobreentenen els morfismes.

Límits projectius (cont.)

Notem que disposem de projeccions de $\hat{\mathbb{Z}}$ en cadascun dels anells $\mathbb{Z}/n\mathbb{Z}$ (la inclusió en el producte seguida de la projecció des del producte), i que aquestes projeccions són compatibles amb els morfismes de reducció $(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})$ per a m divisor de n; és a dir, tenim diagrames commutatius de morfismes (d'anells i, per tant, dels grups additius), per a m divisor de n,



Límits projectius (cont.)

Aquesta propietat se satisfà de manera natural per al grup de Galois absolut d'un cos finit, $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$. Recordem que

Límits projectius (cont.)

Aquesta propietat se satisfà de manera natural per al grup de Galois absolut d'un cos finit, $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$. Recordem que

- *la restricció d'un $\mathbb{F}$-automorfisme qualsevol de $\overline{\mathbb{F}}$ a un cos extensió finita $L|\mathbb{F}$ és un $\mathbb{F}$-automorfisme*, perquè tota extensió finita d'un cos finit és normal;

Límits projectius (cont.)

Aquesta propietat se satisfà de manera natural per al grup de Galois absolut d'un cos finit, $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$. Recordem que

- *la restricció d'un $\mathbb{F}$-automorfisme qualsevol de $\overline{\mathbb{F}}$ a un cos extensió finita $L|\mathbb{F}$ és un $\mathbb{F}$-automorfisme*, perquè tota extensió finita d'un cos finit és normal;
- i que *per a subcossos finits de $\overline{\mathbb{F}}$, $\mathbb{F} \subseteq K \subseteq L$, la restricció a K d'un $\mathbb{F}$-automorfisme ψ de $\overline{\mathbb{F}}$ és la restricció a K de la restricció de ψ a L.*

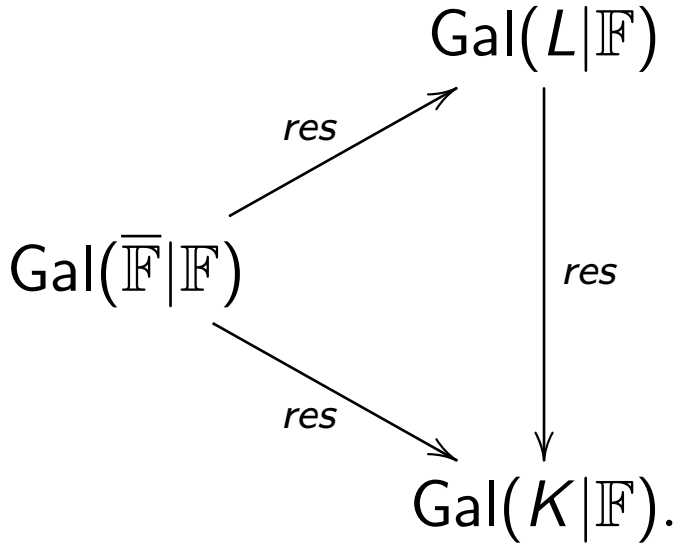
Límits projectius (cont.)

Aquesta propietat se satisfà de manera natural per al grup de Galois absolut d'un cos finit, $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$. Recordem que

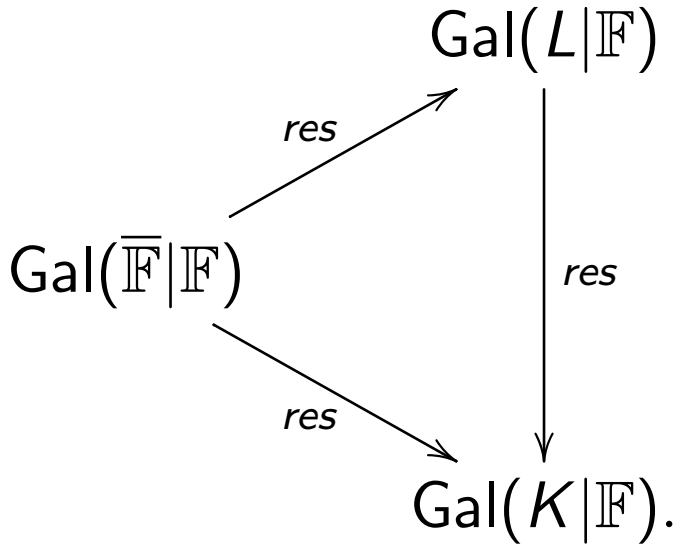
- *la restricció d'un $\mathbb{F}$-automorfisme qualsevol de $\overline{\mathbb{F}}$ a un cos extensió finita $L|\mathbb{F}$ és un $\mathbb{F}$-automorfisme*, perquè tota extensió finita d'un cos finit és normal;
- i que *per a subcossos finits de $\overline{\mathbb{F}}$, $\mathbb{F} \subseteq K \subseteq L$, la restricció a K d'un $\mathbb{F}$-automorfisme ψ de $\overline{\mathbb{F}}$ és la restricció a K de la restricció de ψ a L.*

És a dir, per al grup de Galois absolut, se satisfà la propietat anterior de compatibilitat respecte dels grups de Galois de les extensions finites $L|\mathbb{F}$.

Límits projectius (cont.)

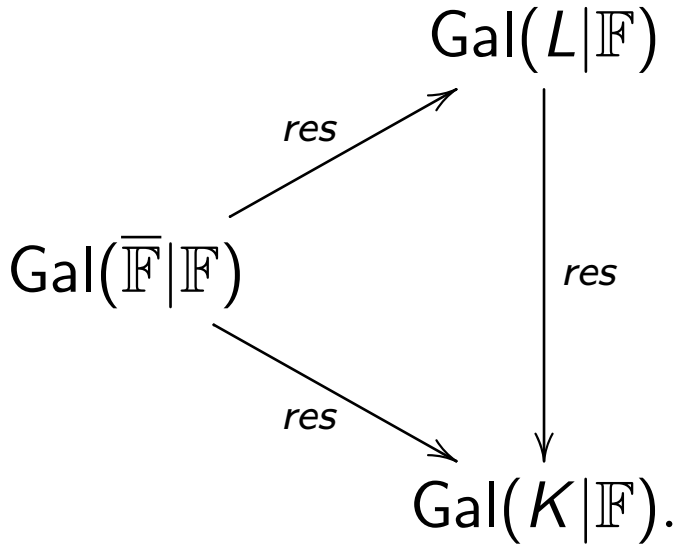


Límits projectius (cont.)



I tenim que $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F}) = \varprojlim_{L|\mathbb{F} \text{ finita}} \mathrm{Gal}(L|\mathbb{F})$.

Límits projectius (cont.)



I tenim que $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F}) = \varprojlim_{L|\mathbb{F} \text{ finita}} \mathrm{Gal}(L|\mathbb{F})$.

En efecte, com que $\overline{\mathbb{F}}$ és la reunió dels subcossos L tals que $L|\mathbb{F}$ és finita, donar un $\mathbb{F}$-automorfisme de $\overline{\mathbb{F}}$ és equivalent a donar-ne la reducció a tots els subcossos L; és a dir, a donar un $\mathbb{F}$-automorfisme de cada cos L extensió finita de $\mathbb{F}$, de manera que aquests automorfismes siguin coherents. $\square$

Límits projectius (cont.)

On és la topologia?

Límits projectius (cont.)

On és la topologia?

Considerem, en cadascun dels grups finits $\mathrm{Gal}(L|\mathbb{F})$ (o, equivalentment, en cadascun dels grups $\mathbb{Z}/n\mathbb{Z}$) la topologia discreta.

Límits projectius (cont.)

On és la topologia?

Considerem, en cadascun dels grups finits $\mathrm{Gal}(L|\mathbb{F})$ (o, equivalentment, en cadascun dels grups $\mathbb{Z}/n\mathbb{Z}$) la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.

Límits projectius (cont.)

On és la topologia?

Considerem, en cadascun dels grups finits $\mathrm{Gal}(L|\mathbb{F})$ (o, equivalentment, en cadascun dels grups $\mathbb{Z}/n\mathbb{Z}$) la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.
I en el producte cartesià $\prod_{L|\mathbb{F} \text{ finita}} \mathrm{Gal}(L|\mathbb{F})$, la topologia producte. Pel teorema de Tykhonov, es tracta d'un grup topològic compacte.

Límits projectius (cont.)

On és la topologia?

Considerem, en cadascun dels grups finits $\mathrm{Gal}(L|\mathbb{F})$ (o, equivalentment, en cadascun dels grups $\mathbb{Z}/n\mathbb{Z}$) la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.

I en el producte cartesià $\prod_{L|\mathbb{F} \text{ finita}} \mathrm{Gal}(L|\mathbb{F})$, la topologia producte. Pel teorema de Tykhonov, es tracta d'un grup topològic compacte.

I en el subgrup $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$, la topologia induïda. El subgrup és tancat (exercici), de manera que també es tracta d'un grup topològic compacte.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$

- És un grup topològic commutatiu, que conté estrictament un subgrup cíclic infinit, $\langle \varphi_q \rangle$, on φ_q és l'automorfisme de Frobenius, donat per $\alpha \mapsto \alpha^q$, per a $q := \#\mathbb{F}$.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$

- És un grup topològic commutatiu, que conté estrictament un subgrup cíclic infinit, $\langle \varphi_q \rangle$, on φ_q és l'automorfisme de Frobenius, donat per $\alpha \mapsto \alpha^q$, per a $q := \#\mathbb{F}$.
- Com a conseqüència de la commutativitat, tots els subgrups són normals, de manera que els cossos fixos corresponents són extensions normals de $\mathbb{F}$.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$

- És un grup topològic commutatiu, que conté estrictament un subgrup cíclic infinit, $\langle\varphi_q\rangle$, on φ_q és l'automorfisme de Frobenius, donat per $\alpha \mapsto \alpha^q$, per a $q := \#\mathbb{F}$.
- Com a conseqüència de la commutativitat, tots els subgrups són normals, de manera que els cossos fixos corresponents són extensions normals de $\mathbb{F}$.
- El cos fix per φ_q (o sigui, pel subgrup generat per φ_q) coincideix amb el cos fix per tot el grup $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$

• És un grup topològic commutatiu, que conté estrictament un subgrup cíclic infinit, $\langle\varphi_q\rangle$, on φ_q és l'automorfisme de Frobenius, donat per $\alpha \mapsto \alpha^q$, per a $q := \#\mathbb{F}$.

• Com a conseqüència de la commutativitat, tots els subgrups són normals, de manera que els cossos fixos corresponents són extensions normals de $\mathbb{F}$.

• El cos fix per φ_q (o sigui, pel subgrup generat per φ_q) coincideix amb el cos fix per tot el grup $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$.

• Doncs, no podem esperar una bijecció (similar a la del cas finit) entre el conjunt dels subgrups i el conjunt dels subcossos...

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ (cont.)

Ara bé...

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ (cont.)

Ara bé...

• En un grup topològic, G, tot subgrup obert, H, és automàticament tancat, perquè el seu complementari és la reunió de les classes laterals gH per a $g \notin H$, que són oberts, homeomorfs a H.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ (cont.)

Ara bé...

- En un grup topològic, G, tot subgrup obert, H, és automàticament tancat, perquè el seu complementari és la reunió de les classes laterals gH per a $g \notin H$, que són oberts, homeomorfs a H.
- I resulta que $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ és l'adherència del subgrup $\langle \varphi_q \rangle$.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ (cont.)

Ara bé...

- En un grup topològic, G, tot subgrup obert, H, és automàticament tancat, perquè el seu complementari és la reunió de les classes laterals gH per a $g \notin H$, que són oberts, homeomorfs a H.
- I resulta que $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ és l'adherència del subgrup $\langle \varphi_q \rangle$. Es diu que el grup de Galois és generat topològicament per φ_q.

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ (cont.)

Ara bé...

• En un grup topològic, G, tot subgrup obert, H, és automàticament tancat, perquè el seu complementari és la reunió de les classes laterals gH per a $g \notin H$, que són oberts, homeomorfs a H.

• I resulta que $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ és l'adherència del subgrup $\langle \varphi_q \rangle$. Es diu que el grup de Galois és generat topològicament per φ_q.

Més generalment...

• Els subgrups oberts són exactament els d'índex finit, i es corresponen amb les extensions finites $L|\mathbb{F}$;

Algunes propietats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ (cont.)

Ara bé...

• En un grup topològic, G, tot subgrup obert, H, és automàticament tancat, perquè el seu complementari és la reunió de les classes laterals gH per a $g \notin H$, que són oberts, homeomorfs a H.

• I resulta que $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ és l'adherència del subgrup $\langle \varphi_q \rangle$. Es diu que el grup de Galois és generat topològicament per φ_q.

Més generalment...

• Els subgrups oberts són exactament els d'índex finit, i es corresponen amb les extensions finites $L|\mathbb{F}$;

• i, en general, el cos fix per un subgrup coincideix amb el cos fix pel subgrup adherència topològica.

Teorema fonamental de la teoria de Galois

Teorema (fonamental de la teoria de Galois sobre cossos finits)

Sigui $\mathbb{F}$ un cos finit. L'assignació $H \mapsto \overline{\mathbb{F}}^H|\mathbb{F}$ defineix una bijecció que inverteix l'ordre donat per inclusió del conjunt dels subgrups tancats de $\mathrm{Gal}(\overline{\mathbb{F}}|\mathbb{F})$ en el conjunt de totes les subextensions $K|\mathbb{F}$ de $\overline{\mathbb{F}}|\mathbb{F}$, amb inversa donada per $K|\mathbb{F} \mapsto \mathrm{Gal}(\overline{\mathbb{F}}|K)$. I els subgrups oberts es corresponen exactament amb les extensions finites.

Grups de Galois absoluts

Observació

En general, si $\overline{k}$ és una clausura algebraica d'un cos qualsevol, l'extensió $\overline{k}|k$ pot no ser de Galois, perquè pot no ser separable.

Grups de Galois absoluts

Observació

En general, si $\overline{k}$ és una clausura algebraica d'un cos qualsevol, l'extensió $\overline{k}|k$ pot no ser de Galois, perquè pot no ser separable. (A classe hem vist l'exemple de l'extensió no separable $\mathbb{F}_p(t^{1/p})|\mathbb{F}_p(t)$, t una indeterminada, de manera que $\overline{\mathbb{F}_p(t)}|\mathbb{F}_p(t)$ no és de Galois.)

Grups de Galois absoluts

Observació

En general, si $\overline{k}$ és una clausura algebraica d'un cos qualsevol, l'extensió $\overline{k}|k$ pot no ser de Galois, perquè pot no ser separable. (A classe hem vist l'exemple de l'extensió no separable $\mathbb{F}_p(t^{1/p})|\mathbb{F}_p(t)$, t una indeterminada, de manera que $\overline{\mathbb{F}_p(t)}|\mathbb{F}_p(t)$ no és de Galois.)

Ara bé, si denotem per $k^s \subseteq \overline{k}$ la clausura separable de k en $\overline{k}$, o sigui, la màxima subextensió separable $k^s|k$ de $\overline{k}|k$, tenim una extensió de Galois (recordem que la clausura normal d'una extensió separable és separable, de manera que la clausura normal de $k^s|k$ és $k^s|k$).

Grups de Galois absoluts

Observació

En general, si $\overline{k}$ és una clausura algebraica d'un cos qualsevol, l'extensió $\overline{k}|k$ pot no ser de Galois, perquè pot no ser separable. (A classe hem vist l'exemple de l'extensió no separable $\mathbb{F}_p(t^{1/p})|\mathbb{F}_p(t)$, t una indeterminada, de manera que $\overline{\mathbb{F}_p(t)}|\mathbb{F}_p(t)$ no és de Galois.)

Ara bé, si denotem per $k^s \subseteq \overline{k}$ la clausura separable de k en $\overline{k}$, o sigui, la màxima subextensió separable $k^s|k$ de $\overline{k}|k$, tenim una extensió de Galois (recordem que la clausura normal d'una extensió separable és separable, de manera que la clausura normal de $k^s|k$ és $k^s|k$).

El grup de Galois $\mathrm{Gal}(k^s|k)$ és el grup de Galois absolut de k.

Grups de Galois absoluts

Observació

En general, si $\overline{k}$ és una clausura algebraica d'un cos qualsevol, l'extensió $\overline{k}|k$ pot no ser de Galois, perquè pot no ser separable. (A classe hem vist l'exemple de l'extensió no separable $\mathbb{F}_p(t^{1/p})|\mathbb{F}_p(t)$, t una indeterminada, de manera que $\overline{\mathbb{F}_p(t)}|\mathbb{F}_p(t)$ no és de Galois.)

Ara bé, si denotem per $k^s \subseteq \overline{k}$ la clausura separable de k en $\overline{k}$, o sigui, la màxima subextensió separable $k^s|k$ de $\overline{k}|k$, tenim una extensió de Galois (recordem que la clausura normal d'una extensió separable és separable, de manera que la clausura normal de $k^s|k$ és $k^s|k$).

El grup de Galois $\mathrm{Gal}(k^s|k)$ és el grup de Galois absolut de k.

I per al grup de Galois absolut, se satisfà una propietat semblant.

Grups de Galois

Més generalment,

Grups de Galois

Més generalment,

considerem una extensió de Galois de cossos, $K|k$, no necessàriament finita.

Grups de Galois

Més generalment,

considerem una extensió de Galois de cossos, $K|k$, no necessàriament finita.
Hem vist que donat un k-automorfisme de K, o sigui un element de $\mathrm{Gal}(K|k)$, podem considerar-ne la restricció a qualsevol subcòs L de K (que contingui k); i que això proporciona una immersió de L en $\overline{k}$. I que si l'extensió $L|k$ és de Galois, aquesta restricció és un automorfisme; és a dir, un element del grup de Galois $\mathrm{Gal}(L|k)$.

Grups de Galois

Més generalment,

considerem una extensió de Galois de cossos, $K|k$, no necessàriament finita.
Hem vist que donat un k-automorfisme de K, o sigui un element de $\mathrm{Gal}(K|k)$, podem considerar-ne la restricció a qualsevol subcòs L de K (que contingui k); i que això proporciona una immersió de L en $\overline{k}$. I que si l'extensió $L|k$ és de Galois, aquesta restricció és un automorfisme; és a dir, un element del grup de Galois $\mathrm{Gal}(L|k)$.
Tenim, doncs, morfismes de grups, donats per restricció, $\mathrm{Gal}(K|k) \longrightarrow \mathrm{Gal}(L|k)$, per a totes les subextensions de Galois $L|k$ (no només les finites, tot i que ens interessen aquestes),

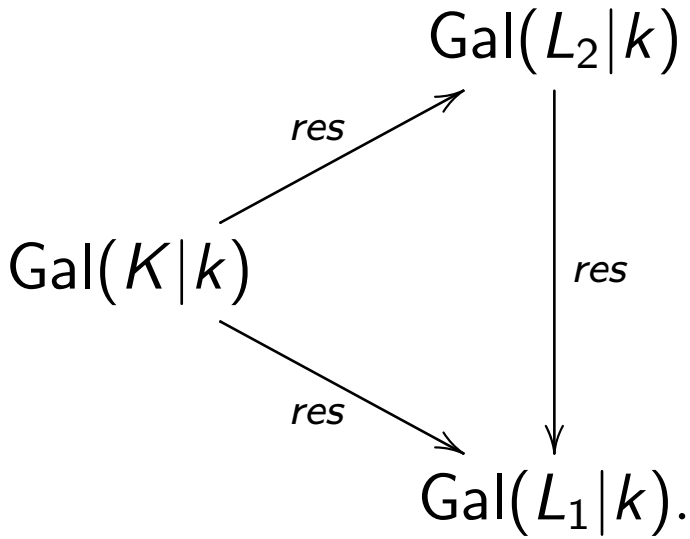
Grups de Galois

Més generalment,

considerem una extensió de Galois de cossos, $K|k$, no necessàriament finita.
Hem vist que donat un k-automorfisme de K, o sigui un element de $\mathrm{Gal}(K|k)$, podem considerar-ne la restricció a qualsevol subcòs L de K (que contingui k); i que això proporciona una immersió de L en $\overline{k}$. I que si l'extensió $L|k$ és de Galois, aquesta restricció és un automorfisme; és a dir, un element del grup de Galois $\mathrm{Gal}(L|k)$.
Tenim, doncs, morfismes de grups, donats per restricció, $\mathrm{Gal}(K|k) \longrightarrow \mathrm{Gal}(L|k)$, per a totes les subextensions de Galois $L|k$ (no només les finites, tot i que ens interessen aquestes), i hem vist que són exhaustius, pel teorema d'extensió d'automorfismes.

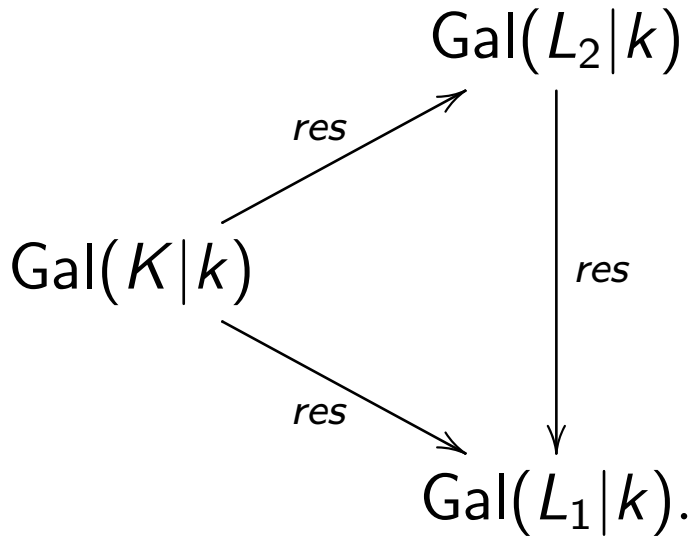
Grups de Galois (cont.)

A més a més, per a subextensions de Galois $L_1|k$, $L_2|k$ tals que $L_1 \subseteq L_2$, els morfismes de restricció són compatibles:



Grups de Galois (cont.)

A més a més, per a subextensions de Galois $L_1|k$, $L_2|k$ tals que $L_1 \subseteq L_2$, els morfismes de restricció són compatibles:



I també es té que K és la reunió dels subcossos $L \subseteq K$ tals que $L|k$ és de Galois finita.

Grups de Galois (cont.)

Teorema

$$\mathrm{Gal}(K|k) = \varprojlim_{L|k \text{ de Galois, finita, } L\subseteq K} \mathrm{Gal}(L|k).$$

Grups de Galois (cont.)

Teorema

$$\mathrm{Gal}(K|k) = \varprojlim_{L|k \text{ de Galois, finita, } L\subseteq K} \mathrm{Gal}(L|k).$$

Demostració

Copiem l'anterior del cas de cossos finits!

Grups de Galois (cont.)

Teorema

$$\mathrm{Gal}(K|k) = \varprojlim_{L|k \text{ de Galois, finita, } L\subseteq K} \mathrm{Gal}(L|k).$$

Demostració

Copiem l'anterior del cas de cossos finits!

(Les restriccions d'un automorfisme formen una família coherent d'automorfismes, i l'automorfisme es recupera a partir de les seves restriccions a subextensions finites.) $\square$

Grups de Galois (cont.)

Topologia?

Grups de Galois (cont.)

Topologia?

Considerem, en cadascun dels grups $\mathrm{Gal}(L|k)$, per a $L|k$ de Galois finita, $L \subseteq K$, la topologia discreta.

Grups de Galois (cont.)

Topologia?

Considerem, en cadascun dels grups $\mathrm{Gal}(L|k)$, per a $L|k$ de Galois finita, $L \subseteq K$, la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.

Grups de Galois (cont.)

Topologia?

Considerem, en cadascun dels grups $\mathrm{Gal}(L|k)$, per a $L|k$ de Galois finita, $L \subseteq K$, la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.
I en el producte cartesià $\prod_{L|k \text{ de Galois, finita, } L \subseteq K} \mathrm{Gal}(L|k)$, la topologia producte. Pel teorema de Tykhonov, es tracta d'un grup topològic compacte.

Grups de Galois (cont.)

Topologia?

Considerem, en cadascun dels grups $\mathrm{Gal}(L|k)$, per a $L|k$ de Galois finita, $L \subseteq K$, la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.
I en el producte cartesià $\prod_{L|k \text{ de Galois, finita, } L \subseteq K} \mathrm{Gal}(L|k)$, la topologia producte. Pel teorema de Tykhonov, es tracta d'un grup topològic compacte.
I en el subgrup $\mathrm{Gal}(K|k)$ del producte, la topologia induïda. El subgrup és tancat, de manera que també es tracta d'un grup topològic compacte.

Grups de Galois (cont.)

Topologia?

Considerem, en cadascun dels grups $\mathrm{Gal}(L|k)$, per a $L|k$ de Galois finita, $L \subseteq K$, la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.
I en el producte cartesià $\prod_{L|k \text{ de Galois, finita, } L \subseteq K} \mathrm{Gal}(L|k)$, la topologia producte. Pel teorema de Tykhonov, es tracta d'un grup topològic compacte.
I en el subgrup $\mathrm{Gal}(K|k)$ del producte, la topologia induïda. El subgrup és tancat, de manera que també es tracta d'un grup topològic compacte.
Aquesta topologia en $\mathrm{Gal}(K|k)$ s'anomena la topologia de Krull.

Grups de Galois (cont.)

Topologia?

Considerem, en cadascun dels grups $\mathrm{Gal}(L|k)$, per a $L|k$ de Galois finita, $L \subseteq K$, la topologia discreta. Notem que, com que els grups són finits, són grups topològics compactes.
I en el producte cartesià $\prod_{L|k \text{ de Galois, finita, } L \subseteq K} \mathrm{Gal}(L|k)$, la topologia producte. Pel teorema de Tykhonov, es tracta d'un grup topològic compacte.
I en el subgrup $\mathrm{Gal}(K|k)$ del producte, la topologia induïda. El subgrup és tancat, de manera que també es tracta d'un grup topològic compacte.
Aquesta topologia en $\mathrm{Gal}(K|k)$ s'anomena la topologia de Krull.
Notem que si $K|k$ és finita, la topologia que obtenim és la discreta.

Teorema fonamental de la teoria de Galois

Teorema (fonamental de la teoria de Galois)

Sigui $K|k$ una extensió de Galois de cossos. L'assignació $H \mapsto K^H|k$ defineix una bijecció que inverteix l'ordre donat per inclusió del conjunt dels subgrups tancats de $\mathrm{Gal}(K|k)$ en el conjunt de totes les subextensions $L|k$ de $K|k$, amb inversa donada per $L|k \mapsto \mathrm{Gal}(K|L)$. I els subgrups oberts es corresponen exactament amb les extensions finites.

Teorema fonamental de la teoria de Galois

Teorema (fonamental de la teoria de Galois)

Sigui $K|k$ una extensió de Galois de cossos. L'assignació $H \mapsto K^H|k$ defineix una bijecció que inverteix l'ordre donat per inclusió del conjunt dels subgrups tancats de $\mathrm{Gal}(K|k)$ *en el conjunt de totes les subextensions $L|k$ de $K|k$, amb inversa donada per $L|k \mapsto \mathrm{Gal}(K|L)$. I els subgrups oberts es corresponen exactament amb les extensions finites.*

Notem que la bijecció que predica el teorema no es restringeix ni a subextensions finites, ni a subextensions de Galois.

Teorema fonamental de la teoria de Galois

Teorema (fonamental de la teoria de Galois)

Sigui $K|k$ una extensió de Galois de cossos. L'assignació $H \mapsto K^H|k$ defineix una bijecció que inverteix l'ordre donat per inclusió del conjunt dels subgrups tancats de $\mathrm{Gal}(K|k)$ *en el conjunt de totes les subextensions $L|k$ de $K|k$, amb inversa donada per $L|k \mapsto \mathrm{Gal}(K|L)$. I els subgrups oberts es corresponen exactament amb les extensions finites.*

Notem que la bijecció que predica el teorema no es restringeix ni a subextensions finites, ni a subextensions de Galois.

La consideració de subextensions finites i de Galois només és per a la definició de la topologia de Krull.

Teorema fonamental de la teoria de Galois

Teorema (fonamental de la teoria de Galois)

Sigui $K|k$ una extensió de Galois de cossos. L'assignació $H \mapsto K^H|k$ defineix una bijecció que inverteix l'ordre donat per inclusió del conjunt dels subgrups tancats de $\mathrm{Gal}(K|k)$ *en el conjunt de totes les subextensions $L|k$ de $K|k$, amb inversa donada per $L|k \mapsto \mathrm{Gal}(K|L)$. I els subgrups oberts es corresponen exactament amb les extensions finites.*

Notem que la bijecció que predica el teorema no es restringeix ni a subextensions finites, ni a subextensions de Galois.

La consideració de subextensions finites i de Galois només és per a la definició de la topologia de Krull.

No en detallaré aquí cap demostració (tot i que no és difícil).

Teorema fonamental de la teoria de Galois (cont.)

Proposició

Una definició equivalent de la topologia de Krull s'obté en considerar com a (una) base d'entorns oberts de cada element $\sigma \in \mathrm{Gal}(K|k)$, *la família formada per totes les classes laterals* $\sigma\,\mathrm{Gal}(K|L)$, *quan* $L|k$ *recorre totes les subextensions de Galois finites de* $K|k$.

Teorema fonamental de la teoria de Galois (cont.)

Proposició

Una definició equivalent de la topologia de Krull s'obté en considerar com a (una) base d'entorns oberts de cada element $\sigma \in \mathrm{Gal}(K|k)$, *la família formada per totes les classes laterals* $\sigma\,\mathrm{Gal}(K|L)$, *quan* $L|k$ *recorre totes les subextensions de Galois finites de* $K|k$.

Això equival a establir un homeomorfisme entre els grups topològics $\mathrm{Gal}(K|k)$ (amb la topologia definida d'aquesta manera) i el subgrup del producte cartesià,

$$\varprojlim_{L|k \text{ de Galois, finita, } L\subseteq K} \mathrm{Gal}(L|k),$$

amb la topologia induïda, com hem fet més amunt.

Exemples

Si, per a un cos finit $\mathbb{F}_q$, en comptes de considerar totes les extensions finites $\mathbb{F}_{q^n}|\mathbb{F}_q$ considerem només les de grau potència d'un nombre primer ℓ (que pot ser igual o diferent de la característica), és a dir, $n = \ell^m$, tenim que la família de grups de Galois sobre $\mathbb{F}_q$ és una família de grups cíclics d'ordre ℓ^m, per a tot $m \geq 0$.

Exemples

Si, per a un cos finit $\mathbb{F}_q$, en comptes de considerar totes les extensions finites $\mathbb{F}_{q^n}|\mathbb{F}_q$ considerem només les de grau potència d'un nombre primer ℓ (que pot ser igual o diferent de la característica), és a dir, $n = \ell^m$, tenim que la família de grups de Galois sobre $\mathbb{F}_q$ és una família de grups cíclics d'ordre ℓ^m, per a tot $m \geq 0$.

I per al cos $\mathbb{F}_{q^{\ell^\infty}}$, reunió de tots els $\mathbb{F}_{q^{\ell^m}}$, $\mathbb{F}_{q^{\ell^\infty}} = \bigcup_{m\geq 0} \mathbb{F}_{q^{\ell^m}}$,

tenim que el grup de Galois sobre $\mathbb{F}_q$, $\mathrm{Gal}(\mathbb{F}_{q^{\ell^\infty}}|\mathbb{F}_q)$, és isomorf (com a grup topològic) al grup additiu de l'anell

$$\mathbb{Z}_\ell := \varprojlim_m (\mathbb{Z}/\ell^m\mathbb{Z}).$$

Exemples

Si, per a un cos finit $\mathbb{F}_q$, en comptes de considerar totes les extensions finites $\mathbb{F}_{q^n}|\mathbb{F}_q$ considerem només les de grau potència d'un nombre primer ℓ (que pot ser igual o diferent de la característica), és a dir, $n = \ell^m$, tenim que la família de grups de Galois sobre $\mathbb{F}_q$ és una família de grups cíclics d'ordre ℓ^m, per a tot $m \geq 0$.

I per al cos $\mathbb{F}_{q^{\ell^\infty}}$, reunió de tots els $\mathbb{F}_{q^{\ell^m}}$, $\mathbb{F}_{q^{\ell^\infty}} = \bigcup_{m\geq 0} \mathbb{F}_{q^{\ell^m}}$,

tenim que el grup de Galois sobre $\mathbb{F}_q$, $\mathrm{Gal}(\mathbb{F}_{q^{\ell^\infty}}|\mathbb{F}_q)$, és isomorf (com a grup topològic) al grup additiu de l'anell

$$\mathbb{Z}_\ell := \varprojlim_m (\mathbb{Z}/\ell^m\mathbb{Z}).$$

Aquest anell s'anomena l'anell dels nombres enters ℓ-àdics.

Exemples (cont.)

Observació

La construcció de $\mathbb{Z}_\ell$ a partir dels $\mathbb{Z}/\ell^m\mathbb{Z}$ és la construcció de successions coherents de nombres enters mòdul les successives potències de ℓ.

Exemples (cont.)

Observació

La construcció de $\mathbb{Z}_\ell$ a partir dels $\mathbb{Z}/\ell^m\mathbb{Z}$ és la construcció de successions coherents de nombres enters mòdul les successives potències de ℓ.

Això imita el mètode de Newton de la tangent, que ensenya Gauss a les Disquisicions Aritmètiques, i que s'explica a l'assignatura d'Aritmètica, per a *aixecar* arrels de polinomis mòdul una potència ℓ^m d'un nombre primer ℓ, a la potència següent, ℓ^{m+1}.

Exemples (cont.)

Observació

La construcció de $\mathbb{Z}_\ell$ a partir dels $\mathbb{Z}/\ell^m\mathbb{Z}$ és la construcció de successions coherents de nombres enters mòdul les successives potències de ℓ.

Això imita el mètode de Newton de la tangent, que ensenya Gauss a les Disquisicions Aritmètiques, i que s'explica a l'assignatura d'Aritmètica, per a *aixecar* arrels de polinomis mòdul una potència ℓ^m d'un nombre primer ℓ, a la potència següent, ℓ^{m+1}.

Aquest resultat demostra que *si un polinomi de coeficients enters té una arrel simple mòdul ℓ, té una arrel simple en $\mathbb{Z}_\ell$* (lema de Hensel).

Exemples (cont.)

El teorema fonamental de l'Aritmètica —*tot nombre enter* $n > 0$ *és producte de potències de nombres primers,* $n = \prod_{\ell} \ell^{v_\ell(n)}$—, i el teorema xinès del residu —$\mathbb{Z}/n\mathbb{Z} \cong \prod_{\ell} \mathbb{Z}/\ell^{v_\ell(n)}\mathbb{Z}$—, impliquen la descomposició

Teorema

$$\hat{\mathbb{Z}} \cong \prod_{\ell} \mathbb{Z}_\ell. \ \square$$

Exemples (cont.)

El teorema fonamental de l'Aritmètica —*tot nombre enter* $n > 0$ *és producte de potències de nombres primers,* $n = \prod_\ell \ell^{v_\ell(n)}$—, i el teorema xinès del residu —$\mathbb{Z}/n\mathbb{Z} \cong \prod_\ell \mathbb{Z}/\ell^{v_\ell(n)}\mathbb{Z}$—, impliquen la descomposició

Teorema

$$\hat{\mathbb{Z}} \cong \prod_\ell \mathbb{Z}_\ell. \ \square$$

En conseqüència, els anells (els grups abelians additius) $\mathbb{Z}_\ell$ són quocients de l'anell (del grup abelià additiu) $\hat{\mathbb{Z}}$.

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,
- de característica zero,

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,
- de característica zero,
- principal,

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,
- de característica zero,
- principal,
- té un únic ideal primer no nul, $\ell\mathbb{Z}_\ell$,

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,
- de característica zero,
- principal,
- té un únic ideal primer no nul, $\ell\mathbb{Z}_\ell$, amb cos residual $(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) \cong \mathbb{F}_\ell = (\mathbb{Z}/\ell\mathbb{Z})$,

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,
- de característica zero,
- principal,
- té un únic ideal primer no nul, $\ell\mathbb{Z}_\ell$, amb cos residual $(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) \cong \mathbb{F}_\ell = (\mathbb{Z}/\ell\mathbb{Z})$,
- tots els nombres enters no divisibles per ℓ hi són elements invertibles,

Exemples (cont.)

Però, així com $\hat{\mathbb{Z}}$ és un producte cartesià no trivial i, per tant, té divisors de zero no nuls, els anells $\mathbb{Z}_\ell$ tenen altres propietats interessants. Per exemple, $\mathbb{Z}_\ell$

- és un domini d'integritat,
- de característica zero,
- principal,
- té un únic ideal primer no nul, $\ell\mathbb{Z}_\ell$, amb cos residual $(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) \cong \mathbb{F}_\ell = (\mathbb{Z}/\ell\mathbb{Z})$,
- tots els nombres enters no divisibles per ℓ hi són elements invertibles,
- i per al grup dels seus elements invertibles, es té que

$$\mathbb{Z}_\ell^* \cong \begin{cases} (\mathbb{Z}/(\ell-1)\mathbb{Z}) \times \mathbb{Z}_\ell, & \text{si } \ell \neq 2, \\ (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_2, & \text{si } \ell = 2. \end{cases}$$

Exemples (cont.)

Alguns resultats provats en aquest curs sobre els cossos ciclotòmics proporcionen els resultats següents.

Exemples (cont.)

Alguns resultats provats en aquest curs sobre els cossos ciclotòmics proporcionen els resultats següents.

Teorema

Sigui $\mu(\overline{\mathbb{Q}})$ el grup de totes les arrels de la unitat de $\overline{\mathbb{Q}}$. L'extensió $\mathbb{Q}(\mu(\overline{\mathbb{Q}}))|\mathbb{Q}$ és de Galois i

$$\mathrm{Gal}(\mathbb{Q}(\mu(\overline{\mathbb{Q}}))|\mathbb{Q}) \cong \hat{\mathbb{Z}}^* \cong (\mathbb{Z}/2\mathbb{Z}) \times \prod_{\ell}(\mathbb{Z}/(\ell-1)\mathbb{Z}) \times \prod_{\ell} \mathbb{Z}_\ell.$$

Exemples (cont.)

Corol·lari

Sigui $K \subseteq \overline{Q}$ el cos composició de tots els cossos quadràtics sobre $\mathbb{Q}$. Llavors, $K|\mathbb{Q}$ és de Galois i

$$\mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \prod_{\ell} (\mathbb{Z}/2\mathbb{Z}),$$

un factor $\mathbb{Z}/2\mathbb{Z}$ per a cada nombre primer (inclòs el primer 2), i un factor $\mathbb{Z}/2\mathbb{Z}$ extra. $\square$

Exemples (cont.)

Els anells $\mathbb{Z}_\ell$ són dominis d'integritat topològics compactes.

Exemples (cont.)

Els anells $\mathbb{Z}_\ell$ són dominis d'integritat topològics compactes.

I, igual que també ho és l'anell de Prüfer, són complets per a la topologia del límit projectiu.

Exemples (cont.)

Els anells $\mathbb{Z}_\ell$ són dominis d'integritat topològics compactes.

I, igual que també ho és l'anell de Prüfer, són complets per a la topologia del límit projectiu.

Com a conseqüència, el cos de fraccions, $\mathbb{Q}_\ell$, de $\mathbb{Z}_\ell$ és un cos topològic complet, que conté $\mathbb{Q}$ com a subcòs.

Exemples (cont.)

Els anells $\mathbb{Z}_\ell$ són dominis d'integritat topològics compactes.

I, igual que també ho és l'anell de Prüfer, són complets per a la topologia del límit projectiu.

Com a conseqüència, el cos de fraccions, $\mathbb{Q}_\ell$, de $\mathbb{Z}_\ell$ és un cos topològic complet, que conté $\mathbb{Q}$ com a subcòs.

De fet, és la compleció de $\mathbb{Q}$ per al valor absolut ℓ-àdic de $\mathbb{Q}$, de la mateixa manera que $\mathbb{R}$ és la compleció de $\mathbb{Q}$ per al valor absolut arquimedià usual.

Exemples (cont.)

Se satisfà que *totes les extensions finites* $L|\mathbb{Q}_\ell$ *són resolubles*,

Exemples (cont.)

Se satisfà que *totes les extensions finites* $L|\mathbb{Q}_\ell$ *són resolubles*,

igual que *totes les extensions finites de* $\mathbb{R}$ *són resolubles*;

Exemples (cont.)

Se satisfà que *totes les extensions finites* $L|\mathbb{Q}_\ell$ *són resolubles*,

igual que *totes les extensions finites de* $\mathbb{R}$ *són resolubles*;

és a dir, que *totes les equacions polinòmiques sobre* $\mathbb{Q}_\ell$ *són resolubles per radicals* (sobre $\mathbb{Q}_\ell$),

Exemples (cont.)

Se satisfà que *totes les extensions finites* $L|\mathbb{Q}_\ell$ *són resolubles*,

igual que *totes les extensions finites de* $\mathbb{R}$ *són resolubles*;

és a dir, que *totes les equacions polinòmiques sobre* $\mathbb{Q}_\ell$ *són resolubles per radicals* (sobre $\mathbb{Q}_\ell$),

igual que *totes les equacions polinòmiques sobre* $\mathbb{R}$ *són resolubles per radicals* (sobre $\mathbb{R}$);

Exemples (cont.)

Se satisfà que *totes les extensions finites* $L|\mathbb{Q}_\ell$ *són resolubles*,

igual que *totes les extensions finites de* $\mathbb{R}$ *són resolubles*;

és a dir, que *totes les equacions polinòmiques sobre* $\mathbb{Q}_\ell$ *són resolubles per radicals* (sobre $\mathbb{Q}_\ell$),

igual que *totes les equacions polinòmiques sobre* $\mathbb{R}$ *són resolubles per radicals* (sobre $\mathbb{R}$);

i que *el grup de Galois absolut,* $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell|\mathbb{Q}_\ell)$ *és un subgrup del grup de Galois absolut de* $\mathbb{Q}$, $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$,

Exemples (cont.)

Se satisfà que *totes les extensions finites* $L|\mathbb{Q}_\ell$ *són resolubles*,

igual que *totes les extensions finites de* $\mathbb{R}$ *són resolubles*;

és a dir, que *totes les equacions polinòmiques sobre* $\mathbb{Q}_\ell$ *són resolubles per radicals* (sobre $\mathbb{Q}_\ell$),

igual que *totes les equacions polinòmiques sobre* $\mathbb{R}$ *són resolubles per radicals* (sobre $\mathbb{R}$);

i que *el grup de Galois absolut,* $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell|\mathbb{Q}_\ell)$ *és un subgrup del grup de Galois absolut de* $\mathbb{Q}$, $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$,

igual que *el grup de Galois absolut,* $\mathrm{Gal}(\overline{\mathbb{R}}|\mathbb{R})$ *és un subgrup del grup de Galois absolut de* $\mathbb{Q}$, $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

• Si k és algebraicament tancat (o més generalment, separablement tancat),

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

• Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal,

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial. (Teorema d'Artin-Schreier)

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial. (Teorema d'Artin-Schreier)

- Si $k = \mathbb{F}$ és un cos finit,

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial. (Teorema d'Artin-Schreier)

- Si $k = \mathbb{F}$ és un cos finit, $G_k \cong \hat{\mathbb{Z}}$.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial. (Teorema d'Artin-Schreier)

- Si $k = \mathbb{F}$ és un cos finit, $G_k \cong \hat{\mathbb{Z}}$. És un grup abelià.

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial. (Teorema d'Artin-Schreier)

- Si $k = \mathbb{F}$ és un cos finit, $G_k \cong \hat{\mathbb{Z}}$. És un grup abelià.
- Si k és un cos ℓ-àdic (extensió finita de $\mathbb{Q}_\ell$),

El grup de Galois absolut en general

Acabem amb alguns exemples, només a títol informatiu.
Per a un cos k, posem $G_k := \mathrm{Gal}(k^s|k)$, el seu grup de Galois absolut.

- Si k és algebraicament tancat (o més generalment, separablement tancat), G_k és el grup trivial, $G_k = \{1\}$.
- Si k és un cos (totalment) ordenat maximal, $G_k \cong \mathbb{Z}/2\mathbb{Z}$.

Són els únics cossos k per als quals G_k és finit i no trivial. (Teorema d'Artin-Schreier)

- Si $k = \mathbb{F}$ és un cos finit, $G_k \cong \hat{\mathbb{Z}}$. És un grup abelià.
- Si k és un cos ℓ-àdic (extensió finita de $\mathbb{Q}_\ell$), G_k és un grup (pro)-resoluble.

El grup de Galois absolut en general

Observacions

Notem, doncs, que

• totes les extensions d'un cos finit són abelianes (tots els quocients d'un grup abelià són abelians),

El grup de Galois absolut en general

Observacions

Notem, doncs, que

- totes les extensions d'un cos finit són abelianes (tots els quocients d'un grup abelià són abelians),
- tots els subgrups tancats del grup de Galois absolut d'un cos ℓ-àdic són pro-resolubles; i, els seus quocients, pro-resolubles (i els quocients per subgrups oberts, resolubles).

El grup de Galois absolut en general

Observacions

Notem, doncs, que

• totes les extensions d'un cos finit són abelianes (tots els quocients d'un grup abelià són abelians),

• tots els subgrups tancats del grup de Galois absolut d'un cos ℓ-àdic són pro-resolubles; i, els seus quocients, pro-resolubles (i els quocients per subgrups oberts, resolubles).

• El grup de Galois absolut de $\mathbb{Q}$ és molt més complicat; de fet, hem vist exemples explícits de quocients no resolubles, per exemple, de grup de Galois isomorf al grup simètric S_5.

El grup de Galois absolut en general

Observacions

Notem, doncs, que

- totes les extensions d'un cos finit són abelianes (tots els quocients d'un grup abelià són abelians),
- tots els subgrups tancats del grup de Galois absolut d'un cos ℓ-àdic són pro-resolubles; i, els seus quocients, pro-resolubles (i els quocients per subgrups oberts, resolubles).
- El grup de Galois absolut de $\mathbb{Q}$ és molt més complicat; de fet, hem vist exemples explícits de quocients no resolubles, per exemple, de grup de Galois isomorf al grup simètric S_5.
- ...

El grup de Galois absolut en general

Observacions

Notem, doncs, que

- totes les extensions d'un cos finit són abelianes (tots els quocients d'un grup abelià són abelians),
- tots els subgrups tancats del grup de Galois absolut d'un cos ℓ-àdic són pro-resolubles; i, els seus quocients, pro-resolubles (i els quocients per subgrups oberts, resolubles).
- El grup de Galois absolut de $\mathbb{Q}$ és molt més complicat; de fet, hem vist exemples explícits de quocients no resolubles, per exemple, de grup de Galois isomorf al grup simètric S_5.
- ...
- Es conjectura que *tot grup finit és grup de Galois d'una extensió finita de* $\mathbb{Q}$; és a dir, que *tot grup finit és quocient del grup de Galois absolut de* $\mathbb{Q}$.

El grup de Galois absolut en general

Observacions

Notem, doncs, que

- totes les extensions d'un cos finit són abelianes (tots els quocients d'un grup abelià són abelians),
- tots els subgrups tancats del grup de Galois absolut d'un cos ℓ-àdic són pro-resolubles; i, els seus quocients, pro-resolubles (i els quocients per subgrups oberts, resolubles).
- El grup de Galois absolut de $\mathbb{Q}$ és molt més complicat; de fet, hem vist exemples explícits de quocients no resolubles, per exemple, de grup de Galois isomorf al grup simètric S_5.
- ...
- Es conjectura que *tot grup finit és grup de Galois d'una extensió finita de* $\mathbb{Q}$; és a dir, que *tot grup finit és quocient del grup de Galois absolut de* $\mathbb{Q}$.
- ...

Acabo...

Acabo...

Només un desig final, que reprodueix unes paraules de Galois, de la seva darrera carta.

Acabo...

Només un desig final, que reprodueix unes paraules de Galois, de la seva darrera carta.

Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

Cronologia

Euclides (Εὐκλείδης) Euclides d'Alexandria (Alexandria, Egipte, aprox. 323 a.C.; Alexandria, Egipte, aprox. 285 a.C.)

Pierre de **Fermat** (Beaumont de Lomagne, França, 17 d'agost de 1601; Castres, França, 12 de gener de 1665)

Isaac **Newton** (Woolfsthorpe by Colsterworth, Anglaterra, 25 de desembre de 1642 (Ju), 4 de gener de 1643 (Gr); Kensington, Anglaterra, 20 de març de 1717 (Ju), 31 de març de 1717 (Gr))

Johann Carl Friedrich **Gauss** (Brunsvic, Baixa Saxònia, Sacre Imperi, 30 d'abril de 1777; Göttingen, Baixa Saxònia, Prússia, 23 de febrer de 1855)

Cronologia (cont.)

Bernard Placidus Johann Nepomuk **Bolzano** (Praga, Bohèmia, Imperi Austro-Húngar (ara República Txeca), 5 d'octubre de 1781; Praga, Bohèmia, Imperi Austro-Húngar (ara República Txeca) 18 de desembre de 1848)

Évariste **Galois** (Bourg la Reine, París, França, 25 d'octubre de 1811; París, França, 31 de maig de 1832)

Ferdinand Georg **Frobenius** (Berlín–Charlottenburg, Prússia, 26 d'octubre de 1849; Berlín, Prússia, Imperi Alemany, 3 d'agost de 1917)

Kurt **Hensel** (Königsberg, Prússia, 29 de desembre de 1861; Marburg, Hessen, Alemanya, 1 de juny de 1941)

Cronologia (cont.)

Ernst Paul Heinz **Prüfer** (Wilhelmshaven, Alemanya, 10 de novembre de 1896; Münster, Alemanya, 7 d'abril de 1934)

Emil **Artin** (Viena, Àustria, Imperi Austrohongarès, 3 de març de 1898; Hamburg, Alemanya, 20 de desembre de 1962)

Wolfgang **Krull** (Baden–Baden, Baden Württemberg, Imperi Alemany, 26 d'agost de 1899; Bonn, Rin del Nord Westfàlia, Alemanya, 12 d'abril de 1971)

Otto **Schreier** (Viena, Àustria, 3 de març de 1901; Hamburg, Alemanya, 2 de juny de 1929)

Cronologia (cont.)

Max August **Zorn** (Krefeld, Alemanya, 6 de juny de 1906; Bloomington, Indiana, Estats Units, 9 de març de 1993)

Andrey Nikolayevich **Tykhonov** (Gzhatska, Smolensk, Imperi rus, 17 d'octubre de 1906 (Ju), 30 d'octubre de 1906 (Gr); Moscow, Rússia, 7 d'octubre de 1993)

Griselda **Pascual** Xufré (Barcelona, 11 de febrer de 1926; Barcelona. 8 de juny de 2001)

Jürgen **Neukirch** (Dortmund, Alemanya, 24 de juliol de 1937; Regensburg, Alemanya, 5 de febrer de 1997)

Referències

[Ga 1801] Gauss, C. F.: *Disquisicions Aritmètiques*. Traducció i pròleg de Griselda Pascual Xufré. Institut d'Estudis Catalans, Barcelona, 1996. ISBN: 84-7283-313-5.

[Ne 1986] Neukirch, J.: *Class Field Theory*, Springer Verlag, Grundlehren der mathematischen Wissenschaften, **280**, Berlin (1986), ISBN: 3-540-152251-2.

[Ba-Mo-Tr 1990] Bayer, P.; Montes, J.; Travesa, A.: *Problemes d'Àlgebra*, Publicacions de la Universitat de Barelona, col·lecció Materials Docents, n. 7 (1990), ISBN: 84-7875-361-3.

UNIVERSITAT DE BARCELONA