Àlgebra Abstracta curs 07/08
Teorema de Jordan-Hölder

Jordi Quer

28 de setembre de 2007

El teorema d'isomorfisme diu: per a tot morfisme de grups $f\colon G_1 \to G_2$ l'aplicació $a(\ker f) \mapsto f(a)$ és un isomorfisme entre el grup quocient $G_1/\ker f$ i el grup imatge $\operatorname{im} f = f(G_1)$.

Proposició 1 *Els resultats següents es coneixen també, de vegades, com a teoremes d'isomorfisme.*

1. *Siguin H i K subgrups normals de G amb $H \subseteq K$. Aleshores*
$$\frac{G/H}{K/H} \simeq G/K.$$
2. *Sigui $f\colon G_1 \to G_2$ un morfisme i H_2 un subgrup normal de G_2. Aleshores $H_1 = f^{-1}(H_2)$ és un subgrup normal de G_1 i l'aplicació $f_*(aH_1) = f(a)H_2$ és un monomorfisme $G_1/H_1 \to G_2/H_2$. Si f és exhaustiu, aleshores f_* és un isomorfisme.*
3. *Siguin H i K subgrups de G tals que HK és un subgrup del qual H n'és subgrup normal[1]. Aleshores*
$$K/(H \cap K) \simeq HK/H.$$

Prova: 1. Es defineix $f\colon G/H \to G/K$ posant $f(aH) = aK$. Està ben definit ja que si $aH = bH$ aleshores $b^{-1}a \in H \subseteq K$ i per tant $aK = bK$. És clarament morfisme gràcies al fet de ser K normal. És exhaustiu. Finalment,
$$aH \in \ker f \Leftrightarrow f(aH) = aK = K \Leftrightarrow a \in K \Leftrightarrow aH \in K/H,$$
i el teorema d'isomorfisme ens dóna el resultat.

2. Per a tot $h \in H_1$ i $a \in G_1$ és $f(aha^{-1}) = f(a)f(h)f(a)^{-1} \in H_2$. Per tant $aha^{-1} \in H_1$ i H_1 és normal. Si $aH_1 = bH_1$ aleshores $b^{-1}a \in H_1$ i per tant $f(b)^{-1}f(a) \in H_2$, d'on resulta que $f(a)H_2 = f(b)H_2$ i l'aplicació està ben definida. De la normalitat dels grups es dedueix immediatament que és morfisme. Com que
$$f_*(aH_1) = f(a)H_2 = H_2 \Leftrightarrow f(a) \in H_2 \Leftrightarrow a \in f^{-1}(H_2) = H_1 \Leftrightarrow aH_1 = H_1$$
el morfisme f_* és injectiu. Si f és exhaustiu tot element bH_2 és imatge d'algun aH_1 per un element $a \in G_1$ tal que $f(a) = b$, de manera que f_* també és exhaustiu.

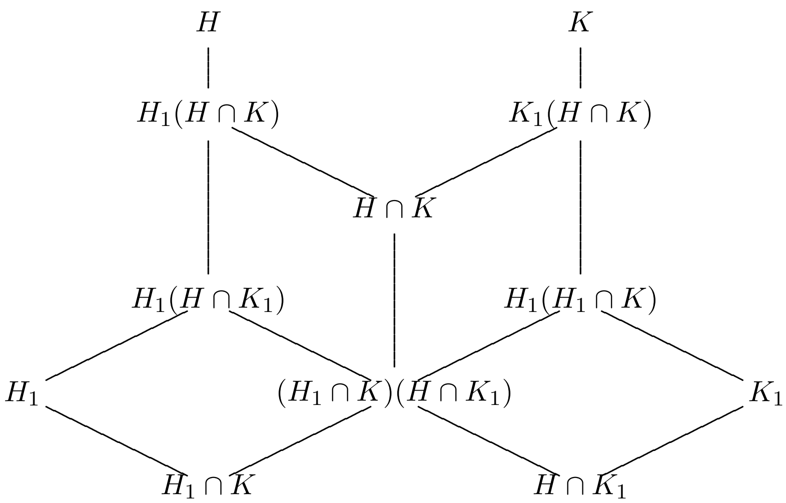
[1] Es compleix sempre que H sigui normal a G, que és una condició més forta amb la que moltes vegades s'enuncia aquest resultat.

3. La condició de que H sigui normal a HK implica que $kH = Hk$ per a tot $k \in K$, que és simplement la condició de normalitat aplicada a $k = 1 \cdot k \in HK$. Per a tot $k \in K$ i $a \in H \cap K$ és $kak^{-1} \in H \cap K$ i $H \cap K$ és normal a K. Es considera la composició de la inclusió $K \to HK$ amb la projecció canònica $HK \to HK/H$. Clarament, el nucli d'aquest morfisme és $H \cap K$ i del teorema d'isomorfisme se'n dedueix el resultat. □

Lema 2 (Lema de Zassenhaus o de la papallona) *Siguin H i K subgrups de G i H_1, K_1 subgrups normals de H i K, respectivament. Aleshores:*

$$\frac{H_1(H \cap K)}{H_1(H \cap K_1)} \simeq \frac{H \cap K}{(H_1 \cap K)(H \cap K_1)} \simeq \frac{(H \cap K)K_1}{(H_1 \cap K)K_1}$$

Prova: El nom del lema ve del diagrama de subgrups següent:



La demostració del lema es redueix pràcticament a comprovar que tots els grups que apareixen en aquest diagrama com a productes de subgrups són efectivament grups (o sigui, els dos factors commuten) i que les relacions d'inclusió estan ben posades, el qual és pràcticament immediat, i que els subgrups pels quals es fa quocient en l'enunciat són efectivament subgrups normals.

Quant al producte de subgrups, per exemple, per a tot $a \in H \cap K$ es té $aH_1 = H_1 a$, ja que $a \in H$ i H_1 és normal a H. La resta es fan exactament igual.

Si $a \in H_1$ i $b \in H \cap K$ aleshores

$$abH_1(H \cap K_1) = H_1(H \cap K_1)b = (H \cap K_1)H_1 b = H_1(H \cap K_1)ab,$$

i per tant $H_1(H \cap K_1)$ és normal a $H_1(H \cap K)$. El fet que el denominador del grup del mig és normal en el numerador és immediat.

Siguin $U = H_1(H \cap K_1)$ i $V = H \cap K$. Aleshores $UV = H_1(H \cap K)$, $U \cap V = (H_1 \cap K)(H \cap K_1)$, U és normal a UV, i aplicant el teorema d'isomorfisme $UV/V \simeq U/(U \cap V)$ s'obté el resultat. □

Definició 1 (Torre de subgrups) *Donat un grup G, una* torre normal de subgrups *és una successió*

$$G = H_1 \supseteq H_2 \supseteq H_3 \supseteq \cdots \supseteq H_r = 1.$$

on cada H_i és normal a H_{i+1}.

Un *refinament* d'una torre normal és una altra torre normal obtinguda intercalant subgrups a la primera. Un refinament és *trivial* quan tots els subgrups afegits ja formaven part de la torre de partida.

S'anomenen *quocients* d'una torre normal els grups H_i/H_{i+1}, $1 \leqslant i \leqslant r-1$. Un refinament trivial afegeix quocients trivials als quocients de la torre de partida.

Dues torres normals es diuen *equivalents* si tenen la mateixa longitud i els seus quocients són isomorfs, llevat d'una permutació.

Exemples:

- tot grup té una torre normal trivial $G \supseteq \{1\}$;
- $D_{2n} \supseteq C_n \supseteq \{1\}$;
- $\mathfrak{S}_4 \supseteq V_4 \supseteq \{1\}$, on $V_4 \simeq C_2 \times C_2$ és el grup d'ordre 4 format pels tres productes de dues transposicions disjuntes més l'element neutre, amb quocients isomorfs a $\mathfrak{S}_3$ i V_4;
- $\mathfrak{S}_4 \supseteq \mathfrak{A}_4 \supseteq V_4 \supseteq C_2 \supseteq \{1\}$ és un refinament de l'anterior amb quocients isomorfs als grups C_2, C_3, C_2, C_2.

Teorema 3 (Teorema de Schreier) *Dues torres normals d'un grup sempre tenen refinaments equivalents.*

PROVA: Siguin

$$G = H_1 \supseteq H_2 \cdots \supseteq H_r = 1,$$

$$G = K_1 \supseteq K_2 \cdots \supseteq K_s = 1$$

dues torres normals d'un grup G. Es consideren els grups

$$H_{i,j} = H_{i+1}(K_j \cap H_i), \quad 1 \leqslant i \leqslant r-1, \quad 1 \leqslant j \leqslant s.$$

Aquests grups són un refinament de la primera torre, ja que

$$H_i = H_{i,1} \supseteq H_{i,2} \supseteq \cdots \supseteq H_{i,s-1} \supseteq H_{i,s} = H_{i+1}.$$

Quan $i < r-1$, $H_{i,s} = H_{i+1} = H_{i+1,1}$, i s'identificaran aquests dos grups (però conservant la doble notació). La longitud del refinament és $(r-1)(s-1)+1$.

Anàlogament, els grups

$$K_{i,j} = K_{j+1}(K_j \cap H_i), \quad 1 \leqslant i \leqslant r, \quad 1 \leqslant j \leqslant s-1,$$

són un refinament de la segona torre. També en aquest cas, per $j < s-1$ és $K_{r,j} = K_{r+1} = K_{r+1,1}$ i, identificant aquests grups, es té també un refinament de longitud $(r-1)(s-1)+1$.

Els dos refinaments així construïts són equivalents. En efecte, per i, j amb $1 \leqslant i \leqslant r-1$ i $1 \leqslant j \leqslant s-1$, el lema de Zassenhaus, aplicat als grups H_i, K_j i als seus subgrups normals H_{i+1}, K_{j+1}, respectivament, dona un isomorfisme

$$\frac{H_{i,j}}{H_{i,j+1}} = \frac{H_{i+1}(H_i \cap K_j)}{H_{i+1}(H_i \cap K_{j+1})} \simeq \frac{K_{j+1}(H_i \cap K_j)}{K_{j+1}(H_{i+1} \cap K_j)} = \frac{K_{i,j}}{K_{i+1,j}}.$$

$\square$

Definició 2 (Sèrie de composició) *Una* sèrie de composició *d'un grup G és una torre normal amb $H_i \neq H_{i+1}$ que no admet refinaments no trivials.*

Clarament, una torre normal és una sèrie de composició si, i només si, cadascun dels grups que hi apareixen és maximal en el conjunt dels subgrups normals de l'anterior.

És clar que tot grup finit té una sèrie de composició. Encara més, qualsevol torre normal d'un grup finit formada per subgrups diferents es pot refinar fins arribar a una sèrie de composició.

Teorema 4 (Teorema de Jordan-Hölder) *Totes les sèries de composició d'un grup són equivalents. Per tant, el conjunt dels grups simples que formen part d'una sèrie de composició d'un grup queda unívocament determinat per la classe d'isomorfisme del grup.*

PROVA: Donades dues sèries de composició d'un grup, pel Teorema de Schreier existeixen refinaments equivalents. Pel fet de tractar-se de sèries de composició, aquests refinaments han de ser trivials i no poden afegir-hi nous grups, sinó només repetir grups que ja hi eren. Per tant, els quocients dels refinaments són els quocients de les sèries de composició de partida afegint-hi alguns grups trivials. Com que els refinaments són equivalents, tenen els quocients isomorfs (llevat de l'ordre); en particular els quocients no trivials de l'un i l'altre (que són els de les sèries de composició) són isomorfs. $\square$

Definició 3 (Grup simple) *Un* grup simple *és un grup no trivial que no té subgrups normals propis no trivials.*

O sigui, un grup G tal que $H \lhd G \ \Rightarrow\ H = 1$ o $H = G$.

Per exemple, els grups (cíclics) d'ordre primer són simples i és clar que aquests són els únics grups abelians simples llevat d'isomorfisme.

Siguin G un grup i $H \subseteq G$ un subgrup normal. El quocient G/H és simple si, i només si, H és maximal en el conjunt dels subgrups normals propis de G.

Una torre normal és una sèrie de composició si, i només si, tots els seus quocients són grups simples.

Teorema 5 *Si $n \geqslant 5$ el grup alternat $\mathfrak{A}_n$ és simple.*

PROVA: Per veure-ho n'hi ha prou a comprovar els tres fets següents:

- $\mathfrak{A}_n$ està generat per 3-cicles;
- tots els 3-cicles són conjugats a $\mathfrak{A}_n$;
- tot subgrup normal no trivial d'$\mathfrak{A}_n$ conté algun 3-cicle.

Tenim que $(a_1, a_2)(a_2, a_3) = (a_1, a_2, a_3)$ i $(a_1, a_2)(a_3, a_4) = (a_1, a_2, a_3)(a_2, a_3, a_4)$. Com que tot element de $\mathfrak{A}_n$ és producte d'un nombre parell de transposicions, els 3-cicles el generen.

Donats 3-cicles (a_1, a_2, a_3) i (b_1, b_2, b_3), sigui $\sigma \in \mathfrak{S}_n$ una permutació amb $\sigma(a_i) = b_i$. Aleshores $\sigma(a_1, a_2, a_3)\sigma^{-1} = (b_1, b_2, b_3)$. Si $\sigma \in \mathfrak{A}_n$ ja hem acabat. En cas contrari, sigui $\tau = (a_4, a_5)$ amb a_4 i a_5 diferents de a_1, a_2, a_3 (això és possible si $n \geqslant 5$). Aleshores la permutació $\sigma\tau$ també envia a_i a b_i i és parella.

Sigui ara H un subgrup normal no trivial de $\mathfrak{A}_n$. Observem que si $\sigma \in H$ i τ és un 3-cicle, $\tau\sigma\tau^{-1}\sigma^{-1} \in H$. Considerem els casos següents, segons la descomposició en cicles disjunts d'un element $\sigma \in H$ no trivial:

- σ té un cicle de longitud $r \geqslant 4$, $\sigma = (a_1, a_2, a_3, a_4, \ldots, a_r)c_2 \cdots c_k$. Sigui τ el 3-cicle (a_1, a_2, a_3). Aleshores $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_3, a_1, a_4, \ldots, a_r)(a_r, \ldots, a_4, a_3, a_2, a_1) = (a_1, a_2, a_4)$, i H conté un 3-cicle.

- σ té dos cicles de longitud 3, $\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)c_3 \cdots c_k$. Sigui $\tau = (a_1, a_2, a_4)$. Tenim $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_4, a_3)(a_1, a_5, a_6)(a_3, a_2, a_1)(a_6, a_5, a_4) = (a_1, a_2, a_5, a_3, a_4)$ i pel cas anterior H conté un 3-cicle.

- σ té un cicle de longitud 3 i la resta de longitud 1 o 2. Aleshores $\sigma^2 \in H$ és un 3-cicle.

- σ descompon en producte de dues transposicions disjuntes, $\sigma = (a_1, a_2)(a_3, a_4)$. Escollim un a_5 diferent de a_1, a_2, a_3, a_4 (possible ja que $n \geqslant 5$). Sigui $\tau = (a_1, a_2, a_5)$. Aleshores $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_5)(a_1, a_2) = (a_1, a_5, a_2)$. Per tant H conté un 3-cicle.

- σ descompon en producte de més de dues transposicions disjuntes, $\sigma = (a_1, a_2)(a_3, a_4)(a_5, a_6)c_4 \cdots c_k$. Sigui $\tau = (a_1, a_2, a_3)$. Aleshores $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_3)(a_1, a_4)(a_1, a_2)(a_3, a_4) = (a_1, a_3)(a_2, a_4)$. Aplicant el cas anterior, H conté un 3-cicle.

Per tant, tot subgrup normal d'$\mathfrak{A}_n$ $(n \geqslant 5)$ conté un 3-cicle. Per tant, conté els seus conjugats per elements de $\mathfrak{A}_n$; en particular, conté tots els 3-cicles, de manera que ha de ser tot $\mathfrak{A}_n$. □

Definició 4 (Grups resolubles) *Un* grup resoluble *és un grup que admet una torre normal amb tots els quocients abelians.*

De vegades a una torre normal amb tots els quocients abelians se li diu una torre abeliana. És clar que els grups resolubles finits són exactament aquells que tenen com a quocients d'una serie de composició només grups cíclics d'ordre primer.

Proposició 6 *Tot subgrup (no necessàriament normal) i tot quocient d'un grup resoluble és resoluble. Una extensió d'un grup resoluble per un grup resoluble és resoluble.*

PROVA: Suposi's que G és resoluble, i sigui $G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = 1$ una torre abeliana. Si $H \subseteq G$ és un subgrup, siguin $H_i = H \cap G_i$. Aleshores la inclusió $H \to G$ indueix monomorfismes de H_i/H_{i+1} en G_i/G_{i+1}. Com que tot subgrup d'un abelià és abelià, H és resoluble. Si $K = G/H$ és un quocient de G per un subgrup normal H, siguin $K_i = \pi(G_i)$ les imatges dels G_i per la projecció canònica $\pi\colon G \to K$. Aleshores π indueix epimorfismes naturals $G_i \to K_i \to K_i/K_{i+1}$. Com que tot quocient d'un grup abelià és abelià, K és resoluble.

Suposi's que H i K són resolubles i que es té una successió exacta

$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1$$

Siguin $H = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_r = 1$ i $K = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_s = 1$ torres abelianes. Aleshores la torre de subgrups de G següent:

$$G = g^{-1}(K_1) \supseteq \cdots \supseteq g^{-1}(K_s) = \ker g = \operatorname{im} f = f(H_1) \supseteq \cdots \supseteq f(H_r) = 1$$

té quocients isomorfs als quocients de les dues torres anteriors, i per tant és una torre abeliana.
□

Alguns resultats importants sobre grups resolubles, que no es demostraran aquí, són: tot grup d'ordre lliure de quadrats és resoluble; tot grup d'ordre $p^n q^m$, amb p i q primers diferents, és resoluble (Burnside, 1904); tot grup d'ordre senar és resoluble (Feit-Thompson, 1962). En particular es dedueix que l'ordre de tot grup simple no abelià ha de ser divisible al menys per tres primers diferents, un dels quals ha de ser el 2, i un dels quals ha de dividir-lo al menys dues vegades. Observi's que $60 = 2^2 35$ és l'enter més petit que compleix aquesta condició.

Classificació dels grups finits. Pel Teorema de Jordan-Hölder, cada grup finit té associat un conjunt ben determinat de grups simples: els quocients d'una sèrie de composició. Aquest conjunt no determina encara la classe d'isomorfisme del grup. El problema de classificar (llevat d'isomorfisme) tots els grups finits es pot considerar en dues fases:

(1) Classificació dels grups simples finits: trobar tots els grups simples finits.

(2) Problema de les extensions: donats un grup K i un grup simple H, trobar tots els grups G que tenen un subgrup normal H' isomorf a H amb quocient G/H' isomorf a K.

El primer d'aquests dos problemes està resolt des de l'any 1980. La solució és el resultat de gairebé cent anys de feina d'una legió de matemàtics i la demostració completa ocupa diversos milers de pàgines d'articles a revistes. El resultat és el següent:

Hi ha 18 famílies infinites de grups simples. Per exemple, tres d'aquestes famílies són

- els grups cíclics d'ordre primer (grups C_p),
- els grups de permutacions parells (grups alternats $\mathfrak{A}_n$) quan $n \geqslant 5$, i
- els grups $\mathrm{PSL}(n,q) = \mathrm{SL}_n(\mathbb{F}_q)/\mathbb{F}_q^*, n \geqslant 2$, excepte si $n = 2$ i $q = 2$ o 3.

Les altres famílies admeten descripcions més o menys complicades en termes de grups de matrius sobre cossos finits.

A més de les 18 famílies hi ha 26 grups que no formen part de cap d'elles, que s'anomenen *grups esporàdics*. El més gran de tots té $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ elements i es coneix com "el monstre."

Les 18 famílies infinites i els 26 grups esporàdics exhaureixen tots els grups simples finits.