

Àlgebra Abstracta curs 07/08

Grups que operen en conjunts

Jordi Quer

4 d'octubre de 2007

Siguin G un grup i X un conjunt. Es diu que G *opera* (per l'esquerra) sobre X si es té una aplicació $G \times X \rightarrow X$, que es denotarà com un producte $(a, x) \mapsto ax$, tal que

$$a(bx) = (ab)x \quad \text{i} \quad 1x = x \quad \forall a, b \in G, x \in X.$$

També es diu que l'aplicació anterior dóna una *acció* de G sobre X . Un conjunt on hi ha donada una acció del grup G es diu de vegades un *G -conjunt*.

Per cada $a \in G$ l'aplicació "multiplicar per a " $m_a: x \mapsto ax$ és una permutació de X , i l'aplicació $a \mapsto m_a$ és un homomorfisme de G en el grup \mathfrak{S}_X de les permutacions del conjunt X . Recíprocament, qualsevol homomorfisme de grups $m: G \rightarrow \mathfrak{S}_X$, $a \mapsto m_a$, indueix una acció de G en X definida per $ax = m_a(x)$. Per tant, les accions de G sobre X (és a dir, les estructures de X com a G -conjunt) es corresponen bijectivament amb el conjunt dels homomorfismes de grups $G \rightarrow \mathfrak{S}_X$.

L'acció es diu *fidel* si elements de G diferents operen sobre X de forma diferent. O sigui, si l'homomorfisme $m: G \rightarrow \mathfrak{S}_X$ corresponent és injectiu. En aquest cas el grup G es pot identificar amb un subgrup de \mathfrak{S}_X .

Les definicions, tal com s'han donat, corresponen a accions per l'esquerra. També es poden considerar accions per la dreta i tot funciona anàlogament, obtenint-se una teoria que és la imatge en un mirall de l'anterior. Canviar de costat per a un grup donat és el mateix que treballar pel mateix costat però canviant el grup G pel seu oposat G^{op} .

Òrbites, punts fixos, estabilitzadors. L'òrbita de $x \in X$ és el conjunt Gx . Les òrbites formen una partició de X . El conjunt d'òrbites es denota $G \backslash X$ si l'acció és per l'esquerra; X/G si és per la dreta. L'element $x \in X$ és un *punt fix* si la seva òrbita es redueix al propi x , és a dir, si $ax = x$ per tot $a \in G$. L'acció es diu *transitiva* quan per tot parell $x, y \in X$ existeix un $a \in G$ amb $ax = y$, o sigui, quan el conjunt X consisteix en una única òrbita.

L'*estabilitzador* d'un element $x \in X$ és el subgrup format pels elements de G que el deixen fix, $G_x = \{a \in G \mid ax = x\}$. També se l'anomena *subgrup d'isotropia* de x . Els estabilitzadors dels elements d'una mateixa òrbita són subgrups conjugats: si $y = ax$ aleshores $G_y = aG_x a^{-1}$.

Si $Y \subseteq X$, l'estabilitzador de Y és el subgrup de G format pels elements que deixen fixos tots els elements de Y , o sigui, la intersecció dels G_x quan x recorre Y . L'estabilitzador de tot X és el subgrup format pels elements que operen trivialment, i coincideix amb el nucli de l'homomorfisme $m: G \rightarrow \mathfrak{S}_X$ associat. En particular $\ker m = \bigcap G_x$.

L'aplicació $ax \mapsto aG_x$ és una bijecció entre l'òrbita d'un $x \in X$ i les classes laterals per l'esquerra del seu estabilitzador G_x . En particular, $|Gx| = |G/G_x|$ i, si G és finit, el nombre

d'elements de cada òrbita divideix $|G|$. Quan X és finit es té la *fórmula de les òrbites*: si $\{x_i\}_{i \in I}$ és una família de representants de les diverses òrbites, aleshores

$$|X| = \sum_{i \in I} |Gx_i| = \sum_{i \in I} [G : Gx_i].$$

Translació i conjugació. Tot grup opera sobre ell mateix de dues maneres especialment importants. Per translació:

$$G \times G \rightarrow G \quad (a, b) \mapsto ab,$$

i per conjugació:

$$G \times G \rightarrow G \quad (a, b) \mapsto aba^{-1}.$$

L'acció per translació de G sobre ell mateix és transitiva i fidel, donant lloc a un monomorfisme $G \hookrightarrow \mathfrak{S}_G$ del grup G en el grup de les permutacions de G pensat com a conjunt (teorema de Cayley: tot grup finit és isomorf a un subgrup d'un grup de permutacions \mathfrak{S}_n). També es pot considerar l'acció per translació en el conjunt $\mathcal{P}(G)$ dels subconjunts de G posant $(a, S) \mapsto aS$ o sobre el conjunt G/H de les classes laterals per l'esquerra respecte un subgrup H fixat $(a, bH) \mapsto abH$. L'acció sobre les classes laterals és transitiva i l'estabilitzador de la classe aH és el subgrup conjugat aHa^{-1} . Per tant, aquesta acció és fidel si, i només si, $\bigcap_{a \in G} aHa^{-1} = 1$.

L'acció per conjugació de G sobre ell mateix és trivial si, i només si, el grup és abelià. Els seus punts fixos són els elements del centre $Z(G)$ i en general l'estabilitzador d'un element $a \in G$ és el seu centralitzador $Z_G(a) = \{g \in G : ga = ag\}$. Lla fórmula de les òrbites, aplicada a aquest cas, diu

$$|G| = |Z(G)| + \sum [G : Z_G(x)],$$

on al sumatori apareixen els índexs dels centralitzadors dels elements que no són del centre; o sigui, els cardinals de les classes de conjugació que contenen més d'un element. L'acció per conjugació es pot considerar també sobre el conjunt de les parts de G posant $(a, S) \mapsto aSa^{-1}$ o sobre el conjunt dels subgrups de G posant $(a, H) \mapsto aHa^{-1}$, ja que si H és un subgrup aleshores aHa^{-1} també ho és. Les òrbites d'aquesta acció s'anomenen de vegades classes de conjugació (d'un element, subconjunt o subgrup, segons on s'estigui operant). L'estabilitzador d'un subgrup H és el normalitzador $N_G(H) = \{g \in G : gHg^{-1} = H\}$, que és el subgrup de G més gran on H és normal. En particular, el nombre de conjugats d'un subgrup és igual a l'índex del seu normalitzador i un subgrup és normal si, i només si, el seu normalitzador és d'índex 1 (o sigui, és tot el grup G). El centre d'un grup està format pels punts fixos de l'acció per conjugació

Representacions. Quan X és un conjunt amb una estructura determinada (un anell, un mòdul, un espai vectorial, un espai topològic, mètric, analític, ...), les permutacions de X que conserven aquesta estructura, i tals que les seves inverses també la conserven, s'anomenen automorfismes. Per tal que tot funcioni correctament la composició d'aplicacions que conserven l'estructura també l'ha de conservar, de manera que la composició d'automorfismes sigui un automorfisme. Sigui $\text{Aut } X \subseteq \mathfrak{S}_X$ el subgrup corresponent. Una representació d'un grup G en X (considerat com a objecte amb estructura) és un homomorfisme de grups $\rho : G \rightarrow \text{Aut } X$. O sigui, és una estructura de G -conjunt sobre X amb la particularitat que les permutacions de X que corresponen als elements de G no són permutacions qualsevol sinó que sempre són automorfismes. Casos especialment importants són:

- Considerar X simplement com a conjunt. Els automorfismes són les permutacions. Aquest és el cas general que de l'acció d'un grup sobre un conjunt. Les representacions corresponents s'anomenen *representacions de permutació* de G .
- Sigui ara $X = A$ un grup abelià. Aut A està format per les permutacions de A que són morfismes de grups. Aquest cas s'estudia a la teoria de les *representacions de grups*.
- Sigui $X = V$ un espai vectorial sobre un cos K . Els automorfismes de V són aplicacions K -lineals invertibles i les representacions són homomorfismes $G \rightarrow \text{GL}(V)$. Es diuen *representacions lineals* i són la classe més important de representacions de grups. Quan V és de dimensió finita sobre K , en fixar una base es té una identificació de $\text{GL}(V)$ amb $\text{GL}_n(K)$. Per tant, una representació lineal en dimensió finita permet "veure" els elements d'un grup com a matrius.

1 p -Grups i grups de Sylow

Sigui p un nombre primer. Un grup finit és un *p -grup* si el seu ordre és una potència de p . Un *p -subgrup de Sylow* d'un grup finit G és un subgrup que té per ordre la màxima potència de p que divideix $|G|$.

Teorema 1 *Un p -grup no trivial té centre no trivial.*

Per tant, tot p -grup és resoluble i l'únic p -grup simple és C_p .

PROVA: Sigui G un p -grup no trivial. Es fa operar sobre ell mateix per conjugació. Per la fórmula de les òrbites, es té

$$|G| = |Z(G)| + \sum_x [G : G_x],$$

ja que cada punt fix és un element del centre $Z(G)$, i on els G_x són centralitzadors $Z_G(x)$ d'elements que no són del centre. Els índexs $[G : G_x]$ són divisors no trivials de $|G|$. Com que p divideix $|G|$ i també cada $[G : G_x]$, aleshores ha de dividir $|Z(G)|$. Per tant $Z(G)$ és no trivial.

Sigui G un p -grup. Per inducció sobre $|G|$ es demostrarà que és resoluble. Si $|G| = 1$ aleshores ho és. Si G és no trivial aleshores té centre no trivial, i es té una torre normal $G \supseteq Z(G) \supseteq \{1\}$. Com que el grup $Z(G)$ és abelià, és resoluble. El quocient $G/Z(G)$ és un p -grup d'ordre estrictament més petit que $|G|$, i per tant és resoluble. Com que G té un subgrup normal resoluble amb quocient resoluble, ell mateix és resoluble.

Els únics grups resolubles simples són els cíclics d'ordre primer, per tant l'únic p -grup no trivial resoluble és C_p . \square

Teorema 2 (Teorema de Cauchy) *Tot grup finit d'ordre divisible per un primer p conté algun element d'ordre p .*

PROVA: Es provarà primer per a grups abelians per inducció sobre $|A|$. Si $|A| = p$ aleshores tot element no trivial té ordre p . Altrament, sigui $a \in A$ un element no trivial d'ordre $n > 1$. Si $p \mid n$ aleshores $a^{n/p}$ és un element d'ordre p . Si $p \nmid n$ aleshores el grup quocient $A/\langle a \rangle$ té ordre $|A|/n$ divisible per p . Per hipòtesi d'inducció aquest quocient conté algun element d'ordre p ; tota antiimatge d'aquest element per la projecció canònica $\pi: A \rightarrow A/\langle a \rangle$ és un element de A d'ordre múltiple de p , i una potència seva té ordre p .

Alternativament, es pot fer servir el teorema de classificació dels grups abelians finits. Serà $A \simeq C_{d_1} \times \cdots \times C_{d_r}$ amb $d_i \mid d_{i+1}$ i com que $|A| = \prod d_i$ l'enter d_r ha de ser divisible per p . Aleshores el grup cíclic C_{d_r} conté elements d'ordre p i per tant A també.

A continuació es farà el cas general, també per inducció sobre l'ordre del grup. Es considera G operant sobre si mateix per conjugació. La fórmula de les òrbites diu

$$|G| = |Z(G)| + \sum_x [G : G_x].$$

Si algun dels índexs $[G : G_x]$ és primer amb p , aleshores G té un subgrup propi $G_x \subset G$ d'ordre divisible per p que, per hipòtesi d'inducció, conté elements d'ordre p . Si, pel contrari, tots els índexs $[G : G_x]$ són divisibles per p , aleshores p divideix l'ordre del centre de G , que és abelià, i conté elements d'ordre p . \square

Lema 3 *Siguin H un p -subgrup i P un p -subgrup de Sylow d'un grup G . Si $H \subseteq N_G(P)$ aleshores $H \subseteq P$.*

PROVA: Com que $H \subseteq N_G(P)$, $HP = PH$ és un subgrup de G i P n'és un subgrup normal. Aleshores $HP/P \simeq H/H \cap P$ i, per tant, $[HP : P] = [H : H \cap P]$ és una potència de p . Aleshores $|HP| = [HP : P]|P|$ també és una potència de p i, per maximalitat de P , necessàriament $HP = P$. Per tant $H \subseteq P$. \square

Teorema 4 (Teorema de Sylow) *Per a tot grup finit G i nombre primer p ,*

- (a) *G té algun p -subgrup de Sylow;*
- (b) *tot p -subgrup està contingut dins d'algun p -subgrup de Sylow;*
- (c) *tots els p -subgrups de Sylow són conjugats;*
- (d) *si $|G| = p^r n$ amb $p \nmid n$ aleshores el nombre de p -subgrups de Sylow de G divideix n i és congruent amb 1 mòdul p .*

PROVA: (a) Inducció sobre $|G|$. Si $|G| = 1$ aleshores G és un p -subgrup de Sylow. Es fa operar G sobre ell mateix per conjugació. La fórmula de les òrbites diu

$$|G| = |Z(G)| + \sum_x [G : G_x].$$

Si algun dels índexs $[G : G_x]$ és primer amb p , el grup G_x té ordre $p^r m < p^r n$ amb $(p, m) = 1$ i per hipòtesi d'inducció té p -subgrups de Sylow, que ho són també de G . Suposi's que tots aquests índexs són divisibles per p . Aleshores també ho és l'ordre del centre $Z(G)$. Sigui a un element d'ordre p a $Z(G)$. El subgrup $\langle a \rangle$ és normal a G , ja que està contingut dins de $Z(G)$. El quocient $G/\langle a \rangle$ té ordre $p^{r-1}n$ i, per hipòtesi d'inducció, té p -subgrups de Sylow, que són subgrups d'ordre p^{r-1} . L'antiimatge d'un p -subgrup de Sylow de $G/\langle a \rangle$ per la projecció canònica és un p -subgrup de Sylow de G , ja que té ordre $p \cdot p^{r-1} = p^r$.

Per a la resta d'apartats es considerarà la situació següent: sigui P un p -subgrup de Sylow fixat, i sigui $X = \{Q = aPa^{-1} \mid a \in G\}$ el conjunt dels seus conjugats. Aleshores G opera (transitivament) sobre X per conjugació i $|X| = [G : N_G(P)]$. Com que $P \subseteq N_G(P)$ l'índex d'aquest normalitzador és un divisor de n . Per tant el nombre d'elements de X és un divisor de n i per tant no és divisible per p .

(b) Sigui H un p -subgrup. Es considera l'acció per conjugació de H sobre el conjunt X . La fórmula de les òrbites diu

$$|X| = [G : N_G(P)] = \sum [H : H_Q],$$

on cada H_Q és l'estabilitzador d'un p -subgrup de Sylow $Q = aPa^{-1}$ conjugat de P . Com que els índexs en el sumatori són potències de p i $p \nmid |X|$, algun d'aquests índexs ha de ser 1. Per tant l'acció té punts fixos. Sigui Q un punt fix. Aleshores $hQh^{-1} = Q$ i per tant $H \subseteq N_G(Q)$. Pel lema anterior, $H \subseteq Q$.

(c) L'argument de l'apartat anterior, aplicant en el cas que H és un p -subgrup de Sylow, diu que $H = Q = aPa^{-1}$ per algun a . Per tant tots els subgrups de Sylow són conjugats de P .

(d) El nombre de p -subgrups de Sylow és el cardinal de X , que és un divisor de n . Consideri's l'acció del grup P sobre el conjunt X . Si Q és un punt fix d'aquesta acció, l'argument dels apartats anteriors diu que $Q = P$, i per tant aquesta acció té un únic punt fix, que és el propi grup P . Per la fórmula de les òrbites, es té $|X| = 1 + \sum [P : P_Q]$, on el sumatori correspon a les òrbites dels grups $Q \neq P$. Com que p divideix cadascun dels índexs del sumatori, es dedueix $\equiv 1 \pmod{p}$. \square