ESTRUCTURES ALGEBRAIQUES
Curs 2014-15

Teresa Crespo

19 de setembre de 2014

Índex

Part I
Grups

1 Grups

1.1 Definicions

Recordem que, si A és un conjunt no buit, una operació binària interna a A és una aplicació de $A \times A$ en A. Indiquem la imatge de (a, b) per aquesta aplicació per ab.

Definició 1.1. Un *grup* és un conjunt G dotat d'una operació binària interna que compleix

1) per a tots $x, y, z \in G$, $(xy)z = x(yz)$ (*Propietat associativa*);

2) existeix $e \in G$ tal que $ex = xe = x$, per a tot $x \in G$ (e es diu *element neutre* de G);

3) per a tot $x \in G$, existeix $x' \in G$ tal que $x'x = xx' = e$ (x' es diu *element simètric* de x).

Diem que G és *abelià* si l'operació de G és commutativa, és a dir $xy = yx$, per a tots $x, y \in G$.

Si l'operació de G és producte, es posa 1 l'element neutre, el simètric de x es diu invers i s'indica per x^{-1}. Si G és abelià, l'operació es denota com a suma, es posa 0 l'element neutre, el simètric de x es diu oposat i s'indica per $-x$.

Observació 1.2. L'element neutre d'un grup és únic. En efecte, si $e, e' \in G$ compleixen la propietat de ser neutre, tenim $e = ee' = e'$. L'element oposat d'un element x d'un grup és únic. En efecte, si $x', x'' \in G$ compleixen la propietat de ser oposats de x, tenim $x'' = ex'' = (x'x)x'' = x'(xx'') = x'e = x'$.

Exemples 1.3. 1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot), (\mathbb{Z}/m\mathbb{Z}, +), ((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ són grups abelians.

2) $\mathrm{GL}(n, \mathbb{R})$ és grup amb el producte de matrius. És no abelià, per a tot $n \geq 2$.

A partir d'ara, denotarem per x^{-1} el simètric d'un element x del grup G.

Propietats. De la definició de grup es dedueixen fàcilment les propietats següents d'un grup G.

1) *Llei de simplificació.* Donats $a, x, y \in G$,

$$\begin{array}{l} ax = ay \Rightarrow x = y \\ xa = ya \Rightarrow x = y \end{array}.$$

En particular, $xx = x \Rightarrow x = e$.

2) Donats $x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.

Definició 1.4. Un *subgrup* d'un grup G és un subconjunt no buit H de G tal que

1) $x, y \in H \Rightarrow xy \in H$ (H és tancat respecte de l'operació de G);

2) H és grup, amb l'operació de G.

Proposició 1.5. *Siguin G un grup i $H \subseteq G$ un subconjunt no buit. Els tres enunciats següents són equivalents:*

(a) H és subgrup de G.

(b) H satisfà les propietats:

(1) $e \in H$,

(2) Per a tot $x \in H$, es compleix $x^{-1} \in H$,

(3) Per a tot $x, y \in H$, es compleix $xy \in H$,

(c) Per a tot $x, y \in H$, es compleix $xy^{-1} \in H$.

Proposició 1.6. *Si H_1, H_2 són subgrups d'un mateix grup G, aleshores $H_1 \cap H_2$ és subgrup de G.*

Exemples 1.7. 1) Tot grup G té com a subgrups G (subgrup total) i $\{e\}$ (subgrup trivial);

2) $(\mathbb{Z}, +)$ és subgrup de $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ és subgrup de $(\mathbb{C}, +)$;

3) per a $m \in \mathbb{N}$, $m\mathbb{Z}$ és subgrup de $\mathbb{Z}$.

Proposició 1.8. *Tot subgrup H de $\mathbb{Z}$ és igual a $m\mathbb{Z}$, per a algun enter natural m.*

Demostració. Sigui H un subgrup de $\mathbb{Z}$. Si $H = \{0\}$, aleshores $H = m\mathbb{Z}$ amb $m = 0$. Suposem $H \neq \{0\}$. Com $n \in H \Rightarrow -n \in H$, H conté elements estrictament positius. Sigui m l'enter estrictament positiu més petit contingut a H. Tenim $m\mathbb{Z} \subset H$. Vegem ara l'inclusió contrària. Si $a \in H$, fem la divisió entera de a entre m. Tenim $a = mq + r$, amb $0 \leq r < m$ i $r = a - mq \in H$. Per tant $r = 0$ i $a \in m\mathbb{Z}$.

1.2 Grups de permutacions

Donat un conjunt X, una permutació de X és una aplicació bijectiva de X en X. Posem S_X el conjunt de permutacions de X. El conjunt S_X amb la composició d'aplicacions és un grup.

Per a n enter, $n \geq 1$, posem S_n el grup de permutacions de $\{1, 2, \ldots, n\}$. Es diu *grup simètric de grau n*. Si $\sigma \in S_n$, donem σ per

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix},$$

és a dir per una matriu de dues files on a la primera posem els elements $1, 2, 3, \ldots, n$ en ordre creixent i a la segona posem $\sigma(i)$ a sota de i, per a $i = 1, 2, 3, \ldots, n$. Clarament S_n té cardinal $n!$.

Exemples 1.9. $S_1 = \{Id\}$

$$S_2 = \left\{ Id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_3 = \left\{ Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \right.$$

$$\left. t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

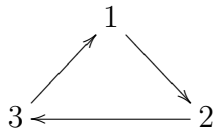
Observem que $t_1t_2 = s_1$ i $t_2t_1 = s_2$, per tant S_3 no és abelià. A S_n, podem considerar dues permutacions que operin sobre $1, 2, 3$ com t_1 i t_2, respectivament, i deixin fixos els índexs $k > 3$. Com aquestes dues permutacions no commuten entre elles, podem dir que S_n és un grup no abelià per a $n \geq 3$.

Donats r elements diferents dos a dos $k_1, k_2, \ldots k_r$ de $\{1, 2, \ldots, n\}$, posem $(k_1, k_2, \ldots, k_r)$ la permutació σ de S_n definida per

$$\sigma(k_1) = k_2, \sigma(k_2) = k_3, \ldots, \sigma(k_{r-1}) = k_r, \sigma(k_r) = k_1,$$
$$\sigma(p) = p, \text{ si } p \notin \{k_1, k_2, \ldots, k_r\}.$$

Diem que $(k_1, k_2, \ldots, k_r)$ és un *r-cicle*.

Amb aquesta notació podem escriure els elements de S_3 com $t_1 = (2, 3)$, $t_2 = (1, 3), t_3 = (1, 2), s_1 = (1, 2, 3), s_2 = (1, 3, 2)$ i tenim que els elements de S_3 diferents de l'identitat són tres 2-cicles i dos 3-cicles. Gràficament, podem representar, per exemple, el cicle $(1, 2, 3)$ com



i veiem que $(1, 2, 3) = (2, 3, 1) = (3, 1, 2)$. En general, la forma de representar un cicle no és única.

Un 2-cicle s'anomena també *transposició*. Tenim $(k_1, k_2, \ldots, k_r)^{-1} = (k_r, k_{r-1}, \ldots, k_1)$ i l'invers d'una transposició és ella mateixa.

Dos cicles $(k_1, k_2, \ldots, k_r), (h_1, \ldots, h_s)$ es diuen *disjunts* si ho són els conjunts $\{k_1, k_2, \ldots, k_r\}$ i $\{h_1, \ldots, h_s\}$. Clarament dos cicles disjunts commuten entre ells.

Proposició 1.10. *Tota permutació de S_n, diferent de la identitat, és producte de cicles, disjunts 2 a 2, unívocament determinats trets de l'ordre.*

Demostració. Sigui $\sigma \in S_n$, diferent de la identitat. Tenim al menys un índex $k \in \{1, 2, \ldots, n\}$ tal que $\sigma(k) \neq k$. Considerem $k, \sigma(k), \sigma^2(k), \ldots$. Com $\{1, 2, \ldots, n\}$ és finit, ha d'existir un r natural tal que $\sigma^r(k) = k$. Prenem l'r més petit amb aquesta condició. Aleshores els índexs $k, \sigma(k), , \ldots, \sigma^{r-1}(k)$ són tots diferents. Considerem el cicle $c_1 = (k, \sigma(k), \ldots, \sigma^{r-1}(k))$. Si per a tot $i \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k)\}$, és $\sigma(i) = i$, tenim $\sigma = c_1$. Si no, sigui $l \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k)\}$ tal que $\sigma(l) \neq l$ i sigui s l'enter més petit tal que $\sigma^s(l) = l$. Posem c_2 el cicle $(l, \sigma(l), \ldots, \sigma^{s-1}(l))$. Observem

que els conjunts $\{k, \sigma(k), \ldots, \sigma^{r-1}(k)\}$ i $\{l, \sigma(l), \ldots, \sigma^{s-1}(l)\}$ són disjunts. Si per a tot $i \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k), l, \sigma(l), \ldots, \sigma^{s-1}(l)\}$, és $\sigma(i) = i$, tenim $\sigma = c_1 c_2$. Si no, seguiríem el procés amb $m \in \{1, 2, \ldots, n\} \setminus \{k, \sigma(k), \ldots, \sigma^{r-1}(k), l, \sigma(l), \ldots, \sigma^{s-1}(l)\}$ tal que $\sigma(m) \neq m$.

Observem que si F és el conjunt d'índexs que queden fixos per σ, aleshores $F \cup \{k, \sigma(k), \ldots, \sigma^{r-1}(k)\}$ és el conjunt d'índexs que queden fixos per $c_1^{-1}\sigma$, $F \cup \{k, \sigma(k), \ldots, \sigma^{r-1}(k)\} \cup \{l, \sigma(l), \ldots, \sigma^{s-1}(l)\}$ és el conjunt d'índexs que queden fixos per $c_2^{-1}c_1^{-1}\sigma, \ldots$, per tant en un nombre finit de passos arribem a una descomposició de σ com a producte de cicles. Els factors són únics ja que per a cada $i \in \{1, 2, \ldots, n\}$ hi ha un únic factor c tal que $c(i) \neq i$ i per aquest $c(i) = \sigma(i)$.

Corol·lari 1.11. *Tota permutació és producte de transposicions.*

Demostració. N'hi ha prou amb veure que tot cicle és producte de transposicions. Ara tenim $(k_1, k_2, \ldots, k_r) = (k_1, k_2)(k_2, k_3) \ldots (k_{r-1}, k_r)$.

Exemple 1.12.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 7 & 10 & 11 & 9 & 4 & 5 & 8 & 2 & 3 & 6 & 1 \end{pmatrix}$$
$$= (1, 12)(2, 7, 5, 9)(3, 10)(4, 11, 6)$$
$$= (1, 12)(2, 7)(5, 7)(5, 9)(3, 10)(4, 11)(6, 11).$$

La descomposició d'una permutació en producte de transposicions no és única. Veurem ara que la paritat del nombre de factors en la descomposició si que ho és.

Lema 1.13. *Si $a, b, c \in \{1, 2, \ldots, n\}$ són tots tres diferents, tenim a S_n la igualtat $(a, b)(b, c) = (a, c)(a, b)$.*

Lema 1.14. *La identitat no és igual a un producte d'un nombre senar de transposicions.*

Demostració. Volem veure que la identitat no és producte de $2k + 1$ transposicions, per a k enter ≥ 0, per inducció sobre k.

1) per a $k = 0$, és clar que Id no és una transposició.

2) suposem que la identitat no és producte de $2k-1$ transposicions i provem que tampoc no ho és de $2k+1$ transposicions.

   Posem $Id = t_1 t_2 \dots t_{2k+1}$, per a t_i transposicions, $1 \leq i \leq 2k+1$, i $t_{2k+1} = (a, x)$. Com el producte de les $t_i's$ ha de ser Id, ha d'haver algun factor de la forma (a, y). Pel lema 1.13, podem suposar $t_{2k} = (a, y)$. Si fos $x = y$, Id seria producte de $2k-1$ transposicions, que no pot ser per hipòtesi d'inducció. Per tant $x \neq y$. Ara y té imatge a pel producte $t_{2k} t_{2k+1}$ i per tant un dels altres factors ha de ser de la forma (a, z). Pel lema 1.13, podem suposar $t_{2k-1} = (a, z)$ i, per la hipòtesi d'inducció, ha de ser $z \neq y$ i $z \neq x$. Reiterant aquest raonament arribariem a que totes les t_i són de la forma (a, v), amb tots els $v's$ diferents i per tant el seu producte no pot donar Id.

Proposició 1.15. *Si $t_1, \dots, t_r, \tau_1, \dots, \tau_s$ són transposicions i*

$$t_1 \dots t_r = \tau_1 \dots \tau_s,$$

aleshores $r \equiv s \pmod 2$.

Demostració. $t_1 \dots t_r = \tau_1 \dots \tau_s \Rightarrow t_1 \dots t_r \tau_s \dots \tau_1 = Id \Rightarrow r + s$ parell.

Definim la *signatura* d'una permutació σ de S_n com $\varepsilon(\sigma) = (-1)^r$, si σ és producte de r transposicions. La proposició 1.15 dóna que la signatura està ben definida. Diem que σ és *parella* si $\varepsilon(\sigma) = 1$, *senar* si $\varepsilon(\sigma) = -1$. Clarament, per a dues permutacions σ, τ de S_n tenim $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Proposició 1.16. *El conjunt de permutacions parelles de S_n és un subgrup de S_n. Es diu grup alternat de grau n i es denota per A_n.*

Demostració. Pel lema 1.14, $\varepsilon(Id) = 1$, per tant $Id \in A_n$; $\sigma, \tau \in A_n \Rightarrow \sigma\tau \in A_n$; $\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$.

Exemple 1.17. La permutació $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 7 & 10 & 11 & 9 & 4 & 5 & 8 & 2 & 3 & 6 & 1 \end{pmatrix}$ té signatura -1.

1.3 Morfismes de grups

Si G i G' són grups, una aplicació $f : G \to G'$ és un morfisme de grups si

$$f(xy) = f(x)f(y), \forall x, y \in G.$$

Proposició 1.18. *Si G i G' són grups, e l'element neutre de G, e' el de G' i $f : G \to G'$ és un morfisme de grups, es compleix*

1) $f(e) = e'$;

2) $f(x^{-1}) = f(x)^{-1}$, $\forall x \in G$.

Demostració.

1) $f(e) = f(ee) = f(e)f(e) \Rightarrow f(e) = e'$, aplicant la llei de simplificació.

2) $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$.

Exemples 1.19. Les aplicacions següents són morfismes de grups.

$$det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*;$$
$$\varepsilon : S_n \to \{\pm 1\};$$
$$\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto [a].$$

Proposició 1.20. *Si G, G' i G'' són grups, $f : G \to G', g : G' \to G''$ són morfismes de grups, aleshores $g \circ f : G \to G''$ és morfisme de grups.*

Per a un morfisme de grups $f : G \to G'$ definim el *nucli* de f com

$$\mathrm{Ker}\, f = \{x \in G | f(x) = e'\}$$

i definim la *imatge* de f com

$$\mathrm{Im}\, f = \{f(x) | x \in G\}.$$

Proposició 1.21. *Si $f : G \to G'$ és morfisme de grups,* $\mathrm{Ker}\, f$ *és subgrup de G i* $\mathrm{Im}\, f$ *és subgrup de G'.*

Un monomorfisme de grups és un morfisme de grups injectiu, un epimorfisme de grups és un morfisme de grups exhaustiu, un isomorfisme de grups és un morfisme de grups bijectiu. Un endomorfisme d'un grup G és un morfisme de grups de G en G. Un automorfisme de G és un endomorfisme de G bijectiu.

Proposició 1.22. *Si $f : G \to G'$ és isomorfisme de grups, l'aplicació inversa $f^{-1} : G' \to G$ també ho és.*

Diem que dos grups G i G' són isomorfs i posem $G \simeq G'$ si existeix un isomorfisme de grups $f : G \to G'$.

Exemples 1.23. Considerem els exemples 1.19.

$\mathrm{Ker}(det) = \mathrm{SL}(n, \mathbb{R}), det$ és epimorfisme,
$\mathrm{Ker}(\varepsilon) = A_n, \varepsilon$ és epimorfisme,
$\mathrm{Ker}(\pi) = m\mathbb{Z}, \pi$ és epimorfisme.

Proposició 1.24. *Si $f : G \to G'$ és morfisme de grups,*

$$f \text{ és injectiu} \Leftrightarrow \mathrm{Ker}\, f = \{e\}.$$

Demostració. Suposem f injectiu i sigui $x \in \mathrm{Ker}\, f$. Tenim $f(x) = e' = f(e) \Rightarrow x = e$. Per tant $\mathrm{Ker}\, f = \{e\}$.

Suposem ara $\mathrm{Ker}\, f = \{e\}$ i siguin $x, y \in G$ tals que $f(x) = f(y)$. Tenim $f(x) = f(y) \Rightarrow e' = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$. Per tant $xy^{-1} \in \mathrm{Ker}\, f = \{e\}$ i tenim doncs $xy^{-1} = e$ que implica $x = y$.

1.4 Teorema de Lagrange

Donat un grup G, diem que G és finit si el conjunt G és finit i, en aquest cas, diem *ordre* de G i indiquem per $|G|$ el nombre d'elements del conjunt G.

Exemples 1.25. $|S_n| = n!, |\mathbb{Z}/m\mathbb{Z}| = m, \mathbb{Z}$ és infinit.

Donats un grup G i un subgrup H de G, definim a G les relacions D i E per

$$xDy \Leftrightarrow x^{-1}y \in H, \quad xEy \Leftrightarrow yx^{-1} \in H.$$

Proposició 1.26. *Les relacions D i E són relacions d'equivalència.*

Demostració. Ho provem per D. Per E es faria de forma anàlega.

1. Per a $x \in G$, tenim xDx, ja que $x^{-1}x = e \in H$
2. Per a $x, y \in G$, $xDy \Rightarrow x^{-1}y \in H \Rightarrow y^{-1}x = (x^{-1}y)^{-1} \in H \Rightarrow yDx$
3. Per a $x, y, z \in G$, $\left.\begin{array}{l} xDy \\ yDz \end{array}\right\} \Rightarrow \left.\begin{array}{l} x^{-1}y \in H \\ y^{-1}z \in H \end{array}\right\} \Rightarrow x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \Rightarrow xDz.$

Considerem ara les classes d'equivalència per les relacions D i E. Tenim

$$xDy \Leftrightarrow x^{-1}y \in H \Leftrightarrow y = xh \text{ per a algun } \ h \in H.$$

Tenim doncs que la classe d'equivalència de $x \in G$ per la relació D és el conjunt $\{xh|h \in H\}$. Escrivim aquest conjunt com xH i diem que és la classe de x per la dreta mòdul H. Posem G/D el conjunt quocient de G per la relació D. Anàlogament, tenim

$$xEy \Leftrightarrow yx^{-1} \in H \Leftrightarrow y = hx \text{ per a algun } \ h \in H.$$

Tenim doncs que la classe d'equivalència de $x \in G$ per a relació E és el conjunt $\{hx|h \in H\}$. Escrivim aquest conjunt com Hx i diem que és la classe de x per l'esquerra mòdul H. Posem G/E el conjunt quocient de G per la relació E.

Observem que les aplicacions

$$\begin{array}{ll} H \to xH & H \to Hx \\ h \mapsto xh & h \mapsto hx \end{array}$$

són bijectives, per tant totes les classes d'equivalència tant per D com per E tenen el mateix cardinal que H. Ara, per a $x, y \in G$, tenim $y \in xH \Leftrightarrow y^{-1} \in Hx^{-1}$, per tant $y \mapsto y^{-1}$ indueix una bijecció de G/D en G/E.

Observació 1.27. Si G és abelià, $D = E$.

Exemples 1.28.

1. Per a $G = \mathbb{Z}, H = m\mathbb{Z}$, tenim $D = E =$ congruència mòdul m.

2. Determinem ara els conjunts quocients G/D i G/E per a $G = S_3 = \{Id, t_1, t_2, t_3, s_1, s_2\}, H = \{Id, t_1\}$.

   Les classes per la dreta són

   $$IdH = H, t_2H = \{t_2, t_2t_1 = s_2\}, t_3H = \{t_3, t_3t_1 = s_1\}.$$

   I les classes per l'esquerra són

   $$HId = H, Ht_2 = \{t_2, t_1t_2 = s_1\}, Ht_3 = \{t_3, t_1t_3 = s_2\}.$$

   Tenim doncs que G/D i G/E són diferents.

Donats un grup G i un subgrup H de G, posem $[G : H]$ i diem índex de G en H el cardinal de G/D (que hem vist és igual al de G/E).

Exemples 1.29. $[\mathbb{Z} : m\mathbb{Z}] = m, [S_3 : \{Id, t_1\}] = 3$.

Teorema 1.30 (Teorema de Lagrange)**.** *Donats un grup G i un subgrup H de G, el grup G és finit si i només si H i $[G : H]$ són finits. En aquest cas*

$$|G| = |H| \cdot [G : H].$$

En particular, $|H|$ i $[G : H]$ són divisors de $|G|$.

Demostració. Les classes d'equivalència per D formen una partició de G, és a dir G és reunió disjunta de les classes d'equivalència i a cada classe d'equivalència per D hi ha tants elements com a H.

1.5 Subgrups normals. Grup quocient.

Volem ara definir una estructura de grup en el conjunt quocient d'un grup G per la relació D associada a un subgrup H. Considerem el cas $G = S_3, H = \{Id, t_1\}$. Intentem fer el producte de les classes $[t_2]$ de t_2 i $[t_3]$ de t_3. Posem $[t_2][t_3] = [t_2t_3] = [s_1]$. Però $s_2 \in [t_2]$ i $s_1 \in [t_3]$ i en canvi tenim $s_2s_1 = Id \notin [s_1]$. El producte depen del representant, per tant no estaria ben definit. Veiem ara que si podem definir un producte de classes que no depengui del representant escollit a cada classe, aleshores el conjunt quocient té estructura de grup.

Definició 1.31. Sigui T una relació d'equivalència definida en un grup G. Diem que T és compatible amb l'operació de G si per a qualssevol $x, y, x', y' \in G$ es compleix

$$\left.\begin{array}{l} xTx' \\ yTy' \end{array}\right\} \Rightarrow xyTx'y'$$

Proposició 1.32. *Si T és una relació definida en un grup G, compatible amb l'operació de G, aleshores G/T és grup amb l'operació definida per*

$$[x][y] = [xy].$$

Demostració. Clarament l'operació està ben definida, és associativa, l'element neutre és $[e]$ i $[x]^{-1} = [x^{-1}]$.

Proposició 1.33. *Sigui G un grup, H un subgrup de G, D i E les relacions definides a partir de H. Els enunciats següents són equivalents.*

1) $xH = Hx$, per a tot $x \in G$.

2) $xHx^{-1} = H$, per a tot $x \in G$.

3) $xHx^{-1} \subset H$, per a tot $x \in G$.

4) D és compatible amb l'operació de G.

5) E és compatible amb l'operació de G.

Demostració. Les implicacions $1 \Rightarrow 2$ i $2 \Rightarrow 3$ són immediates.
$3 \Rightarrow 1$: Donat $x \in G$, $xHx^{-1} \subset H \Rightarrow xH \subset Hx$. Ara apliquem 3) amb x^{-1} i obtenim $x^{-1}Hx \subset H \Rightarrow Hx \subset xH$.
$1 \Rightarrow 4$: Donats $x, y, x', y' \in G$, volem veure que xDx' i yDy' implica $xyDx'y'$. Ara xDx' implica $x' = xh$, per a un cert $h \in H$ i yDy' implica $y' = yh'$, per a un cert h' de H. Per tant $x'y' = (xh)(yh') = x(hy)h'$. Ara, com $Hy = yH$, tenim $hy = yh''$, per a algun $h'' \in H$. Tenim doncs $x(hy)h' = x(yh'')h' = (xy)(h''h')$, on $h''h' \in H$, per tant $(x'y')D(xy)$ com volíem.
$4 \Rightarrow 3$: Donats $x \in G, h \in H$, volem veure $xhx^{-1} \in H$. Tenim

$$\left.\begin{array}{l} xhDx \\ x^{-1}Dx^{-1} \end{array}\right\} \Rightarrow xhx^{-1}Dxx^{-1} = e \Rightarrow xhx^{-1} \in H.$$

$1 \Rightarrow 5$: Donats $x, y, x', y' \in G$, volem veure que xEx' i yEy' implica $xyEx'y'$. Ara xEx' implica $x' = hx$, per a un cert $h \in H$ i yEy' implica $y' = h'y$, per a un cert h' de H. Per tant $x'y' = (hx)(h'y) = h(xh')y$. Ara, com $Hx = xH$, tenim $xh' = h''x$, per a algun $h'' \in H$. Tenim doncs $h(xh')y = h(h''x)y = (hh'')(xy)$, on $hh'' \in H$, per tant $(x'y')E(xy)$ com volíem.
$5 \Rightarrow 3$: Donats $x \in G, h \in H$, volem veure $xhx^{-1} \in H$. Tenim

$$\left.\begin{array}{l} xEx \\ hx^{-1}Ex^{-1} \end{array}\right\} \Rightarrow xhx^{-1}Exx^{-1} = e \Rightarrow xhx^{-1} \in H.$$

Un subgrup H d'un grup G complint les condicions de la proposició 1.33 es diu *subgrup normal* de G. Posem $H \lhd G$ per indicar que H és subgrup normal de G. Si H és normal en G, posem $G/H = G/D = G/E$ i l'anomenem grup quocient de G per H. Definim la projecció canònica $\pi : G \to G/H$ que

envia cada element de G a la seva classe en G/H. És epimorfisme de grups amb nucli H.

Exemples 1.34. 1. Si G és abelià, tot subgrup de G és subgrup normal.

2. El subgrup $\{Id, t_1\}$ de S_3 no és normal.

Observació 1.35. Si T és relació d'equivalència compatible amb l'operació del grup G, $H := \{x \in G | xTe\}$ és subgrup normal de G i la relació d'equivalència associada a H coincideix amb T.

Proposició 1.36. *Si $f : G \to G'$ és morfisme de grups,* $\operatorname{Ker} f$ *és subgrup normal de G.*

Demostració. Per a $x \in G, h \in \operatorname{Ker} f$, tenim $f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)e'f(x)^{-1} = f(x)f(x)^{-1} = e'$, per tant $xhx^{-1} \in \operatorname{Ker} f$.