USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Retículos de subgrupos

Irene Giadás Amado

2019/2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Retículos de subgrupos

Irene Giadás Amado

Xullo, 2020

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Retículos de subgrupos
Breve descrición do contido
Existen moitas relacións entre a estrutura dun grupo G e a do seu retículo de subgrupos $L(G)$. A máis básica é que os isomorfismos entre grupos inducen isomorfismos entre os seus retículos de subgrupos, pero non á inversa, en xeral. Preguntas máis complexas son se podemos determinar os retículos asociados a unha clase de grupos, ou os grupos asociados a unha clase de retículos, ou que grupos están determinados polo seu retículo de subgrupos. O obxectivo deste traballo é facer unha incursión na teoría de retículos para a continuación dar resposta a algunhas destas preguntas.
Recomendacións
Ter superadas as materias "Estruturas alxébricas" e "Ecuacións alxébricas".
Outras observacións

Índice xeral

Resumo

O obxectivo deste traballo é facer unha incursión na teoría de retículos para dar resposta a algunhas preguntas tales como que relacións hai entre a estrutura dun grupo G e a do seu retículo de subgrupos $L(G)$, centrándonos especialmente nos grupos finitos. Para iso, introduciremos previamente algúns conceptos elementais da teoría básica de retículos, á que lle dedicaremos os primeiros capítulos. A relación máis básica que atopamos é que os isomorfismos entre grupos inducen isomorfismos entre os seus retículos de subgrupos, pero non á inversa. A segunda parte do traballo dedicarase a preguntas máis complexas como determinar se hai grupos asociados a unha clase de retículos. Buscaremos en dúas clases de retículos: os retículos distributivos e os retículos modulares. Finalmente, presentaremos exemplos de grupos que están determinados polo seu retículo de subgrupos.

Abstract

The purpose of this work is to make a foray into lattice theory to answer some questions such that what are the relationships between the structure of a group G and that of its subgroup lattice $L(G)$, focusing especially on finite groups. In order to do this, we will previously introduce some elementary concepts of basic lattice theory, to which we will dedicate the first chapters. The most basic relationship we find is that isomorphisms between groups induce isomorphisms between their subgroup lattices, but not the other way around. The second part of the work will be devoted to more complex questions such as determining whether there are groups associated with a lattice class. We will look at two lattice classes: distributive lattice and modular lattice. Finally, we will introduce examples of groups that are determined by their subgroup lattice.

Introdución

O interese de estudar os retículos de subgrupos vén dado polo teorema de Whitman [12], "Todo retículo é isomorfo a un subretículo dun retículo de subgrupos". Neste traballo centrarémonos especialmente nos retículos de subgrupos dos grupos finitos, cuxa importancia está xustificada pola seguinte versión notable do teorema anterior, "Todo retículo finito é isomorfo a un subretículo dun retículo de subgrupos dalgún grupo finito", probado por Pudlák e Tuma [7].

Comezaremos con algunhas observacións simples sobre os retículos de subgrupos. Xa que nos ocuparemos principalmente dos grupos finitos, sinalemos en primeiro lugar que o retículo de subgrupos $L(G)$ é finito se e só se o grupo G é finito. Para algúns retículos "pequenos" é fácil determinar todos os grupos que teñen o retículo dado como retículo de subgrupos. Por exemplo, $L(G)$ terá un retículo coa estrutura:

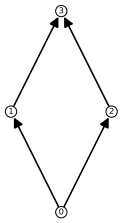
$L(G) =$ se e só se G é o grupo trivial.

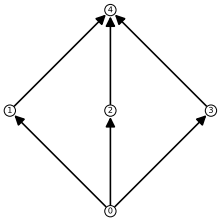
$L(G) =$  se e só se G é cíclico de orde prima.

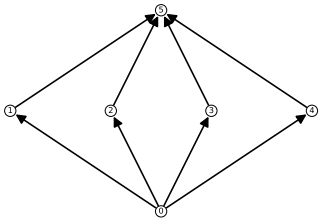
$L(G) =$  se e só se G é cíclico de orde p^2 para un primo p.

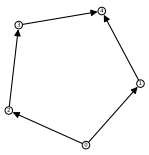
$L(G) =$  se e só se G é cíclico de orde p^3 para un primo.

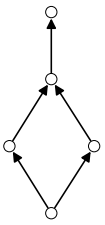
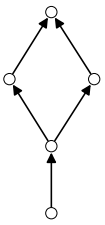
$L(G) =$  se e só se G é cíclico de orde p^4 para un primo.

$L(G) =$  se e só se G é cíclico de orde pq con primos $p \neq q$.

$L(G) =$  se e só se G é o grupo de Klein de catro elementos $C_2 \times C_2$.

$L(G) =$  se e só se $G \cong C_3 \times C_3$ ou $G \cong S_3$.

Con todo, non existe ningún grupo G con $L(G) =$  , retículo coñecido

como pentágono ou N_5, ou $L(G) =$  ou $L(G) =$  .

Así existen retículos que son retículos de subgrupos de infinitos grupos, dun número finito de grupos, dun único grupo, ou de ningún grupo. É dicir, a correspondencia $\mathcal{L}$ entre grupos e retículos,

$$\mathcal{L}\colon G \longrightarrow L(G)$$

non é nin inxectiva, nin sobrexectiva. Este feito dá lugar ás dúas seguintes cuestións:

1. A descrición de todos os grupos con retículo de subgrupos isomorfo. Especialmente, que grupos están determinados unicamente polos retículos dos seus subgrupos?

2. Que retículos son retículos de subgrupos?

Outra segunda dirección importante na investigación dos retículos de subgrupos consiste en procurar caracterizacións reticulares de clases de grupos, é dicir, en responder á seguinte pregunta:

3. Para que clase de grupos $\mathfrak{X}$ existe unha clase de retículos $\mathcal{D}$ tal que, para todo grupo G, $G \in \mathfrak{X}$ se e só se $L(G) \in \mathcal{D}$?

As respostas a estas cuestións son moi complicadas (véxase [6]). Ao longo deste traballo procuraremos darlles respostas parciais.

Doutra banda, o estudo dos retículos de subgrupos tamén serve para comprender mellor certos aspectos da teoría de grupos. Vexamos un exemplo.

Un dos resultados máis simples e á vez máis potentes da teoría dos grupos finitos é o teorema de Lagrange: se H é un subgrupo dun grupo finito G, entón a orde de H é un divisor da orde de G.

Os grupos que satisfán o recíproco do teorema de Lagrange coñécense como grupos de tipo Lagrange. Exemplos de grupos de tipo Lagrange son: S_4, cíclicos, abelianos, p-grupos, nilpotentes. Pola contra, A_4 non é de tipo Lagrange.

A procura de recíprocos parciais deste teorema motivou gran parte do traballo inicial en grupos finitos. Unha relación clara cos retículos de subgrupos pode verse se reformulamos o teorema de Lagrange do seguinte xeito: se denotamos por T_n o retículo dos divisores

enteiros positivos de $n \in \mathbb{N}$, dado un grupo finito G de orde n, a aplicación $\omega\colon L(G) \to T_n$ que asigna a cada subgrupo H de G a súa orde $|H|$ conserva a orde de $L(G)$ en T_n.

Tres cuestións veñen inmediatamente á mente.

- Para que grupos finitos é ω sobrexectiva?
- Para que grupos finitos é ω un homomorfismo de retículos?
- Para que grupos finitos é ω inxectiva?

A primeira pregunta equivale a preguntar por un recíproco do teorema de Lagrange. Ademais, pódese probar que se ω é un homomorfismo de retículos, entón é inxectiva, e, como veremos no capítulo 4, son equivalentes:.

(A) A aplicación $\omega\colon L(G) \to T_n$ é un isomorfismo de retículos.

(B) $L(G)$ é un retículo distributivo.

(C) G é cíclico.

A continuación pasamos a describir brevemente a organización do traballo. Comezaremos recordando resultados básicos de teoría de grupos no primeiro capítulo, como o teorema de Lagrange antes mencionado, e que se empregarán de apoio á hora de demostrar resultados nos capítulos posteriores.

No segundo capítulo presentaremos conceptos básicos da teoría de retículos que ilustraremos cunha ampla variedade de exemplos e desenvolveremos propiedades elementais de retículos. Tamén definiremos os retículos de subgrupos, os retículos distributivos e os retículos modulares, conceptos que serán o tema de estudo dos capítulos 3, 4 e 5, respectivamente.

O terceiro capítulo centrarase nos retículos de subgrupos, comezando por tres exemplos notorios nos que poderemos comprobar resultados do capítulo anterior. Tras eles, faremos fincapé no teorema de Whitman xunto con outros resultados cos que procuraremos responder ás cuestións 1 e 2 anteriores. Comprobaremos que non todos os retículos son retículos de subgrupos, e interesarémonos na relación entre os isomorfismos entre retículos de subgrupos e os isomorfismos entre os respectivos grupos.

A continuación estudaremos os retículos de subgrupos de grupos cíclicos. O principal resultado do capítulo 4 é o teorema de Ore, que caracteriza os retículos de subgrupos distributivos como retículos de subgrupos de grupos localmente cíclicos. Restrinxíndonos ao caso finito, chegamos á conclusión de que unha clase de grupos como son os cíclicos

finitos correspóndense coa clase dos retículos distributivos, e aportamos información sobre a pregunta 3 anterior.

Continuamos buscando outras relacións entre clases de grupos e tipos de retículos de subgrupos no capítulo 5 cos retículos modulares. Aínda que non atopamos relacións tan boas como no capítulo anterior, observamos que hai unha certa relación entre os conceptos de retículo modular e grupo abeliano. Para chegar a isto, introduciremos un concepto importante, os elementos modulares. Acabaremos este capítulo cun notorio teorema de Iwasawa, o cal determina completamente a estrutura dun p-grupo finito con retículo de subgrupos modular.

Para rematar, veremos exemplos de grupos que están caracterizados polos seus retículos de subgrupos, entre os que destacamos o grupo alternado A_4. Deste xeito, afondaremos na cuestión 1 presentada anteriormente.

Capítulo 1

Preliminares

Comezaremos recordando algúns resultados de teoría de grupos, que se poden atopar en referencias básicas como [8] e que son pertinentes para o desenvolvemento do traballo. Como son resultados coñecidos, non incluiremos a súa demostración. Usaremos a notación $H \subseteq G$ para referirnos a que H é un subgrupo do grupo G e, no caso de subgrupos normais, escribiremos $H \trianglelefteq G$. Denotaremos por $|G|$ a orde de G e por $|G : H|$ o índice de H en G.

Se S é un subgrupo de G, denotaremos por $\langle S \rangle$ o subgrupo de G xerado por S, é dicir, o menor subgrupo de G que contén a S. Se $S = \{g_1, \dots, g_n\}$ empregaremos o abuso de notación $\langle S \rangle = \langle g_1, \dots, g_n \rangle$. Se $G = \langle g \rangle$ para algún $g \in G$, diremos que é cíclico. Denotaremos o grupo cíclico de orde n como C_n, onde $n \in \mathbb{N} \cup \{\infty\}$, é dicir, n é un número natural ou o símbolo ∞. Para $n = \infty$, temos que $C_\infty \simeq \mathbb{Z}$. En particular, todo grupo cíclico é abeliano.

Teorema 1.1. *Consideremos un grupo cíclico $G = \langle g \rangle$. Entón,*

1. *Todo subgrupo de G é cíclico.*
2. *Se G é un grupo finito de orde n, para cada divisor positivo k de n hai exactamente un subgrupo de índice k, $\langle g^k \rangle$, e cada subgrupo non trivial de G é desta forma. Ademais, se $s \mid n$, $r \mid n$, tense que $\langle g^r \rangle \subseteq \langle g^s \rangle$ se, e só se, $s \mid r$.*
3. *Se G é infinito, para todo $r \in \mathbb{N}$ hai un subgrupo de índice r en G, $\langle g^r \rangle$, e cada subgrupo non trivial de G é desta forma. Ademais, tense que $\langle g^r \rangle \subseteq \langle g^s \rangle$ se, e só se, $s \mid r$.*

Teorema 1.2 (Teorema de Lagrange)**.** *Sexa G un grupo finito e H un subgrupo de G. Entón,*

$$|G| = |H||G : H|.$$

Corolario 1.3. *Sexa G un grupo con $|G| = n$. Entón a orde de calquera subgrupo de G divide a n.*

Definición 1.4. Se G é un grupo e H e K son subgrupos de G, defínese o subconxunto produto $HK = \{hk \mid h \in H, k \in K\}$.

Proposición 1.5. *Se H e K son subgrupos de G, as seguintes afirmacións son equivalentes:*

1. *HK é subgrupo de G.*
2. *$KH = HK$, é dicir, H e K conmutan.*

   Neste caso, HK é exactamente o subgrupo de G xerado por H e K.

Proposición 1.6. *Sexa G un grupo e H e K subgrupos de G. Entón:*

$$|H||K| = |HK||H \cap K|.$$

Teorema 1.7. *Sexan H e K subgrupos dun grupo G, con K subgrupo normal de G. Entón, HK é subgrupo de G e $H/(H \cap K) \simeq HK/K$.*

Teorema 1.8 (Teorema de Correspondencia)**.** *Sexa $f\colon G \longrightarrow G'$ un homomorfismo sobrexectivo entre os grupos G e G'. Entón, hai unha bixección entre o conxunto dos subgrupos de G que conteñen ao núcleo de f,* $\mathrm{Ker}(f)$*, e o conxunto dos subgrupos de G'.*

En particular, hai unha bixección entre o conxunto dos subgrupos normais de G que conteñen a $\mathrm{Ker}(f)$ e o conxunto dos subgrupos normais de G'.

Definición 1.9. Un **p-grupo** é un grupo de orde p^n para algún primo p con $n \geq 1$.

Proposición 1.10. *Sexa G un p-grupo. Entón, para todo subgrupo H de G, existen subgrupos distintos $H_0 = H, H_1, \ldots, H_n = G$, tales que $H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$ cumprindo $|H_{k+1} : H_k| = p$.*

Definición 1.11. Se G é un grupo, chamaremos ao subgrupo $Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}$ **centro** de G.

Proposición 1.12. *Sexa H un subgrupo de G, e sexa $H \subseteq Z(G)$. Entón, $H \trianglelefteq G$. Ademais, se G/H é cíclico, entón G é abeliano.*

Definición 1.13. Para un subconxunto X de G, chámase **normalizador** de X en G ao conxunto $N_G(X) = \{g \in G \mid gXg^{-1} = X\}$.

En particular, se H é un subgrupo de G, $N_G(H)$ é o maior subgrupo de G no que H é normal.

Definición 1.14. Sexan $a, b \in G$. Chámase **conmutador** de a e b ao elemento $[a, b] = aba^{-1}b^{-1}$. O grupo $[G, G]$ é o subgrupo xerado por todos os conmutadores de elementos de G, e chámase **subgrupo conmutador** de G.

Nótese que o conmutador $[G, G]$ é trivial se, e só se, G é abeliano.

Proposición 1.15. *Se H é un subgrupo normal de G, G/H é abeliano se, e só se, $[G, G] \subseteq H$.*

Acabaremos o capítulo presentando unhas definicións e un resultado máis específicos que necesitaremos ao longo do traballo.

Definición 1.16. Dirase que un grupo G é **localmente cíclico** se cada subconxunto finito de G xera un subgrupo cíclico. De forma equivalente, podemos dicir que $\langle a, b\rangle$ é cíclico para cada par a, b de elementos de G.

En particular, cada grupo localmente cíclico é abeliano.

Exemplo 1.17. O grupos aditivos dos racionais $\mathbb{Q}$ e $\mathbb{Q}/\mathbb{Z}$ son localmente cíclicos. Pola contra, o grupo aditivo dos reais $\mathbb{R}$ non é localmente cíclico.

Un grupo é localmente cíclico se e só se é isomorfo a un subgrupo de $\mathbb{Q}$ ou de $\mathbb{Q}/\mathbb{Z}$ (véxase [9]).

Definición 1.18. Un subgrupo M de G diremos que é **permutable** en G, se $MH = HM$ para todo subgrupo H de G.

Proposición 1.19. *Sexa G un grupo. Se N é un subgrupo normal de G, entón N é permutable.*

Demostración. Se N é subgrupo normal de G, $N \trianglelefteq G$, entón $Nx = xN$ para todo $x \in G$. □

Definición 1.20. Un grupo non abeliano dise **hamiltoniano** se todos os seus subgrupos son normais.

Exemplo 1.21. O exemplo máis familiar (e máis pequeno) dun grupo hamiltoniano é o grupo dos cuaternios de orde 8, denotado por Q_8.

Definición 1.22. Un grupo abeliano dise p-**grupo abeliano elemental** se todos os seus elementos non triviais teñen orde p para un p primo.

Definición 1.23. Dados dous grupos H e K, e un homomorfismo $\phi\colon K \to \mathrm{Aut}(H)$, $k \mapsto \phi(k)$, o **produto semi-directo** de H e K, denotado por $H \rtimes_\phi K$, ou $H \rtimes K$, é o produto cartesiano $H \times K$ co produto definido polo

$$(h,k)(h',k') = (h\ \phi(k)(h'), kk'),$$

onde o elemento neutro é $(1,1)$ e $(\phi(k^{-1})(h^{-1}), k^{-1})$ é o inverso do elemento (h,k).

Nótese, que no caso de que o homomorfismo $\phi\colon K \to \mathrm{Aut}(H)$ sexa trivial, entón o produto semi-directo é o produto directo. Veremos un exemplo no capítulo 3.

Capítulo 2

Teoría básica de retículos

Neste capítulo introduciremos os conceptos básicos da teoría de retículos acompañados de exemplos, presentaremos propiedades elementais de retículos e estudaremos dúas clases importantes de retículos (véxase [1, 2]).

2.1. Conxuntos de orde parcial

Antes de comezar a falar de retículos, debemos coñecer a súa estrutura subxacente, que son os conxuntos parcialmente ordenados.

Definición 2.1. Un **conxunto parcialmente ordenado** é un par $(P, \leq)$ onde P é un conxunto non baleiro e $\leq$ é unha relación binaria que verifica as seguintes propiedades:

1. **Reflexiva:** para todo $a \in P$,
$$a \leq a.$$

2. **Antisimétrica:** para todo $a, b \in P$,
$$\text{se } a \leq b \text{ e } b \leq a, \text{ entón } a = b.$$

3. **Transitiva:** Para todo $a, b, c \in P$,
$$\text{se } a \leq b \text{ e } b \leq c, \text{ entón } a \leq c.$$

A relación $\leq$ recibe o nome de **orde parcial**. Escribiremos $a < b$ se $a \leq b$ pero $a \neq b$. Os conxuntos parcialmente ordenados son coñecidos como **posets**.

Unha das características máis útiles e atractivas dos conxuntos parcialmente ordenados é que, no caso finito, podémolos "debuxar". Para cada poset finito P describimos a súa estrutura usando **diagramas de Hasse**. Representamos cada elemento de P por un punto do plano de tal xeito que o punto p_y asociado a un elemento y está por riba do punto p_x asociado ao punto x se que $x < y$. Ademais, sempre que $y < x$ e non exista $z \in P$ con $x < z < y$, conectaranse os puntos p_x e p_y cunha liña. Para ilustrar esta explicación, a continuación amósanse algúns exemplos de diagramas de Hasse.

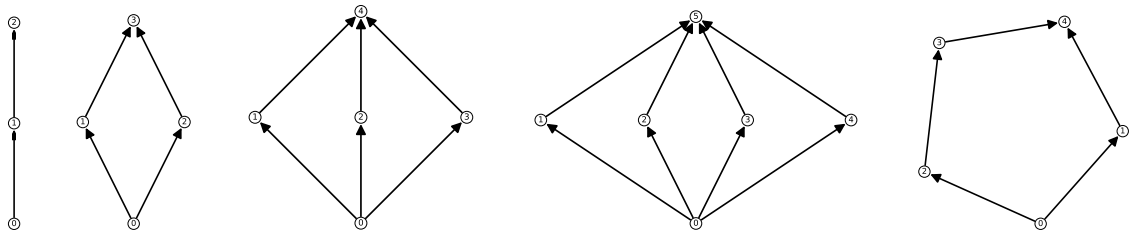


Figura 2.1: Posets M_1, M_2, M_3, M_4 e N_5.

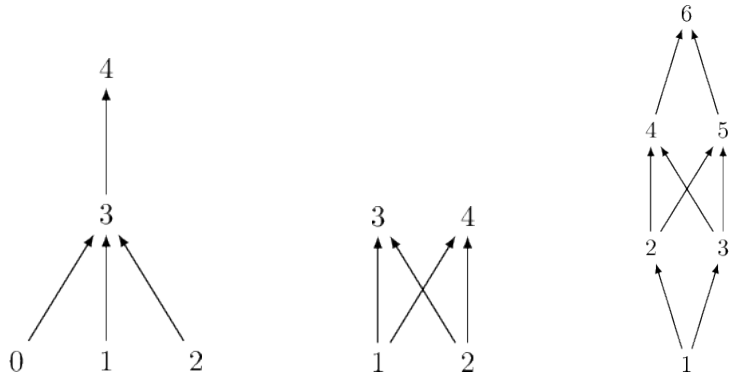


Figura 2.2: Outros posets.

Definición 2.2. Sexa $(P, \leq)$ un conxunto parcialmente ordenado.

1. A orde $\leq$ chámase **orde total** ou **orde lineal** se cada dous elementos de P son comparables, é dicir, se dados dous elementos $a, b \in P$, tense que $a \leq b$ ou $b \leq a$. Neste caso, $(P, \leq)$ chámase **conxunto totalmente ordenado** ou **conxunto linealmente ordenado**.

2. Un subconxunto non baleiro de P que é totalmente ordenado recibe o nome de **cadea** en P.

3. A **lonxitude dunha cadea** finita P é $|P| - 1$. Dise que un poset P ten unha **lonxitude n**, con $n \in \mathbb{N}$, se a cadea de P con lonxitude máxima ten lonxitude n.

4. Para dous elementos a, b nun poset P de xeito que $a \leq b$, o **intervalo** (pechado) $[a, b]$ defínese por $[a, b] \coloneqq \{x \in P \mid a \leq x \leq b\}$. Contén polo menos os elementos a e b. Esta definición xeneraliza a definición de intervalo dos números reais.

Exemplo 2.3.

- O conxunto $\mathbb{N} = \{0, 1, \dots\}$ dos números naturais, xunto coa relación $\mid$ que se define como $n \mid m$ se e só se n divide a m, é un conxunto parcialmente ordenado:

  1. Cumpre a propiedade reflexiva pois todo elemento é divisor de si mesmo.
  2. Para todo par de números naturais n e m, se $n \mid m$ e $m \mid n$ necesariamente n e m deben ser iguais. Podemos escribir n e m como $m = nr$ e $n = ms$, con $r, s \in \mathbb{N}$, polo que $rs = 1$, do que deducimos que $r = s = 1$, verificando así a propiedade antisimétrica.
  3. Sexan $n, m, l \in \mathbb{N}$ de xeito que $n \mid m$ e $m \mid l$, entón $m = nr$ e $l = ms$, con $r, s \in \mathbb{N}$. Así, $l = nrs$, polo que $n \mid l$ e cúmprese a propiedade transitiva.

  Este conxunto non é de orde total pois contén elementos que non poden ser comparados como o 2 e o 3, nin $2|3$ nin $3|2$. A $(\mathbb{N}, |)$ chamarémolo conxunto de divisores naturais e denotarémolo por T_∞. Para $n \in \mathbb{N}$ escribimos T_n para o intervalo $[1, n]$ en T_∞ que se corresponde cos divisores de n. No caso dos divisores de 30, T_{30}, o diagrama de Hasse será da forma:

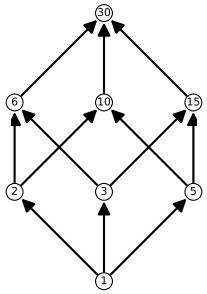


Figura 2.3: Diagrama de Hasse do poset dos divisores de 30.

- O conxunto $\mathbb{N}$ coa relación $\leq$ usual tamén é de orde parcial, e ademais é de orde total.

- Sexa X un conxunto. O conxunto partes de X, denotado por $\mathcal{P}(X)$ e que se define como o conxunto formado por todos os subconxuntos do conxunto dado X, coa relación de inclusión $\subseteq$ é un poset, pero non é de orde total. Para o caso finito do conxunto $\{a, b, c\}$ o diagrama de Hasse que describe a relación de inclusión para o conxunto $\mathcal{P}(\{a, b, c\})$ é o seguinte:

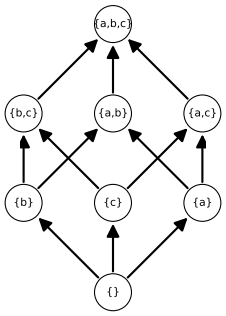


Figura 2.4: Diagrama de Hasse do poset do conxunto de partes de $\{a, b, c\}$.

- O conxunto $X = \{2, 3, 6, 12, 24, 36\}$ é un poset coa relación divisibilidade $|$, pero non é de orde total.

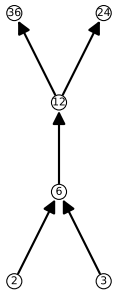


Figura 2.5: Diagrama de Hasse do poset X.

- De todos os posets das Figuras 2.1 e 2.2, o único que é de orde total é M_1.

Definición 2.4. Sexa $(P, \leq)$ un conxunto parcialmente ordenado e S un subconxunto de P.

1. Un elemento $u \in P$ é unha **cota superior** para S se

$$s \leq u \text{ para todo } s \in S.$$

O elemento máis pequeno entre as cotas superiores u de S, de existir, denomínase **supremo** ou **join** de S e denótase por $\bigvee S$. Así, $\bigvee S$ ten a propiedade de que $s \leq \bigvee S$

para todo $s \in S$ e se $s \leq x$ para todo $s \in S$, entón $\bigvee S \leq x$. O supremo dun conxunto finito $S = \{a_1, \dots, a_n\}$ denótase tamén como $a_1 \bigvee \cdots \bigvee a_n$.

2. Un elemento $l \in P$ é unha **cota inferior** de S se

$$l \leq s \text{ para todo } s \in S.$$

O maior elemento entre as cotas inferiores l de S, de existir, denomínase **ínfimo** ou **meet** de S e denótase por $\bigwedge S$. Así, $\bigwedge S$ ten a propiedade de que $\bigwedge S \leq s$ para todo $s \in S$ e se $x \leq s$ para todo $s \in S$, entón $x \leq \bigwedge S$. O ínfimo dun conxunto finito $S = \{a_1, \dots, a_n\}$ denótase tamén como $a_1 \bigwedge \cdots \bigwedge a_n$.

Definición 2.5. Dados dous posets P e Q, o poset **produto directo** está definido como

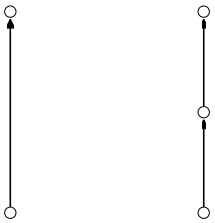
$$(P \times Q, \leq_{P \times Q}),$$

onde $P \times Q$ denota o produto cartesiano de P e Q e $\leq_{P \times Q}$ é a orde produto

$$(p_1, q_1) \leq_{P \times Q} (p_2, q_2) \Longleftrightarrow p_1 \leq_P p_2 \quad \text{e} \quad q_1 \leq_Q q_2.$$

A definición pode estenderse a un conxunto arbitrario de posets.

Exemplo 2.6. Consideremos as cadeas P de dous elementos e Q de tres elementos, con ordes parciais descritas, respectivamente, polos seguintes diagramas de Hasse:



A continuación representamos os diagramas dos produtos directos $P \times P$, $P \times Q$, $P \times P \times P$, $P \times P \times Q$ e $P \times Q \times Q$ respectivamente:

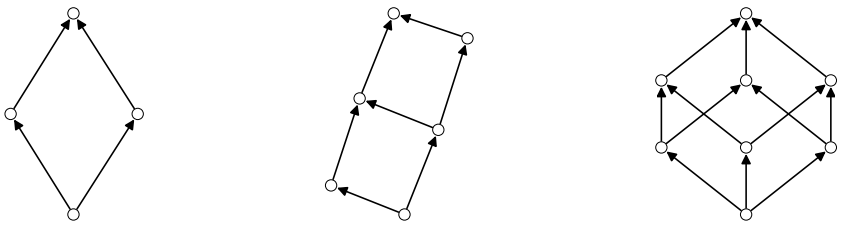


Figura 2.6: Produtos directos de posets.

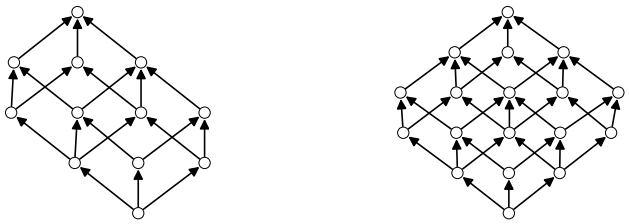


Figura 2.7: Produtos directos de posets.

Definición 2.7. Sexa $(P, \leq)$ un conxunto parcialmente ordenado. Diremos que P satisfai a **condición maximal** se non contén ningunha sucesión infinita de elementos $x_1, x_2, \ldots$ tales que $x_1 < x_2 < x_3 < \cdots$. Analogamente, diremos que P satisfai a **condición minimal** se non contén ningunha sucesión infinita de elementos $x_1, x_2, \ldots$ tales que $x_1 > x_2 > x_3 > \cdots$

2.2. Conservación da orde

Diremos que unha aplicación entre conxuntos parcialmente ordenados $f\colon P \longrightarrow Q$ **conserva a orde** se dados dous elementos x, y de xeito que $x \leq y$ entón $f(x) \leq f(y)$. E diremos que é un **embebemento de orde** se verifica: $x \leq y$ se e só se $f(x) \leq f(y)$.

Nótese que todo embebemento de orde é inxectivo, xa que $f(x) = f(y)$ implica que tanto $f(x) \leq f(y)$ coma que $f(y) \leq f(x)$, o que á súa vez implica que $x \leq y$ e $y \leq x$, é dicir, $x = y$. Se ademais é sobrexectivo, denominarémolo **isomorfismo de orde**.

Exemplo 2.8. Os posets dos divisores de 30, T_{30}, e do conxunto de partes de $\{a, b, c\}$ son isomorfos (de orde), como se aprecia na Figura 2.3 e na Figura 2.4.

No capítulo seguinte veremos outro exemplo máis interesante que aínda non podemos presentar por non ter desenvolvido o marco teórico necesario.

2.3. Retículos e homomorfismos de retículos

Moitas propiedades dun conxunto parcialmente ordenado P exprésanse en termos da existencia de cotas superiores e inferiores de subconxuntos de P. Dúas das clases máis importantes de posets definidos a partir destes obxectos son os retículos e os retículos completos. Ao longo desta sección tamén veremos tres tipos de retículos: os distributivos, os modulares e os booleanos, así como algunhas propiedades básicas.

Definición 2.9.

1. Un conxunto parcialmente ordenado $(P,\leq)$ é un **retículo** se cada par de elementos de P teñen supremo e ínfimo. Isto é equivalente a dicir que cada subconxunto finito de P ten supremo e ínfimo.

2. Un conxunto parcialmente ordenado $(P,\leq)$ é un **retículo completo** se todo subconxunto de P ten supremo e ínfimo.

Así, un retículo completo ten un elemento máximo (supremo de P) e un elemento mínimo (ínfimo de P). Se P é un conxunto finito, os conceptos de retículo e retículo completo coinciden.

Exemplo 2.10.

- Os posets da Figura 2.1 son retículos mentres que os da Figura 2.2 non o son.

- Toda cadea $(P,\leq)$ é un retículo onde $a \vee b = b$ e $a \wedge b = a$ se $a \leq b$. En particular, o conxunto dos números naturais $\mathbb{N}$ coa relación $\leq$ usual, $(\mathbb{N},\leq)$, é un retículo onde $x \vee y = \text{máx}(x,y)$ e $x \wedge y = \text{mín}(x,y)$. Pero non é completo xa que o conxunto total $\mathbb{N}$ non ten supremo.

- O poset $\mathcal{P}(X)$ introducido no Exemplo 2.3 é un retículo completo onde o supremo e ínfimo veñen dados pola unión e a intersección, é dicir,

$$\bigvee_{i\in I} A_i = \bigcup_{i\in I} A_i$$

$$\bigwedge_{i\in I} A_i = \bigcap_{i\in I} A_i$$

  onde os A_i son elementos de $\mathcal{P}(X)$ e I é un conxunto arbitrario. Vexamos que esta afirmación e certa para o ínfimo, xa que para o supremo a proba é análoga. Sexa $\{A_i\}_{i\in I}$ unha familia de elementos de $\mathcal{P}(X)$. Dado que $\bigcap_{i\in I} A_i \subseteq A_j$ para todo $j \in I$, séguese que $\bigcap_{i\in I} A_i$ é unha cota inferior de $\{A_i\}_{i\in I}$. Ademais, se $B \in \mathcal{P}(X)$ é unha cota inferior de $\{A_i\}_{i\in I}$, entón $B \subseteq \bigcap_{i\in I} A_i$. Así, $\bigcap_{i\in I} A_i$ é necesariamente a maior das cotas inferiores de $\bigcap_{i\in I} A_i$ en $\mathcal{P}(X)$.

- Se no exemplo anterior consideramos un conxunto G con estrutura de grupo, é inmediato ver que o conxunto $L(G)$ de todos os seus subgrupos coa inclusión ten por ínfimo dunha familia $\mathcal{F} = \{H_i\}_{i\in I}$ a $\bigwedge \mathcal{F} = \bigwedge_{i\in I} H_i = \bigcap_{i\in I} H_i$ e por supremo a $\bigvee \mathcal{F} = \bigvee_{i\in I} H_i = \langle \bigcup_{i\in I} H_i \rangle$. Así, $L(G)$ é un retículo completo, e referirémonos a el como **retículo de subgrupos de** G. Centrarémonos neles no seguinte capítulo.

En particular, os subgrupos normais tamén forman un retículo que denotaremos por $\mathfrak{N}(G)$.

- O conxunto dos divisores naturais que vimos no Exemplo 2.3, T_∞, é un retículo co máximo común divisor como ínfimo e co mínimo común múltiplo como supremo, isto é, $x \vee y = \text{mcm}(x, y)$ e $x \wedge y = \text{mcd}(x, y)$ para $x, y \in \mathbb{N}$. Pero non é completo pois $\mathbb{N}$ non ten supremo. Para $n \in \mathbb{N}$ acostumaremos a chamar a T_n o **retículo de todos os divisores de** n.

- O poset $X = \{2, 3, 6, 12, 24, 36\}$ coa relación de divisibilidade non é un retículo, xa que $\text{mcm}(24, 36)$ e $\text{mcd}(2, 3)$ non existen en S (véxase a Figura 2.5).

- O produto directo de retículos é un retículo, onde

$$(x_1, y_1) \wedge (x_2, y_2) = (x_1 \wedge x_2, y_1 \wedge y_2) \quad \text{e} \quad (x_1, y_1) \vee (x_2, y_2) = (x_1 \vee x_2, y_1 \vee y_2).$$

  Claramente, todos os posets da Figura 2.6 son retículos.

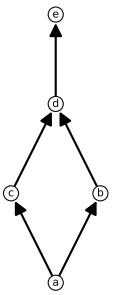
  Notemos que o retículo T_n dos divisores de n é produto directo das cadeas de lonxitude $n_1, \ldots, n_r$ onde $n = p_1^{n_1} \cdots p_r^{n_r}$ para $p_1, \ldots, p_r$ primos distintos. Por exemplo, xa que $30 = 2^1 \cdot 3^1 \cdot 5^1$, o retículo T_{30} será o produto directo de tres cadeas de lonxitude 1, como se pode ver nas Figuras 2.3 e 2.6.

Definición 2.11. Sexan P e L retículos. Unha aplicación $f \colon P \longrightarrow L$ dise un **homomorfismo de retículos** se f conserva supremos e ínfimos, é dicir, para todo $a, b \in P$,

- f conserva o supremo: $f(a \vee b) = f(a) \vee f(b)$;
- f conserva o ínfimo: $f(a \wedge b) = f(a) \wedge f(b)$.

Un homomorfismo de retículos bixectivo é un **isomorfismo de retículos**.

Notemos que todo homomorfismo de retículos $f \colon P \longrightarrow L$ conserva a orde, xa que se $a, b \in P$ con $a \leq b$, tense que $f(a) = f(a \wedge b) = f(a) \wedge f(b)$, polo que $f(a) \leq f(b)$. Porén, non toda aplicación que conserva a orde é un homomorfismo de retículos, como amosa o seguinte exemplo.

Exemplo 2.12. A aplicación f ente os retículos 

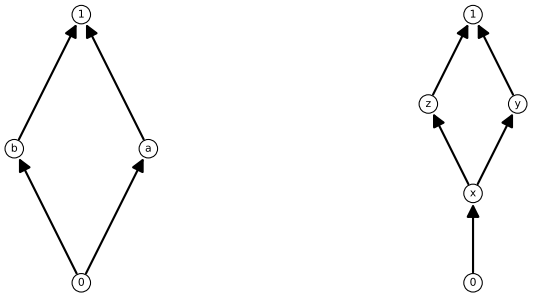
e 

definida por $f(a) = 0$,

$f(b) = f(c) = f(d) = 1$, $f(e) = 2$, conserva a orde pero non é un homomorfismo de retículos, xa que $f(b \wedge c) = 0 \neq f(b) \wedge f(c) = 1$.

Fixémonos en que a aplicación f do exemplo anterior non pode ser un embebemento de orde, xa que non é inxectiva. Presentamos a continuación outro exemplo no que comprobamos que os embebementos de orde tampouco teñen por que ser homomorfismos de retículos.

Exemplo 2.13. Consideremos os conxuntos $P = \{0, a, b, 1\}$ e $Q = \{0, x, y, z, 1\}$ con ordes parciais descritas, respectivamente, polos diagramas de Hasse seguintes:



Sexa a aplicación $f\colon P \longrightarrow Q$ definida por $f(0) = 0$, $f(a) = y$, $f(b) = z$ e $f(1) = 1$. Claramente, f é un embebemento de orde. Se escollemos o conxunto $S = \{a, b\}$ temos que $\bigwedge S = a \wedge b = 0$. Dado que $f(0) = 0 \leq x \leq f(a) = y$ e, da mesma forma, $f(0) \leq x \leq f(b) = z$, $f(0)$ é cota inferior de $f(S)$. Pero $f(S)$ ten outra cota inferior: x. Temos que $\bigwedge f(S) = x \neq 0$, logo f non preserva os ínfimos e non pode ser homomorfismo de retículos.

Agora ben, ao pasar aos isomorfismos non imos atopar conflitos como os anteriores xa que os conceptos de isomorfismo de orde e isomorfismo de retículos resultan ser equivalentes. Verémolo na seguinte proposición xunto con un relación entre a conservación da orde e a conservación de ínfimos e supremos máis fina que a exposta anteriormente.

Proposición 2.14 ([2])**.** *Sexan P e L retículos e $f\colon P \longrightarrow L$ unha aplicación.*

1. *As seguintes afirmacións son equivalentes:*

   - *f conserva a orde;*
   - *$f(a \vee b) \geq f(a) \vee f(b)$, para todo $a, b \in P$;*
   - *$f(a \wedge b) \leq f(a) \wedge f(b)$, para todo $a, b \in P$;*

   En particular, se f é un homomorfismo de retículos, entón f conserva a orde.

2. *f é un isomorfismo de retículos se e só se f é un isomorfismo de orde.*

Demostración. A proba de 1 é inmediata. En canto a 2, só é necesario probar que os isomorfismos de orde conservan supremos e ínfimos.

Sexan $x, y \in P$. Se $x \leq y$, isto equivale a que $x \wedge y = x$ (ou $x \vee y = y$). Sexa S un subconxunto de P tal que existe $z = \bigwedge S$. Como f é un isomorfismo de orde, entón $f(z)$ é cota inferior de $f(S)$ e toda cota inferior de $f(S)$ é da forma $f(w)$ onde w é cota inferior de S. Por ser z a maior das cotas inferiores de S, $w \leq z$ e polo tanto $f(w) \leq f(z)$. Entón, $f(z)$ é a maior das cotas inferiores de $f(S)$, isto é, $f(\bigwedge S) = \bigwedge f(S)$. De forma análoga próbase que $f\left(\bigvee S\right) = \bigvee f(S)$. □

A continuación amosase unha listaxe de todos os retículos (non isomorfos) de cardinalidade menor ou igual que 5:

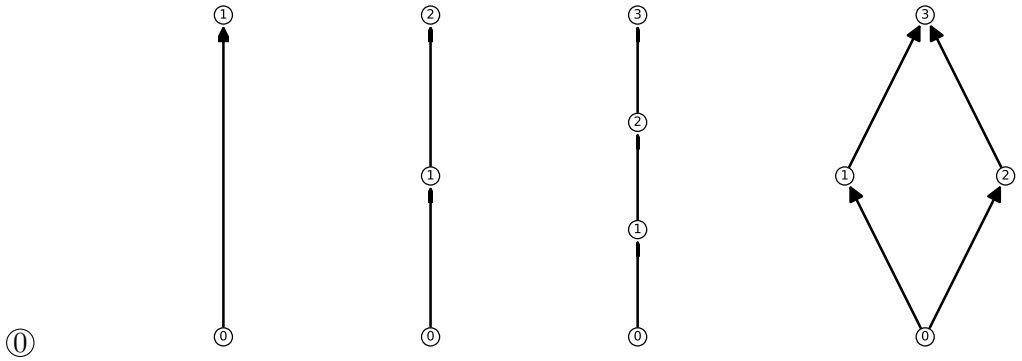


Figura 2.8: Retículos con número de elementos menor ou igual que 4.

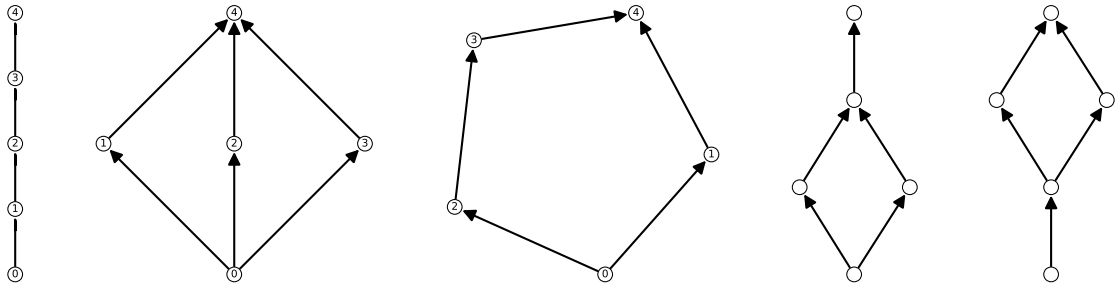


Figura 2.9: Retículos con 5 elementos.

Podemos ver que hai un retículo con 1 elemento, un con 2 elementos, un con 3 elementos, dous con 4 elementos, e cinco con 5 elementos.

A medida que engadimos elementos, aumenta o número de posibles retículos. Continuando coa listaxe, hai 16 retículos con 6 elementos, 53 con 7 elementos, 222 con 8

elementos, 1 078 con 9 elementos, 5 994 con 10 elementos, ... , e por exemplo, hai 165 269 824 761 con 18 elementos.

Os ínfimos e os supremos dos retículos satisfán unhas certas relacións que nos poden servir para caracterizalos, como veremos nos resultados seguintes.

Proposición 2.15 ([2]). *Sexa P un retículo. Entón para calesquera $x, y, z \in P$ satisfaise:*

1. *Lei idempotente:* $x \vee x = x \qquad x \wedge x = x$;
2. *Lei conmutativa:* $x \vee y = y \vee x \qquad x \wedge y = y \ \wedge x$;
3. *Lei asociativa:* $x \vee (y \vee z) = (x \vee y) \vee z \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z$;
4. *Lei absorción:* $x \vee (x \wedge y) = x \qquad x \wedge (x \vee y) = x$.

Proposición 2.16 ([2]). *En calquera retículo P satisfanse as seguintes desigualdades:*

1. *Desigualdades distributivas:*
   - $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$;
   - $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$;
2. *Desigualdades modulares:*
   - $x \leq z \iff x \vee (y \wedge z) \leq (x \vee y) \wedge z$;
   - $z \geq x \iff x \wedge (y \vee z) \geq (x \wedge y) \vee z$;

para todo $x, y, z \in P$.

Teorema 2.17 ([2]). *Sexa P un conxunto non baleiro con dúas operacións binarias.*

P é un retículo se e só se as dúas operacións binarias satisfán as leis da Proposición 2.15, onde a relación de orde $\leq$ en P é $x \leq y$ se $x \vee y = y$.

Ademais das relacións das Proposicións 2.15 e 2.16, os retículos poden cumprir outras propiedades destacadas, dando lugar a tipos particulares de retículos.

No que segue desta sección centrarémonos en estudar dúas clases importantes de retículo: os distributivos e os modulares.

Definición 2.18. Sexa $(P,\leq)$ un retículo. Diremos que un retículo $(P,\leq)$ é **distributivo** se satisfai as seguintes leis, coñecidas como **leis distributivas**:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

para todo $x, y, z \in P$.

Cabe destacar que un retículo é distributivo se, e só se, verifica unha destas dúas leis. Se, por exemplo, $(P, \leq)$ verifica a primeira, entón para $x, y, z \in P$ temos:

$$\begin{aligned}(x \wedge y) \vee (x \wedge z) &= ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee z) = x \wedge (z \vee (x \wedge y)) \\ &= x \wedge ((z \vee x) \wedge (z \vee y)) = x \wedge (y \vee z);\end{aligned}$$

que é a segunda lei distributiva. A outra implicación próbase de xeito similar.

Definición 2.19. Sexa $(P,\leq)$ un retículo. Diremos que un retículo $(P,\leq)$ é **modular** se satisfai a **lei modular**:

$$x \vee (y \wedge z) = (x \vee y) \wedge z$$

para todo $x, y, z \in P$ con $x \leq z$.

Da Proposición 2.16 deducimos que para que se cumpra a lei modular só se require a desigualdade $x \vee (y \wedge z) \geq (x \vee y) \wedge z$.

Exemplo 2.20.

1. Unha cadea é un retículo distributivo e modular.

2. O retículo dos divisores de n, T_n, é un retículo distributivo.

3. O retículo conxunto de partes $P(X)$ dun conxunto X é distributivo.

4. Sexa o conxunto $X = \{0, a, b, c, 1\}$ coa orde parcial descrita polo diagrama de Hasse da Figura 2.10. Estamos ante un retículo que non é distributivo pois $a \wedge (b \vee c) = a$ pero $(a \wedge b) \vee (a \wedge c) = 0$, é dicir, non cumpre as leis distributivas.

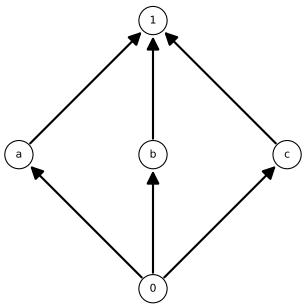


Figura 2.10: Diagrama de Hasse do Diamante M_3.

A forma deste diagrama é coñecida co nome de Diamante ou M_3. Ademais, este retículo é modular.

5. Os conxuntos que teñen como diagrama de Hasse o pentágono N_5, representado na Figura 2.11, son retículos non modulares. No pentágono tense que:

$$x \vee (y \wedge z) = x \vee 0 = x,$$

$$(x \vee y) \wedge (x \vee z) = 1 \wedge z = z,$$

co que tampouco é distributivo. Isto ten sentido pola proposición que veremos tras os exemplos.

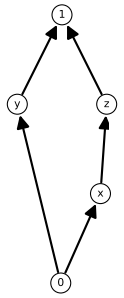


Figura 2.11: Diagrama de Hasse do Pentágono N_5.

6. Todos os retículos con número de elementos menor ou igual a 4 son distributivos e modulares. Ademais, dos cinco retículos con 5 elementos todos son distributivos menos o diamante M_3 e o pentágono N_5, e todos son modulares menos o pentágono N_5.

7. Algúns exemplos de retículos modulares son os subgrupos normais dun grupo, os ideais dun anel ou os subespazos vectoriais dun espazo vectorial.

Proposición 2.21. *Todo retículo distributivo é modular.*

Demostración. Sexa P un retículo e $x, y, z \in P$. Se $x \leq z$, entón $x \vee z = z$ e como P é distributivo $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z$, cumpríndose así a lei modular. □

Para finalizar esta sección, introduciremos unha última clase de retículos que, a diferenza das anteriores, non está definida a través de identidades.

Sexa P un retículo con ínfimo e supremo globais, denotados por 0 e 1, respectivamente. Para $a \in P$ dise que $b \in P$ é un **complemento** de a se $a \wedge b = 0$ e $a \vee b = 1$. Se a ten un único complemento denótase por a'.

Definición 2.22. Un retículo P dise **booleano** se

1. P é distributivo;

2. P ten 0 e 1;

3. cada $a \in P$ ten un (necesariamente único) complemento $a' \in P$.

Exemplo 2.23. Para calquera conxunto X, sexa $A' = X \setminus A$ para todo $A \subseteq X$. O retículo conxunto de partes $P(X)$ coa estrutura $(P(X), \cup, \cap, ', \emptyset, X)$ é booleano.

A importancia deste exemplo vén dada polo seguinte teorema.

Teorema 2.24 ([2])**.** *Calquera retículo booleano finito é isomorfo a un retículo de partes dun conxunto finito.*

2.4. Subretículos

Os subretículos requiren máis coidado, xa que un subconxunto non baleiro S dun retículo P herda a orde de P, pero non necesariamente os ínfimos e supremos de P. É dicir, o ínfimo dun subconxunto T de S pode ser diferente cando consideramos T como un subconxunto de S que cando o consideramos como un subconxunto de P.

Definición 2.25. Sexa P un retículo e $M \subseteq P$ un subconxunto non baleiro de P.

1. M é un **subretículo** de P se o ínfimo en M de calquera subconxunto finito non baleiro $S \subseteq M$, que chamaremos M-ínfimo e denotaremos por $\bigwedge_M S$, existe e é o mesmo que o P-ínfimo de S, e do mesmo xeito para o supremo en M que chamaremos M-supremo e denotaremos por $\bigvee_M S$, isto é, se

$$\bigwedge_M S = \bigwedge_P S \quad \text{e} \quad \bigvee_M S = \bigvee_P S.$$

2. Se P é un retículo completo, entón M é un **subretículo completo** de P se o M-ínfimo de calquera subconxunto $S \subseteq M$ existe e é o mesmo que o P-ínfimo de S, e do mesmo xeito para o supremo, isto é, se

$$\bigwedge_M S = \bigwedge_P S \quad \text{e} \quad \bigvee_M S = \bigvee_P S.$$

Proposición 2.26 ([8])**.**

1. *Un subconxunto non baleiro M dun retículo P é un subretículo de P se, e só se, o P-ínfimo e o P-supremo de calquera subconxunto finito non baleiro $A \subseteq M$ pertencen a M.*

2. *Un subconxunto non baleiro M dun retículo completo P é subretículo completo se, e só se, o P-ínfimo e o P-supremo de calquera subconxunto $A \subseteq M$ pertencen a M.*

A continuación veremos algunhas caracterizacións de retículos distributivos e modulares empregando subretículos e os retículos M_3 e N_5 que vimos no Exemplo 2.20.

Teorema 2.27. *Un retículo P é modular se, e só se, non ten un subretículo isomorfo ao pentágono N_5.*

Equivalentemente, P é modular se e só se $x \leq y$, $a \wedge x = a \wedge y$, $a \vee x = a \vee y$ implica que $x = y$.

Demostración. En primeiro lugar, notemos que a equivalencia é inmediata.

Se P é modular, entón cada subretículo de P é modular e, como vimos no Exemplo 2.20, non pode ser isomorfo ao pentágono. Probaremos que cada retículo non modular P contén un subretículo isomorfo a N_5. Por ser P non modular, existen $x, y, z \in P$ con $x \leq z$ e $x \vee (y \wedge z) < (x \vee y) \wedge z$. Sexa $a = y \wedge z$, $b = x \vee (y \wedge z)$, $c = (x \vee y) \wedge z$, $d = y$, $e = x \vee y$ e $S = \{a, b, c, d, e\}$. Entón, claramente, $a \leq b < c \leq e$ e $a \leq d \leq e$.
Ademais

$$c \wedge d = (x \vee y) \wedge z \wedge y = e \wedge a = a$$

e

$$b \vee d = x \vee (y \wedge z) \vee y = e \vee a = e;$$

séguese que $b \wedge d = a$ e $c \vee d = e$. O resto de ínfimos e supremos dos subconxuntos de S saen trivialmente das cadeas de desigualdades iniciais e pertencen a S. Aplicando a Proposición 2.26 temos que S é un subretículo de P que, claramente, é isomorfo ao pentágono, $S \simeq N_5$. □

Teorema 2.28 (Birkhoff)**.** *Un retículo P é distributivo se, e só se, non ten ningún subretículo isomorfo ao pentágono N_5 nin ao diamante M_3.*

Equivalentemente, P é distributivo se e só se $z \wedge x = z \wedge y$ e $z \vee x = z \vee y$ implica que $x = y$.

Demostración. Nótese en primeiro lugar que estas dúas afirmacións son equivalentes. En efecto, se $x \wedge z = y \wedge z$ e $x \vee z = y \vee z$ con $x \neq y$ entón os dous retículos en cuestión xorden dos casos $x \leq y$ e $x \not\leq y$, que se corresponden cos casos N_5 e M_3 respectivamente.

Supoñamos que P é distributivo e que existen $x, y, z \in P$ tales que $x \wedge z = y \wedge z$ e $x \vee z = y \vee z$. Probaremos que $x = y$. Teremos

$$\begin{aligned} x = x \wedge (x \vee z) = x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ &= (x \wedge y) \vee (y \wedge z) \\ &= y \wedge (x \vee z) = y \wedge (y \vee z) = y. \end{aligned}$$

Empregando a equivalencia, vemos que P non terá subretículos das formas pentágono N_5 nin diamante M_3.

Reciprocamente, se P non ten subretículos de ningunha das forma anteriores, entón polo Teorema 2.27 deducimos que P ten que ser modular. Dados $a, b, c \in P$ definimos:

$$a^* = (b \vee c) \wedge a,\ b^* = (c \vee a) \wedge b,\ c^* = (a \vee b) \wedge c.$$

Entón, claramente $a^* \wedge c^* = a \wedge c,\ b^* \wedge c^* = b \wedge c$ e $a^* \wedge b^* = a \wedge b$. Sexa agora

$$d = (a \vee b) \wedge (b \vee c) \wedge (c \vee a).$$

Logo, como $a^* \leq a \leq a \vee b$ e $c \leq b \vee c$, empregando a modularidade de P vemos que

$$\begin{aligned} a^* \vee c^* &= a^* \vee [(a \vee b) \wedge c] \\ &= (a^* \vee c) \wedge (a \vee b) \\ &= ([(b \vee c) \wedge a] \vee c) \wedge (a \vee b) \\ &= (b \vee c) \wedge (a \vee c) \wedge (a \vee b) \\ &= d. \end{aligned}$$

Por simetría deducimos que

$$a^* \vee c^* = a^* \vee b^* = b^* \vee c^* = d.$$

Observamos agora que

$$\begin{cases} c^* \vee a^* \vee (b \wedge c) = (b^* \vee c^*) \vee (b^* \wedge c^*) = (b^* \vee c^*) = d; \\ c^* \wedge [a^* \vee (b \wedge c)] = (c^* \wedge a^*) \vee (b \wedge c) = (a \wedge c) \vee (b \wedge c). \end{cases}$$

onde na segunda ecuación empregamos a modularidade de P xa que $b \wedge c \leq c^*$. Por simetría,

$$\begin{cases} c^* \vee b^* \vee (a \wedge c) = d; \\ c^* \wedge [b^* \vee (a \wedge c)] = (a \wedge c) \vee (b \wedge c). \end{cases}$$

Por hipótese, deducimos que $a^* \vee (b \wedge c) = b^* \vee (a \wedge c)$ de onde

$$a^* \vee (b \wedge c) = a^* \vee (b \wedge c) \vee b^* \vee (a \wedge c) = a^* \vee b^* = d.$$

Séguese disto que

$$(a \vee b) \wedge c = c^* = c^* \wedge d = c^* \wedge [a^* \vee (b \wedge c)] = (a \wedge c) \vee (b \wedge c)$$

e así P cumpre unha das leis distributivas, que como probamos despois da Definición 2.18, é suficiente para afirmar que P é distributivo. □

Corolario 2.29. *Un retículo modular é distributivo se e só se non contén ao diamante, M_3, como un subretículo.*

Capítulo 3

Retículos de subgrupos

Imos centrarnos agora nos retículos de subgrupos que introducimos anteriormente no Exemplo 2.10. Comezaremos cuns exemplos notorios nos que aplicaremos resultados explicados no capítulo anterior. A continuación amosaremos o motivo da importancia dos retículos de subgrupos, e finalizaremos o capítulo introducindo unha variante do retículo de subgrupos: os retículos de subgrupos nivelados.

3.1. Exemplos importantes

3.1.1. Grupo de permutacións S_3

Denotamos por S_3 o grupo de permutacións de tres elementos, formado polas permutacións dos elementos $\{1,2,3\}$, é dicir, $S_3 = \{1,(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$.
Como a orde do grupo S_3 é 6, o Corolario 1.3 do teorema de Lagrange permítenos afirmar que podemos ter subgrupos de orde 1, 2, 3 e 6. Calculemos os subgrupos de S_3:

1. En primeiro lugar temos os subgrupos obvios: $\{1\}$ e S_3, onde $|\,\{1\}\,| = 1$ e $|S_3| = 6$.

2. Subgrupos de orde 2:
   Dado que todo grupo de orde primo é cíclico, os subgrupos de orde 2 serán cíclicos, é dicir, xerados por un só elemento. Se H é un subgrupo de orde 2 será da forma $H = \{1,a\} = \langle a \rangle$ onde o elemento a ten orde 2. Como os tres elementos de orde 2 de S_3 xeran grupos distintos, teremos os seguintes subgrupos: $\{1,(1,2)\}$, $\{1,(1,3)\}$, $\{1,(2,3)\}$.

3. Subgrupos de orde 3:
   De igual forma que no caso de grupos de orde 2, 3 é primo e por tanto os subgrupos de orde 3 serán cíclicos e xerados por un elemento de orde 3, entón buscamos un

subgrupo da forma $K = \{1, a, a^2\} = \langle a \rangle$. En S_3 temos dous elementos elementos de orde 3 e ambos xeran o mesmo grupo, polo que o único subgrupo de orde 3 é $\{1, (1,2,3), (1,3,2)\}$.

Polo Corolario 1.3, ningún destes grupos está contido noutro, obviando as inclusións triviais, polo que o retículo de subgrupos de S_3 é da forma da Figura 3.1, onde, no primeiro diagrama, H_1, H_2, H_3 e H_4 representan os subgrupos de S_3, no segundo o seu cardinal e no terceiro a súa estrutura.

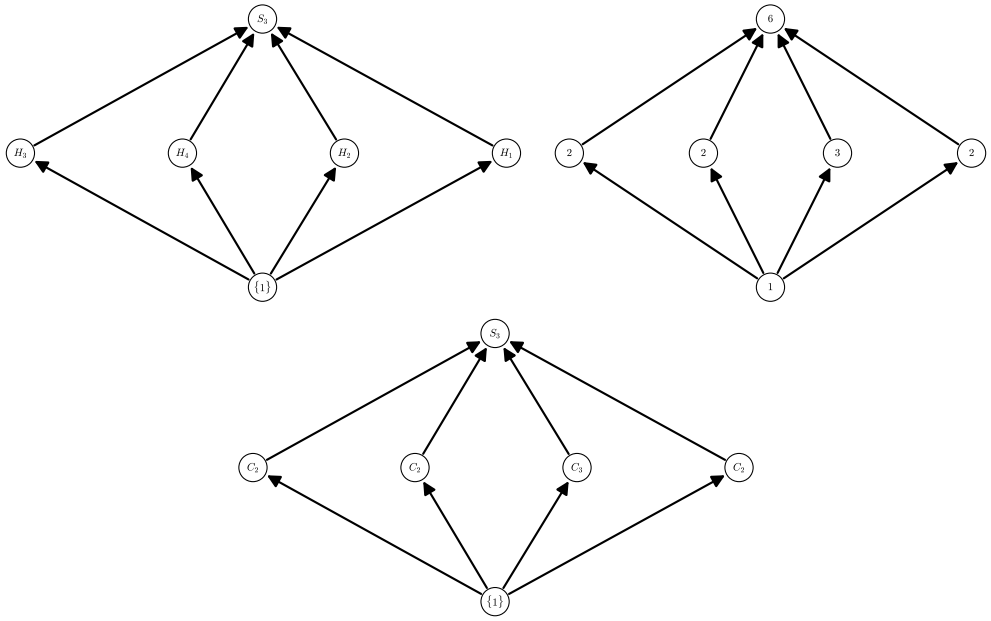


Figura 3.1: Retículo de subgrupos do grupo de permutacións S_3.

3.1.2. Grupo alternado A_4

Sexa o grupo alternado A_4, subgrupo do grupo de permutacións S_4 cuxos elementos poden descompoñerse nun número par de transposicións. Este grupo está formado polos elementos $A_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2)(2,3), (2,3)(1,2), (1,2)(2,4), (2,4)(1,2), (2,3)(2,4), (2,4)(2,3), (1,3)(3,4), (3,4)(1,3)\}$, onde os elementos teñen orde:

1. Orde 1: $\{1\}$.
2. Orde 2: $\{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.
3. Orde 3: $\{(1,2)(2,3), (2,3)(1,2), (1,2)(2,4), (2,4)(1,2), (2,3)(2,4), (2,4)(2,3), (1,3)(3,4), (3,4)(1,3)\}$.

A orde de A_4 é $|A_4| = \dfrac{4!}{2} = 12$. Aplicando o Corolario 1.3 podemos afirmar que pode ter subgrupos de orde 1, 2, 3, 4, 6 e 12. Pero A_4 non ten subgrupos de orde 6. Supoñamos que existe un subgrupo H de orde 6. Como en A_4 non hai ningún elemento de orde 6, tampouco o haberá en H. Polo tanto, H non é cíclico e como a súa orde é 6, deducimos que H ten que ser isomorfo a S_3.

S_3 ten tres elementos de orde 2 e dous elementos de orde 3, polo que deducimos que os elementos de orde 2 de A_4 estarán en H, isto é: $(1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \in H$.

Nótese que:

$$\big((1,2)(3,4)\big)\big((1,3)(2,4)\big) = (1,4)(2,3)$$

$$\big((1,2)(3,4)\big)\big((1,4)(2,3)\big) = (1,3)(2,4)$$

$$\big((1,3)(2,4)\big)\big((1,2)(3,4)\big) = (1,4)(2,3)$$

$$\big((1,3)(2,4)\big)\big((1,4)(2,3)\big) = (1,2)(3,4)$$

Polo tanto, $K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ é un subgrupo de H. Pero $|K| = 4$ e 4 non divide a 6, co que chegamos a unha contradición co Corolario 1.3.

Unha vez comprobado que non temos subgrupos de orde 6, imos calcular os subgrupos de A_4.

1. Os subgrupos obvios son $\{1\}$ e A_4 onde $|\,\{1\}\,| = 1$ e $|A_4| = 12$.

2. Subgrupos de orde 2:
   Son os grupos da forma $\{1, a\} = \langle a \rangle$ onde a é un elemento de orde 2. Temos tres subgrupos de orde 2: $\{1, (1,2)(3,4)\}$, $\{1, (1,3)(2,4)\}$ e $\{1, (1,4)(2,3)\}$.

3. Subgrupos de orde 3:
   Son os subgrupos da forma $\{1, a, a^2\} = \langle a \rangle$ onde a orde de a é 3. É sinxelo ver que $\langle (1,2)(2,3) \rangle = \langle (2,3)(1,2) \rangle$ co que un subgrupo de orde 3 será $\{1, (1,2)(2,3), (2,3)(1,2)\}$.
   De igual forma obtemos o resto de subgrupos de orde 3: $\{1, (1,2)(2,4), (2,4)(1,2)\}$, $\{1, (2,3)(2,4), (2,4)(2,3)\}$ e $\{1, (1,3)(3,4), (3,4)(1,3)\}$.

4. Subgrupos de orde 4:
   Como en A_4 non hai elementos de orde 4, terá que estar formado por catro elementos de orde 2 e 1, polo tanto ten que ser da forma: $\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.
   É sinxelo comprobar que este subconxunto é subgrupo.

É claro que cada subgrupo de orde 2 está contido no subgrupo de orde 4. Polo Corolario 1.3 deducimos que non hai máis subgrupos contidos noutros, fóra das inclusións triviais.

O retículo de subgrupos será da forma da Figura 3.2. Os subgrupos de orde 2 están representados por H_1, H_2 e H_3, os subgrupos de orde 3 represéntanse por H_4, H_5 H_6 e H_7, e por último, H_8 representa o subgrupo de orde 4, como se pode comprobar ao ver o segundo diagrama que nos amosa a cardinalidade dos subgrupos e o terceiro coa estrutura dos subgrupos.

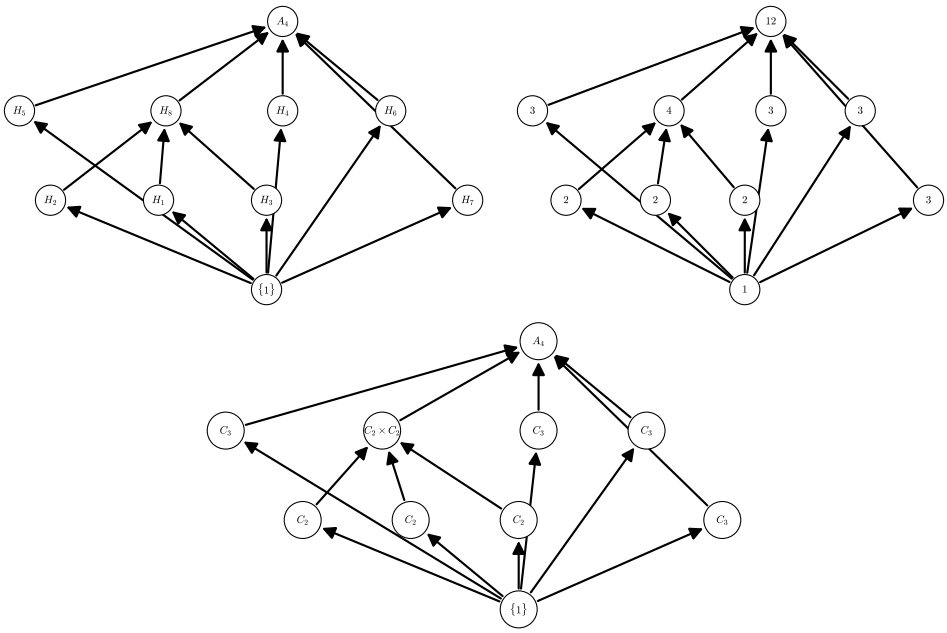


Figura 3.2: Diagrama de Hasse do retículo de subgrupos do grupo alternado A_4.

Podemos observar que ten un subretículo coa forma diamante, polo que deducimos que o retículo de subgrupos do grupo alternado A_4 non é distributivo e tamén ten un subretículo isomorfo ao pentágono polo que tampouco é modular.

Aínda que tanto neste exemplo como no anterior calculamos os subgrupos á man, temos ferramentas dixitais que facilitan este traballo. A continuación mostramos como podemos obter esta información con tan só uns comandos, empregando o programa SageMath.

Primeiro comprobamos que elementos ten o grupo, a súa orde e os subgrupos do grupo A_4.

```
A = AlternatingGroup(4)
A.list()
```

```
[(), (1,3)(2,4), (1,2)(3,4), (1,4)(2,3), (2,4,3), (1,3,4), (1,2,3),
(1,4,2), (2,3,4), (1,3,2), (1,2,4), (1,4,3)]
```

```
A.order()
```

```
12
```

```
A.subgroups()
```

```
[Subgroup generated by [()] of (Alternating group of order 4!/2 as a
permutation group),
Subgroup generated by [(1,2)(3,4)] of (Alternating group of order 4!/2
as a permutation group),
Subgroup generated by [(1,3)(2,4)] of (Alternating group of order 4!/2
as a permutation group),
Subgroup generated by [(1,4)(2,3)] of (Alternating group of order 4!/2
as a permutation group),
Subgroup generated by [(2,4,3)] of (Alternating group of order 4!/2 as
a permutation group),
Subgroup generated by [(1,2,3)] of (Alternating group of order 4!/2 as
a permutation group),
Subgroup generated by [(1,4,2)] of (Alternating group of order 4!/2 as
a permutation group),
Subgroup generated by [(1,3,4)] of (Alternating group of order 4!/2 as
a permutation group),
Subgroup generated by [(1,2)(3,4),(1,3)(2,4)] of (Alternating group of
order 4!/2 as a permutation group),
Subgroup generated by [(2,4,3), (1,2)(3,4), (1,3)(2,4)] of (Alternating
group of order 4!/2 as a permutation group)]
```

Definimos unha función para poder estudar o retículo de subgrupos. Podemos obter de forma sinxela se o retículo de subgrupos é modular ou distributivo. Vemos que, como fixemos notar antes, este retículo non é distributivo nin modular.

```
f = lambda h,k :h.is_subgroup(k)
P = LatticePoset((A.subgroups(),f))
P.is_modular()
```

```
False
```

```
P.is_distributive()
```

```
False
```

Ademáis, este programa permítenos obter o diagrama de Hasse do retículo de subgrupos co seguinte comando:

```
P.plot(label_elements=False, vertex_shape='H', vertex_size\
   =400, nvertex_color= 'white')
```

3.1.3. Grupo dos cuaternios Q_8

O grupo dos cuaternios é un grupo de orde 8 que acostuma escribirse como o conxunto $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ coa multiplicación definida de xeito que 1 é o elemento neutro e

$$i^2 = j^2 = k^2 = -1$$

$$ij = k, \quad jk = i, \quad ki = j$$

$$(-1)x = x(-1) = x$$

para $x \in \{i, j, k\}$. Estudaremos os seus subgrupos e características do retículo de subgrupos empregando SageMath.

```
Q = QuaternionGroup()
Q.order()
```

```
8
```

```
Q.list()
```

```
[(), (1,3)(2,4)(5,7)(6,8), (1,4,3,2)(5,8,7,6), (1,2,3,4)(5,6,7,8),
(1,7,3,5)(2,6,4,8),(1,5,3,7)(2,8,4,6), (1,8,3,6)(2,7,4,5),
(1,6,3,8)(2,5,4,7)]
```

Dado que SageMath considera todos os grupos como subgrupos de grupos de permutacións, a súa forma de denotar os elementos de Q_8 non coincide coa nosa. Engadindo os seguintes comandos que nos faciliten a explicación da correspondencia entra a nosa notación e a do código, identificamos cada elemento de Q_8 na seguinte orde $i, j, k, -1, -i, -j, -k$.

```
I = Q.gen(0);I
```

```
(1,2,3,4)(5,6,7,8)
```

```
J = Q.gen(1);J
```

```
(1,5,3,7)(2,8,4,6)
```

```
K = I*J;K
```

```
(1,8,3,6)(2,7,4,5)
```

```
menos_uno = I^2; menos_uno
```
```
(1,3)(2,4)(5,7)(6,8)
```

```
menos_uno*I
```
```
(1,4,3,2)(5,8,7,6)
```

```
menos_uno*J
```
```
(1,7,3,5)(2,6,4,8)
```

```
menos_uno*K
```
```
(1,6,3,8)(2,5,4,7)
```

Unha vez recoñecido que representa cada elemento no código, vexamos os subgrupos de Q_8.

```
Q.subgroups()
```
```
[Subgroup generated by [()] of (Quaternion group of order 8 as a permutation
group),
Subgroup generated by [(1,3)(2,4)(5,7)(6,8)] of (Quaternion group of order 8
as a permutation group),
Subgroup generated by [(1,3)(2,4)(5,7)(6,8),(1,5,3,7)(2,8,4,6)] of
(Quaternion group of order 8 as a permutation group),
Subgroup generated by [(1,2,3,4)(5,6,7,8),(1,3)(2,4)(5,7)(6,8)] of
(Quaternion group of order 8 as a permutation group),
Subgroup generated by [(1,3)(2,4)(5,7)(6,8),(1,6,3,8)(2,5,4,7)] of
(Quaternion group of order 8 as a permutation group),
Subgroup generated by [(1,2,3,4)(5,6,7,8),(1,3)(2,4)(5,7)(6,8),
(1,5,3,7)(2,8,4,6)] of (Quaternion group of order 8 as a permutation
group)]
```

A continuación amósase un resumo dos subgrupos de Q_8 agrupados segundo a súa orde para maior facilidade de lectura:

1. Os subgrupos obvios son $\{1\}$ e Q_8 onde $|\{1\}| = 1$ e $|Q_8| = 8$.
2. Temos un subgrupo de orde 2 que é $\langle -1 \rangle = \{1, -1\}$.
3. Os subgrupos de orde 4 son: $\langle i \rangle = \{1, -1, i, -i\}$, $\langle j \rangle = \{1, -1, j, -j\}$, $\langle k \rangle = \{1, -1, k, -k\}$.

Agora que coñecemos os subgrupos, estudaremos se o retículo de subgrupos é distributivo e modular. Vemos que, en particular, non é distributivo pero si é modular.

```
f = lambda h,k :h.is_subgroup(k)
P = LatticePoset((Q.subgroups(),f))
P.is_modular()
```

```
True
```

```
P.is_distributive()
```

```
False
```

O retículo de subgrupos do grupo de Q_8 é o representado na Figura 3.3. Represéntase por H_1 o subgrupo $\langle -1 \rangle$ e por H_2, H_3 e H_4 os subgrupos $\langle i \rangle$, $\langle j \rangle$ e $\langle k \rangle$. De igual xeito que nos exemplos anteriores, o primeiro diagrama correspóndese cos subgrupos de Q_8, o segundo coa cardinalidade dos subgrupos e o terceiro coa estrutura dos subgrupos.

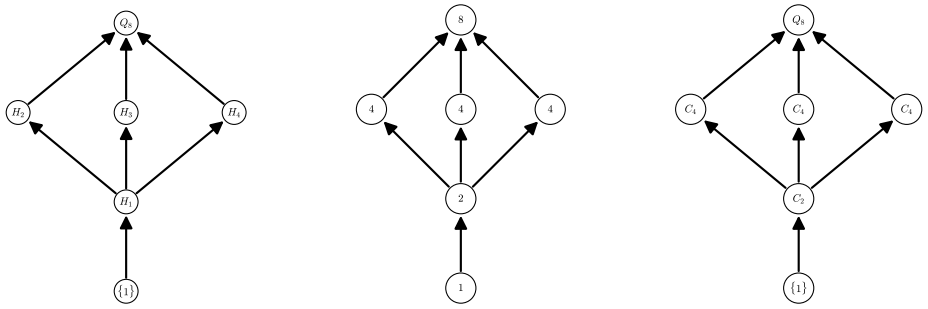


Figura 3.3: Retículo de subgrupos do grupo dos cuaternios Q_8.

3.2. Teoría de retículos de subgrupos

Como comentamos na introdución, a importancia dos retículos de subgrupos vén dada polo seguinte teorema, coñecido dende 1946 e que xustifica plenamente o estudo dos retículos de subgrupos.

Teorema 3.1 (Teorema de Whitman [12])**.** *Todo retículo é isomorfo a un subretículo dun retículo de subgrupos.*

En particular, é claro que todo retículo finito será isomorfo a un subretículo (finito) dun retículo de subgrupos. Parece razoable limitar a busca deste subretículo aos retículos de subgrupos de grupos finitos, especialmente tendo en conta o seguinte lema.

Lema 3.2. *Un grupo G é finito se, e só se, o seu retículo de subgrupos é finito.*

Demostración. Se G é finito, entón G ten un número finito de subgrupos, polo que $L(G)$ é finito. Pola contra, supoñamos que $L(G)$ é finito. Entón G só ten un número finito de

subgrupos cíclicos. En particular, todos son cíclicos finitos xa que os cíclicos infinitos teñen infinitos subgrupos. Podemos expresar G como unión dos seus subgrupos cíclicos. Así, G é unión finita de subgrupos finitos, polo que é finito. □

Neste caso, a intuición non nos engana, xa que Pudlák e Tuma probaron a seguinte adaptación do Teorema 3.1 ao caso finito. A proba data de 1980, máis de trinta anos despois do resultado de Whitman, o que dá idea da dificultade de formalizar a intuición.

Teorema 3.3 (Teorema de Pudlák e Tuma [7])**.** *Todo retículo finito é isomorfo a un subretículo dun retículo de subgrupos dalgún grupo finito.*

Notemos que, nos teoremas anteriores, é fundamental considerar subretículos xa que non todos os retículos poden verse como retículos de subgrupos. Unha proba diso verémola na seguinte proposición.

Proposición 3.4. *Non hai ningún grupo G que teña como retículo de subgrupos ao pentágono N_5.*

Demostración. Sexa G un grupo e supoñamos que N_5 é o seu retículo de subgrupos. O grupo G é finito polo Lema 3.2. Denotaremos os subgrupos de G como se amosa na Figura 3.4.

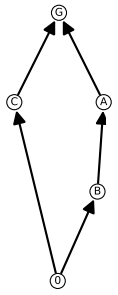


Figura 3.4: Retículo de subgrupos dun grupo G isomorfo ao pentágono N_5.

Vexamos que C é normal. Se C tivera algún conxugado, este debería ser maximal e minimal, posto que C é maximal e minimal. Pero non hai máis subgrupos maximais e minimais, polo que C coincide cos seus conxugados. Así, C é normal. Pola Proposición 1.19, como C é normal sabemos que é permutable, e por ser permutable, $AC = CA$ e $BC = CB$, polo que a Proposición 1.5 dinos que AC é subgrupo e $AC = A \vee C = G$. Analogamente, BC é subgrupo e $BC = G$.

Lembremos, pola Proposición 1.6, que $|AC| = |A||C|/|A \cap C|$, pero como $A \cap C = \{1\}$, $|AC| = |A||C|$. Analogamente para BC. Entón, $G = AC = BC$, polo que $|G| = |A||C| =$

$|B||C|$, do que deducimos que $|A| = |B|$. Chegamos a unha contradición porque B está contido en A e de ter o mesmo cardinal deberían ser iguais, pero non o son. □

Unha vez probado o resultado anterior, sabemos que non sempre un retículo xorde como un retículo de subgrupos dalgún grupo. Entón, aínda que é certo que existe un retículo que é isomorfo a $L(G)$ para todo grupo G, o propio $L(G)$, o recíproco non é certo para todo retículo. Deste xeito, afondamos na cuestión de que a correspondencia $\mathcal{L}$ presentada na introdución non é sobrexectiva.

Centrarémonos agora nos isomorfismos entre retículos de subgrupos. Presentaremos en primeiro lugar un isomorfismo de retículos que non puidemos presentar na sección 2.2 por non ter introducida a definición de retículo de subgrupos dun grupo. Outra interpretación do teorema de Correspondencia (véxase Teorema 1.8) na linguaxe de retículos é a seguinte.

Proposición 3.5 ([8])**.** *Sexan G un grupo, N un subgrupo normal de G e $\pi\colon G \longrightarrow G/N$ a proxección natural. Sexa $[N, G]$ o intervalo do retículo $L(G)$, é dicir, o subretículo de todos os subgrupos de G que conteñen a N. A aplicación $\overline{\pi}\colon [N, G] \longrightarrow L(G/N)$ definida como $\overline{\pi}(H) = H/N$ é un isomorfismo, isto é, π é unha bixección para a cal $H \subseteq K$ equivale a que $H/N \subseteq K/N$ para todo $H, K \in [N, G]$. En particular, todo subgrupo de G/N é da forma H/N para un único $H \in [N, G]$.*

Unha das cuestións máis interesantes no que respecta aos isomorfismos entre retículos de subgrupos é a súa relación cos isomorfismos entre os respectivos grupos. Os grupos isomorfos teñen retículos de subgrupos isomorfos, pois os isomorfismos de grupos respectan a estrutura de subgrupos. Pero a inversa non ten por que cumprirse. Algúns exemplos son os grupos C_p e C_q con p e q primos distintos (C_2 e C_3 por exemplo), ou C_n e C_m, con $n = p_1^{n_1} \cdots p_r^{n_r}$, $m = q_1^{n_1} \cdots q_r^{n_r}$ (C_6 e C_{15}, por exemplo), como veremos no capítulo 4, ou S_3 e $C_3 \times C_3$. Estes dous últimos grupos non son isomorfos, xa que as súas ordes (6 e 9, respectivamente) no coinciden, pero os seus retículos de subgrupos si que o son, como podemos ver a continuación.

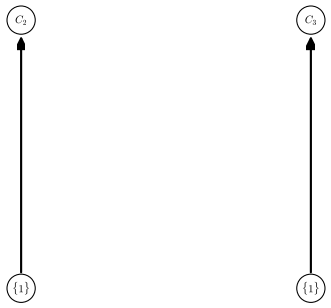


Figura 3.5: Retículos de subgrupos de C_2 e C_3.

Figura 3.6: Retículos de subgrupos de C_6 e C_{15}.

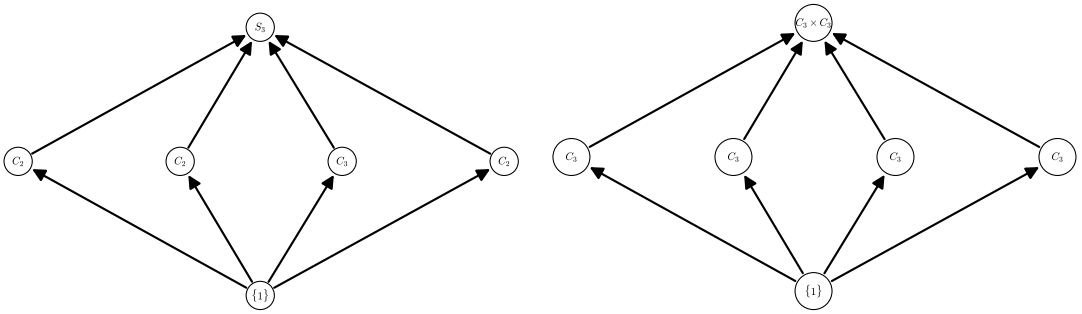


Figura 3.7: Retículos de subgrupos de S_3 e $C_3 \times C_3$.

Notemos tamén que as ordes dos subgrupos de $C_3 \times C_3$ e S_3 non coinciden: todos os subgrupos non obvios de $C_3 \times C_3$ teñen orde 3, mentres que en S_3, como xa vimos, hai tres subgrupos de orde 2 e un de orde 3. Poderíamos preguntarnos se, no caso de que as ordes dos subgrupos de dous grupos G e G' coincidisen, a existencia dun isomorfismo entre os retículos $L(G)$ e $L(G')$ implicaría que os grupos G e G' tamén fosen isomorfos. Para poder responder mellor a esta pregunta introducimos a continuación a noción de retículo de subgrupos nivelado.

3.3. Retículos de subgrupos nivelados

Pódense facer as seguintes observacións iniciais sobre a representación gráfica con niveis do retículo de subgrupos, onde para dous subgrupos tales que $K \subseteq H$, o índice $|H : K| = |H|/|K|$ recibe o nome de función do retículo nivelado

- O vértice que representa o subgrupo trivial ten o nivel 1.
- Os vértices que representan subgrupos da mesma orde n debúxanse á mesma altura. Dise que están ao mesmo nivel n. O comportamento por defecto é colocar un vértice

sobre outro se a orde do subgrupo representado polo primeiro vértice é maior que a orde do subgrupo do segundo.

Unha boa referencia para estudar os retículos de subgrupos nivelados é [3].

Exemplo 3.6.

- A representación do retículo de subgrupos do grupo $C_2 \times C_2$, tamén coñecido como grupo de Klein, mantén todos os subgrupos distintos dos obvios no mesmo nivel xa que todos teñen o mesmo cardinal, 2.

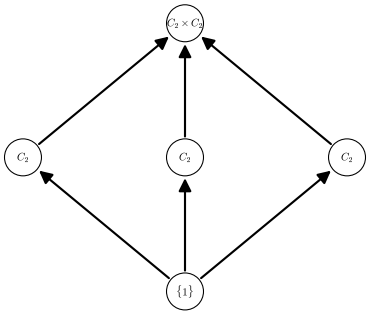


Figura 3.8: Retículo de subgrupos de $C_2 \times C_2$.

- No diagrama do retículo de subgrupos do grupo $C_2 \times C_8$ apréciase a colocación a distintos niveis dos subgrupos de distinta orde.

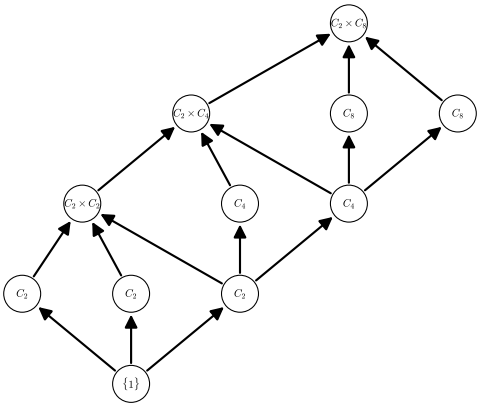


Figura 3.9: Retículo de subgrupos de $C_2 \times C_8$.

Un isomorfismo f de retículos nivelados é un isomorfismo de retículos que conserva a función de nivel, é dicir, para dous vértices $K \subset H$, tense que $|f(H) : f(K)| = |H : K|$.

Exemplo 3.7. Consideremos o produto semi-directo $C_8 \rtimes_\phi C_2$, $\phi\colon C_2 \cong S_2 \to \mathrm{Aut}(C_8)$ onde $\phi(1) = 1$ e $\phi(1,2)$ é o automorfismo de C_8 que leva un xerador de C_8, g, a g^5, por exemplo, $(1,2,3,4,5,6,7,8) \mapsto (1,6,3,8,5,2,7,4)$, vendo C_8 como un grupo de permutacións. É sinxelo ver que $C_8 \times C_2$ e $C_8 \rtimes_\phi C_2$ no son isomorfos, xa que $C_8 \times C_2$ é abeliano e $C_8 \rtimes_\phi C_2$ non o é, de feito son dous dos catorce grupos non isomorfos que hai de orde 16. Con todo, os seus retículos nivelados son isomorfos e as ordes e os tipos de subgrupos que se corresponden no mesmo nivel son isomorfos.

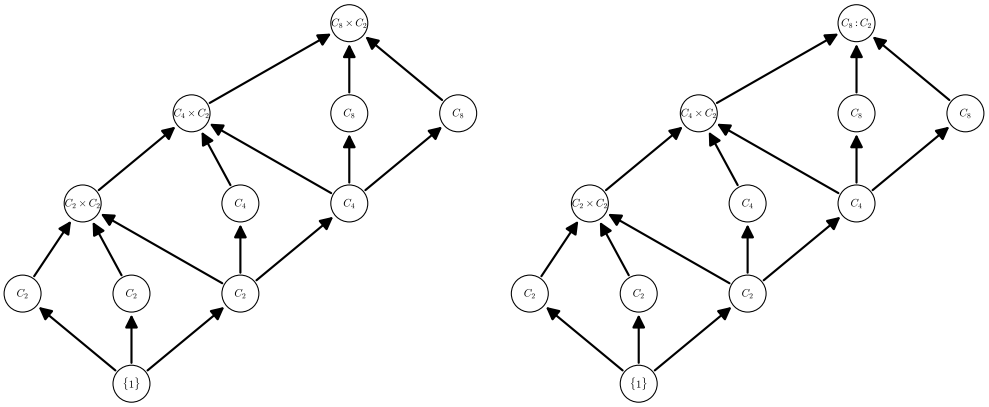


Figura 3.10: Retículos de subgrupos de $C_8 \times C_2$ e $C_8 \rtimes_\phi C_2$.

Estes exemplos fannos preguntarnos se existen grupos que están caracterizados polo seu retículo de subgrupos, é dicir, se $L(G) \simeq L(G')$ implica que $G \simeq G'$. Na introdución anticipabamos que si, pero para responder a esta pregunta con fundamentos teremos que agardar aos capítulos seguintes.

Capítulo 4

Retículos de subgrupos distributivos e grupos cíclicos

Centrarémonos agora nos retículos de subgrupos distributivos, que como veremos gardan gran relación cos grupos cíclicos. Aínda que o traballo céntrase principalmente en retículos de subgrupos de grupos finitos, neste capítulo faremos incursión no mundo dos grupos infinitos para despois particularizar os resultados obtidos ao caso finito.

Comezaremos preguntándonos quen son os retículos de subgrupos nos grupos cíclicos. Lembremos que no primeiro capítulo definimos os grupos cíclicos C_n, para $n \in \mathbb{N} \cup \{\infty\}$. Imos ver algúns exemplos de retículos de subgrupos de grupos cíclicos.

Exemplo 4.1.

- Unha aplicación directa do Corolario 1.3 (do teorema de Lagrange) fainos ver que o grupo cíclico de orde 3, $C_3 = \langle a \rangle = \{1, a, a^2\}$ non ten máis subgrupos que os obvios $\{1\}$ e C_3. Como é obvio o seu retículo de subgrupos é unha cadea de dous elementos.

- O grupo cíclico $C_4 = \{1, a, a^2, a^3\}$ ten orde 4, polo que aplicando de novo o Corolario 1.3 podemos afirmar que pode ter subgrupos de orde 1, 2 e 4. O subgrupo de orde 1 será $\{1\}$, o único de orde 2 é $\langle a^2 \rangle$ e o de orde 4 é o propio conxunto C_4. O seu retículo de subgrupos é unha cadea.

- O mesmo razoamento que usamos para C_3 dinos que o retículo de subgrupos de C_5 tamén é unha cadea de dous elementos, $\{1\}$ e C_5. En xeral, isto ocorre para calquera C_p con p primo.

- O grupo cíclico $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$, a diferencia dos dous anteriores, non ten por retículo de subgrupos unha cadea, como podemos ver a continuación. Ten dous

subgrupos ademais dos obvios, $\{1\}$ e C_6, que son $\langle a^2\rangle$ e $\langle a^3\rangle$. Ademais, $a^2 \notin \langle a^3\rangle$ e $a^3 \notin \langle a^2\rangle$, co que ningún dos dous subgrupos está contido no outro.

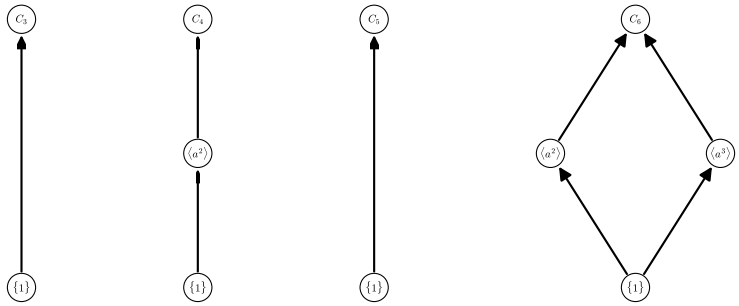


Figura 4.1: Diagramas de Hasse dos retículos de subgrupos de C_3 C_4, C_5 e C_6.

Como comentabamos no capítulo 3, C_3 e C_5 teñen o mesmo retículo de subgrupos, aínda que non son grupos isomorfos.

Lema 4.2. *Se $n \in \mathbb{N}\cup\{\infty\}$, entón o retículo de subgrupos de C_n, $L(C_n)$, é isomorfo a T_n.*

Demostración. Sexa $n \in \mathbb{N} \cup \{\infty\}$. Logo, $C_n = \langle g\rangle$ para un certo elemento g de orde n. Polo Teorema 1.1, a aplicación $\sigma\colon T_n \longrightarrow L(\langle g\rangle)$ definida como $\sigma(r) = \langle g^r\rangle$ para todo $r \in T_n$ é bixectiva. Ademais, para $r, s \in T_n$, temos que $s \mid r$ se, e só se, $\langle g^r\rangle \subseteq \langle g^s\rangle$. Así que σ é un isomorfismo de retículos. □

4.1. Cadeas

Esta sección tratará sobre os grupos que teñen por retículo de subgrupos cadeas. Daremos unha caracterización das cadeas que nos relaciona o concepto de cadea e grupo cíclico. Basearémonos na información do artigo [5] que estuda os grupos que teñen por retículo de subgrupos unha, dúas e máis cadeas, aínda que nós centrarémonos no primeiro caso.

Lema 4.3. *Se G é un grupo finito e o seu retículo de subgrupos é unha cadea, entón G é cíclico.*

Demostración. Consideremos un grupo G finito que non sexa cíclico. Queremos ver que o retículo de subgrupos de G non é unha cadea. Consideremos un elemento $x \in G$ de xeito que $|x| = \max\{|g| \mid g \in G\}$, que existe xa que G é finito. Entón $\langle x\rangle$ é un subgrupo de G de orde $|x|$. Por ser G non cíclico, en particular tense que $G \neq \langle x\rangle$ e existe $y \in G$ tal que y non pertence a $\langle x\rangle$. Logo $\langle y\rangle$ non está contido en $\langle x\rangle$. Supoñamos agora que $\langle x\rangle$ está contido en $\langle y\rangle$. Entón $|y| > |x|$, en contradición coa elección de $|x|$. Así, $\langle x\rangle$ non é un subgrupo de $\langle y\rangle$. Polo tanto, o retículo de subgrupos de G non é unha cadea. □

Proposición 4.4. *Se o retículo de subgrupos de C_n é unha cadea, entón n é potencia dun número primo.*

Demostración. Supoñamos que o retículo de subgrupos de C_n é unha cadea e que n non é potencia dun número primo. Entón $n = kp^a$ e $n = mq^b$ para primos p e q e enteiros positivos a, b, k, m de xeito que p non divide a k e q non divide a m.

Sexa $x \in C_n$ tal que $C_n = \langle x \rangle$. Entón as ordes dos subgrupos $\langle x^k \rangle$ e $\langle x^m \rangle$ de C_n son potencias de p e q respectivamente. Séguese do Corolario 1.3 que ningún destes subgrupos está contido no outro, en contradición con que o retículo de subgrupos de C_n é unha cadea. Polo tanto, n é potencia dun número primo. □

Lema 4.5. *Se p é primo, entón o retículo de subgrupos de C_{p^n} é unha cadea.*

Demostración. A demostración é inmediata a partir do Lema 4.2 xa que o retículo de subgrupos de C_{p^n} será isomorfo a T_{p^n}, polo que será unha cadea. □

O Lema 4.3 xunto coa Proposición 4.4 proban a condición necesaria do seguinte teorema e o Lema 4.5 proba a condición suficiente.

Teorema 4.6. *Un grupo finito ten un retículo de subgrupos que é unha cadea se, e só se, é isomorfo a C_{p^n}, para un primo p e un natural n.*

4.2. Grupos localmente cíclicos e cíclicos

Como anticipabamos ao comezo do capítulo, imos presentar a continuación un resultado encadrado no mundo dos retículos de subgrupos de orde arbitraria (finita ou infinita), que quizais sexa o máis importante do capítulo. Un estudo detallado centrado neste teorema pode atoparse no traballo [11].

Teorema 4.7 (Teorema de Ore)**.** *O retículo de subgrupos dun grupo G é distributivo se, e só se, G é localmente cíclico.*

Demostración. Supoñamos en primeiro lugar que o retículo de subgrupos de G, $L(G)$, é distributivo e sexan $a, b \in G$. Queremos demostrar que o subgrupo xerado por a e b, $\langle a, b \rangle$, é cíclico. Veremos que $\langle a, b \rangle = \langle ab \rangle \vee \langle a \rangle$. É claro que $\langle ab \rangle \subseteq \langle a, b \rangle$ e $\langle a \rangle \subseteq \langle a, b \rangle$, polo que $\langle ab \rangle \vee \langle a \rangle \subseteq \langle a, b \rangle$. Para ver o outro contido, é suficiente ver que os xeradores de $\langle a, b \rangle$ pertencen a $\langle ab \rangle \vee \langle a \rangle$. Como a e ab pertencen a $\langle ab \rangle \vee \langle a \rangle$, $a^{-1}ab = b \in \langle ab \rangle \vee \langle a \rangle$ tamén. Polo tanto $\langle a, b \rangle \subseteq \langle ab \rangle \vee \langle a \rangle$, e así $\langle ab \rangle \vee \langle a \rangle = \langle a, b \rangle$. Analogamente, próbase que $\langle a, b \rangle = \langle ab \rangle \vee \langle b \rangle$.

Agora ben, como $L(G)$ é distributivo,

$$\langle ab\rangle \vee (\langle a\rangle \wedge \langle b\rangle) = (\langle ab\rangle \vee \langle a\rangle) \wedge (\langle ab\rangle \vee \langle b\rangle).$$

Pero como $\langle ab\rangle \vee \langle a\rangle = \langle a, b\rangle = \langle ab\rangle \vee \langle b\rangle$, temos que $\langle ab\rangle \vee (\langle a\rangle \wedge \langle b\rangle) = \langle a, b\rangle$. Nótese que a e b conmutan con todos os elementos de $\langle a\rangle \wedge \langle b\rangle$. Polo tanto $\langle a\rangle \wedge \langle b\rangle \subseteq Z(\langle a, b\rangle)$. Así, pola Proposición 1.12, $\langle a\rangle \wedge \langle b\rangle \trianglelefteq \langle a, b\rangle$, e polo Teorema 1.7,

$$\langle a, b\rangle/(\langle a\rangle \wedge \langle b\rangle) \simeq \langle ab\rangle/\langle ab\rangle \wedge (\langle a\rangle \wedge \langle b\rangle).$$

Nótese que $\langle a, b\rangle/(\langle a\rangle \wedge \langle b\rangle)$ é cíclico xa que o cociente dun grupo cíclico é cíclico, o que implica que $\langle a, b\rangle$ é abeliano, polo Teorema 1.12. Pola estrutura de grupos finitos abelianos finitamente xerados, existen $c, d \in G$ tales que $\langle a, b\rangle = \langle c\rangle \times \langle d\rangle$, un produto directo de grupos cíclicos. En particular, $\langle c\rangle \wedge \langle d\rangle = 1$. Repetindo o argumento anterior, tense que $\langle c, d\rangle/(\langle c\rangle \wedge \langle d\rangle) = \langle c, d\rangle$ é cíclico. Pero $\langle a, b\rangle = \langle c\rangle \times \langle d\rangle = \langle c, d\rangle$, e así $\langle a, b\rangle$ é cíclico, polo que G é localmente cíclico.

Supoñamos agora que G é localmente cíclico e sexan $A, B, C \in L(G)$. Como vimos coa definición de retículo distributivo, para ver que $L(G)$ é distributivo é suficiente con probar a primeira lei distributiva, e neste caso, xa que G é abeliano, pola Proposición 1.5, bastará ver que $A(B \cap C) = AB \cap AC$. Claramente, $A(B \cap C) \subseteq AB \cap AC$. Sexa $x \in AB \cap AC$. Entón $x = ab$ e $x = a'c$ para algúns $a, a' \in A$, $b \in B$ e $c \in C$. Por ser G localmente cíclico, $\langle a, a', b, c\rangle = \langle g\rangle$ para algún $g \in G$. Sexa $A' = A \cap \langle g\rangle$, $B' = B \cap \langle g\rangle$ e $C' = C \cap \langle g\rangle$. Se A' é trivial, $a = 1 = a'$ e $b = x = c$, co que $x \in A(B \cap C)$. Se B' ou C' é trivial, $x = a$ ou $x = a'$, e $x \in A(B \cap C)$. Polo tanto, asumiremos que ningún deles é trivial. Vexamos que $\langle g\rangle = A'B' = A'C'$.

É claro que $A'B' \subseteq \langle g\rangle$ e que $A'C' \subseteq \langle g\rangle$. Para ver que $\langle g\rangle \subseteq A'B'$, só é necesario probar que os xeradores a, a', b e c de $\langle g\rangle$ están en $A'B'$. Nótese que $a, a', b \in A'B'$. Dado que $a'c = ab$, tamén $c = a'^{-1}ab \in A'B'$, e así $\langle g\rangle \subseteq A'B'$. Analogamente, $\langle g\rangle \subseteq A'C'$.

Sexan agora, $\alpha, \alpha', \beta, \gamma \in \mathbb{Z}$ tales que $a = g^\alpha$, $a' = g^{\alpha'}$, $b = g^\beta$ e $c = g^\gamma$. Como $A'B' = \langle g\rangle$ podemos atopar enteiros i e j tales que $g = g^i g^j = g^{i+j}$ con $g^i \in A'$ e $g^j \in B'$, e polo tanto $g^\gamma = g^{(i+j)\gamma}$. Agora, $x = a'c = g^{\alpha'}g^{(i+j)\gamma} = g^{\alpha'}g^{i\gamma}g^{j\gamma}$. Como $g^{\alpha'}g^{i\gamma} \in A'$ e $g^{j\gamma} \in B' \cap C'$, tense que $x \in A'(B' \cap C') \subseteq A(B \cap C)$. Polo tanto, $A(B \cap C) = AB \cap AC$, e así $L(G)$ é distributivo. □

O seguinte resultado séguese inmediatamente do teorema de Ore e da Definición 1.16.

Corolario 4.8. *O retículo de subgrupos dun grupo finito G é distributivo se, e só se, G é cíclico.*

Demostración. Dado que todo grupo cíclico é localmente cíclico, se G é cíclico teremos que G é distributivo polo Teorema 4.7. Reciprocamente, supoñamos que G é distributivo. Entón G é localmente cíclico polo Teorema 4.7. Pero como toda cantidade finita de elementos xera un subgrupo cíclico pola Definición 1.16 e xa que o propio G é un grupo finito, G debe ser cíclico. □

Deste xeito, probamos que as afirmacións (B) e (C) da introdución son equivalentes, como prometíamos daquela. A equivalencia con (A) vén dada polo Lema 4.2 e o Exemplo 2.20.

Ademais, tanto o teorema de Ore como o seu corolario dan exemplos de clases de grupos nas condicións da pregunta 3 da introdución: os grupos localmente cíclicos e os grupos cíclicos finitos admiten as caracterizacións reticulares de ter un retículo de subgrupos distributivo ou finito e distributivo, respectivamente. Veremos a continuación que empregando o anterior Teorema 4.7 tamén é sinxelo caracterizar a clase dos grupos cíclicos.

Lema 4.9. *Un grupo G cun retículo de subgrupos que satisfai a condición maximal é finitamente xerado.*

Demostración. Sexa $\{a_1, a_2, \dots\}$ un conxunto de xeradores de G. Entón, como $L(G)$ satisfai a condición maximal, a sucesión ascendente de subgrupos $\langle a_1\rangle \subseteq \langle a_1, a_2\rangle \subseteq \dots$ debe estabilizarse nalgún paso, chamémoslle n. Así, $a_{n+j} \in \langle a_1, \dots, a_n\rangle$ para todo $j \geq 0$. pero entón $G = \langle a_1, a_2, \dots\rangle \subseteq \langle a_1, a_2, \dots, a_n\rangle$, co que G está finitamente xerado. □

Teorema 4.10. *Un grupo G é cíclico se, e só se, o seu retículo de subgrupos $L(G)$ é distributivo e satisfai a condición maximal.*

Demostración. Supoñamos en primeiro lugar que $L(G)$ é distributivo e satisfai a condición maximal. Polo Lema 4.9, G é finitamente xerado. Como $L(G)$ é distributivo, entón G é localmente cíclico, e polo Teorema 4.7, deducimos que G é cíclico. Reciprocamente, se G é cíclico, entón $L(G)$ é distributivo, polo Teorema 4.7, e só quedaría por probar que satisfai a condición maximal. Por ser G cíclico, $G = \langle g\rangle$ para algún $g \in G$. Entón, $\langle g^j\rangle \subseteq \langle g^k\rangle$ se, e só se, k é un divisor de j, polo Teorema 1.1. Como todos os subgrupos de G son cíclicos (Teorema 1.1), calquera sucesión de elementos de $L(G)$, $G_1, \dots, G_n, \dots$ con $G_1 \subseteq \cdots \subseteq G_n \subseteq \cdots$ será da forma $\langle g^{j_1}\rangle \subseteq \cdots \subseteq \langle g^{j_n}\rangle \subseteq \cdots$. Como os divisores de j_1 son finitos, dedúcese que esta sucesión non pode ser infinita. Polo tanto, $L(G)$ satisfai a condición maximal. □

Polo tanto, temos un novo exemplo de clase de grupos (os cíclicos) con caracterización reticular (retículo de subgrupos distributivo satisfacendo a condición maximal). Aproveitaremos isto para presentar un primeiro exemplo de grupo caracterizado polo seu retículo de subgrupos, comezando así a responder á cuestión 1 da introdución.

Corolario 4.11. *Sexa G un grupo. Entón $G \simeq C_\infty$ se, e só se, $L(G) \simeq T_\infty$.*

Demostración. Se $G \simeq C_\infty$, entón o retículo de subgrupos de G é isomorfo a T_∞ polo Lema 4.2. Pola contra, supoñamos que $L(G) \simeq T_\infty$. Polo Lema 4.2, $L(G) \simeq L(C_\infty)$. Polo Teorema 4.10, $L(C_\infty)$ é distributivo e satisfai a condición maximal, e polo tanto $L(G)$ tamén satisfai estas condicións. Así, aplicando de novo o Teorema 4.10, obtense que G é cíclico. Como claramente $|G|$ é infinito, tense que $G \simeq C_\infty$. □

Así, o grupo cíclico infinito C_∞ está determinado polo seu retículo de subgrupos, é o único grupo G tal que $L(G) \simeq L(C_\infty)$. Para os grupos cíclicos finitos a situación cambia xa que para dous elementos $m, m' \in \mathbb{N}$, os retículos T_m e $T_{m'}$ poden ser isomorfos aínda que m e m' sexan distintos, como ilustra o seguinte teorema.

Teorema 4.12. *Sexa $n_1, \dots, n_r \in \mathbb{N}$. O grupo G é cíclico de orde $p_1^{n_1} \cdots p_r^{n_r}$ con primos p_i distintos se, e só se, o retículo de subgrupos de G é produto directo de r cadeas de lonxitude $n_1, \dots, n_r$.*

Demostración. Se G é un grupo cíclico de orde $m = p_1^{n_1} \cdots p_r^{n_r}$, entón $L(G) \simeq T_m$ é produto directo de cadeas de lonxitude $n_1, \dots, n_r$ como comentamos no Exemplo 2.10. Reciprocamente, supoñamos que $L(G)$ é produto directo de cadeas de lonxitude $n_1, \dots, n_r$. Sexan $q_1, \dots, q_r$ primos distintos e poñamos $m' = q_1^{n_1} \cdots q_r^{n_r}$. Entón $L(G) \simeq T_{m'}$ é distributivo, como vimos no Exemplo 2.20, e finito. Polo Teorema 4.10, G é cíclico. Así, $T_{m'} \simeq L(G) \simeq T_{|G|}$ e polo conseguinte $|G| = q_1^{n_1} \cdots q_r^{n_r}$. □

Deste xeito xustificamos a nosa afirmación do capítulo 3 na que asegurabamos que C_n e C_m, con $n = p_1^{n_1} \cdots p_r^{n_r}$ e $m = q_1^{n_1} \cdots q_r^{n_r}$, tiñan retículos de subgrupos isomorfos. Exemplificabamos a afirmación cos grupos C_6 e C_{15}, vexamos agora outro exemplo.

Exemplo 4.13. Os retículos T_{12} e T_{20} teñen retículos isomorfos, como se pode ver nos diagramas. Estes retículos son exactamente o produto directo dunha cadea de lonxitude 1 con outra de lonxitude 2, xa que $12 = 2^2 3^1$ e $20 = 2^2 5^1$. Porén, os grupos C_{12} e C_{20} non son isomorfos.

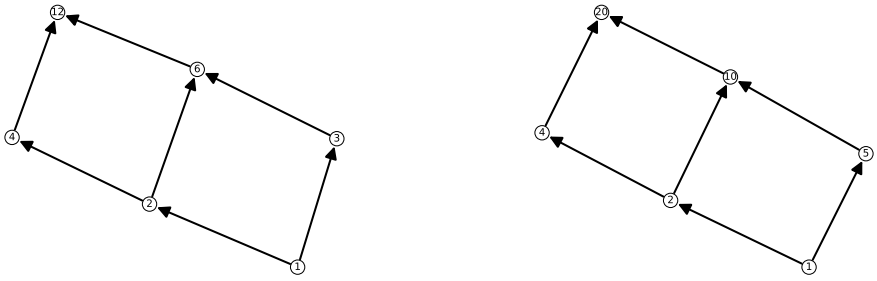
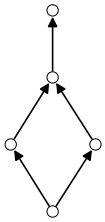
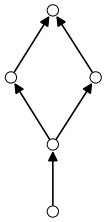


Figura 4.2: Retículos T_{12} e T_{20}.

Presentamos a continuación unha consecuencia directa do Teorema 4.12 que matiza un pouco máis o Teorema 4.6.

Corolario 4.14. *Un grupo finito ten un retículo de subgrupos que é unha cadea de lonxitude n se, e só se, é isomorfo a C_{p^n}, para un certo p primo.*

Podemos aproveitar o teorema de Ore para dar máis exemplos de retículos que non son retículos de subgrupos de ningún grupo, continuando así coa liña da Proposición 3.4. É o caso, por exemplo, de $L(G) =$  ou $L(G) =$  xa que estes retículos son distributivos, e polo teorema de Ore o seu grupo asociado tería que ser cíclico, pero xa vimos que os retículos dun grupo cíclico non son desta forma.

Por último, cabe destacar que como todo retículo booleano é distributivo, é sinxelo obter resultados sobre grupos con retículos de subgrupos booleanos a partir da información precedente sobre retículos de subgrupos distributivos. En particular, para o caso finito temos a seguinte elegante caracterización dos grupos con retículo de subgrupos booleano, cuxa demostración vén dada pola combinación do Corolario 4.8, o Teorema 4.12 e o Teorema 2.29.

Teorema 4.15. *Un grupo finito G ten retículo de subgrupos booleano se, e só se, G é cíclico de orde libre de cadrados, é dicir, $|G| = p_1 \cdots p_k$, con p_i primos diferentes.*

Capítulo 5

Retículos de subgrupos modulares

Este capítulo centrarase na clase de retículos da Definición 2.19, é dicir, nos retículos modulares. A diferencia dos grupos con retículos de subgrupos distributivos, que se correspondían cunha boa clase de grupos como son os localmente cíclicos, cos modulares non pasa o mesmo. Non obstante, veremos que hai unha certa conexión entre os retículos de subgrupos modulares e os grupos abelianos. No libro [9] podemos atopar gran variedade de resultados sobre retículos modulares, moitos dos cales están fóra do alcance deste traballo. Amosamos os máis interesantes dentro dos alcanzables ao longo deste capítulo.

Definición 5.1. Diremos que un elemento m dun retículo P é **modular** en P se

$$x \vee (m \wedge z) = (x \vee m) \wedge z \quad \text{para todo } x, z \in P \text{ con } x \leq z, \tag{5.1}$$

e

$$m \vee (y \wedge z) = (m \vee y) \wedge z \quad \text{para todo } y, z \in P \quad \text{con } m \leq z. \tag{5.2}$$

Un subgrupo M dun grupo G chámase **modular** en G se M é modular no retículo de subgrupos de G.

É inmediato ver que un retículo P é modular se e só se todo elemento de P é modular en P.

Proposición 5.2. *Sexa G un grupo. Se M é permutable, entón M é modular en G.*

Demostración. Se M é permutable, $MH = HM$ para todo subgrupo H de G, e pola Proposición 1.5 tense que $M \vee H = MH$ para todo H subgrupo de G.

Consideremos $X \leq Z \leq G$. Entón, como apuntamos despois da Definición 2.19, tense que $X \vee (M \wedge Z) \leq (X \vee M) \wedge Z$. Ademais, se $g \in (XM) \wedge Z$, entón, como $X \vee M = XM$, existen $x \in X$ e $m \in M$ tales que $g = xm$, e ademais $g \in Z$. Dado que $X \leq Z$, temos que

$m = x^{-1}g \in Z$ e polo tanto $g = xm \in X \vee (M \wedge Z)$. Así, $X \vee (M \wedge Z) = (X \vee M) \wedge Z$ e cúmprese a igualdade (5.1). Sexan agora $Y, Z \leq G$ con $M \leq Z$. Entón, $M \vee (Y \wedge Z) \leq (M \vee Y) \wedge Z$ e tomando $g = my \in (M \vee Y) \wedge Z$ con $m \in M \leq Z$, séguese coma antes que $y \in Z$. Polo tanto, $g \in M \vee (Y \wedge Z)$, cumprindo a igualdade (5.2), co que temos que M é modular en G. □

A Proposición 1.19 amósanos que un subgrupo normal é permutable e a Proposición 5.2 que un subgrupo permutable é modular en G. Polo tanto un subgrupo normal é modular en G e as leis modulares (5.1) e (5.2) son as principais propiedades dun subgrupo normal que se poden ver no retículo de subgrupos.

Teorema 5.3. *O retículo de subgrupos normais dun grupo arbitrario e o retículo de subgrupos dun grupo abeliano son modulares.*

Demostración. Polas Proposicións 1.19 e 5.2, todo subgrupo normal dun grupo G é modular no retículo de subgrupos de G, $L(G)$, e polo tanto tamén no retículo dos subgrupos normais de G, $\mathfrak{N}(G)$, xa que este é un subretículo de $L(G)$. Así, $\mathfrak{N}(G)$ é modular. Se G é abeliano, entón $L(G) = \mathfrak{N}(G)$. □

Corolario 5.4. *Os retículos de subgrupos dos grupos hamiltonianos son modulares.*

A continuación veremos unha caracterización de retículos modulares baseándonos no seguinte resultado sobre elementos modulares de retículos arbitrarios.

Proposición 5.5. *Sexa m un elemento dun retículo P. Se m é modular en P, entón os intervalos $[m, a \vee m]$ e $[a \wedge m, a]$ son isomorfos para todo $a \in P$.*

Demostración. Sexa $a \in P$ e consideremos as aplicacións $\varphi_{a,m}\colon\ [a \wedge m, a] \longrightarrow [m, a \vee m]$ definida por $\varphi_{a,m}(x) = x \vee m$ e $\psi_{a,m}\colon\ [m, a \vee m] \longrightarrow [a \wedge m, a]$ definida por $\psi_{a,m}(z) = z \wedge a$. Se $x \in [a \wedge m, a]$, entón por (5.1),

$$\psi_{a,m}\varphi_{a,m}(x) = (x \vee m) \wedge a = x \vee (m \wedge a) = x$$

e se $z \in [m, a \vee m]$, entón por (5.2),

$$\varphi_{a,m}\psi_{a,m}(x) = (z \wedge a) \vee m = z \wedge (a \vee m) = z.$$

Así, $\varphi_{a,m}\psi_{a,m} = \mathrm{Id}_{[a \wedge m, a]}$ e $\psi_{a,m}\varphi_{a,m} = \mathrm{Id}_{[m, a \vee m]}$. Polo que é inmediato que $[a \wedge m, a] \simeq [m, a \vee m]$ para todo $a \in P$. □

Teorema 5.6. *Un p-grupo finito ten un retículo de subgrupos modular se, e só se, todo par de subgrupos conmutan.*

Demostración. Sexa G un p-grupo finito e supoñamos que todo par de subgrupos de G conmutan. Polo Teorema 5.2, todo elemento do retículo de subgrupos $L(G)$ é modular, o que implica que $L(G)$ é modular.

Supoñamos agora que $L(G)$ é modular. Entón, todo elemento é modular. Pola Proposición 5.5, para todo par de subgrupos H, K de G, temos que os intervalos de $L(G)$, $[H, H \vee K]$ e $[H \wedge K, K]$ son isomorfos. En particular, teñen a mesma lonxitude n. Como H e $H \vee K$ son subgrupos de G, temos que $|H| = p^s$ e $|H \vee K| = p^t$. Combinando a lonxitude do intervalo $[H, H \vee K]$ coa Proposición 1.10, deducimos que $t = s + n$, polo que $|H \vee K : H| = \dfrac{|H \vee K|}{|H|} = \frac{p^t}{p^s} = \frac{p^{s+n}}{p^s} = p^n$. Analogamente, $|K : H \wedge K| = p^n$.

Deducimos que $|H \vee K| = \frac{|H||K|}{|H \wedge K|} = |HK| < \infty$, e como $HK \subseteq H \vee K$, temos que $HK = H \vee K$. Polo Teorema 1.5 obtemos que $HK = KH$ para todo H, K subgrupo de G. □

Para rematar o capítulo, amosaremos un teorema sen proba que caracteriza os retículos de subgrupos modulares.

Teorema 5.7 (Teorema de Iwasawa [4])**.** *Un p-grupo finito G ten un retículo de subgrupos modular se, e só se, se dá unha das condicións seguintes:*

1. *G é produto directo do grupo de cuaternios Q_8 cun 2-grupo abeliano elemental.*
2. *G contén un subgrupo normal abeliano A de xeito que G/A é cíclico; ademais existe un elemento $b \in G$ con $G = A\langle b \rangle$ e un enteiro positivo s tal que $b^{-1}ab = a^{1+p^s}$ para todo $a \in A$, con $s \geq 2$ no caso no que $p = 2$.*

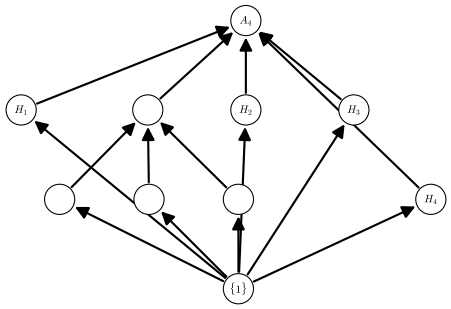
Capítulo 6

Grupos caracterizados polo seu retículo de subgrupos

Neste capítulo recuperaremos unha cuestión que comentamos no capítulo 3 e non puidemos abarcar daquela: se existían grupos caracterizados polo seu retículo de subgrupos. Agora podemos afirmar que a resposta a esta pregunta é afirmativa. Xa vimos o exemplo de $\mathbb{Z} \simeq C_\infty$ no Corolario 4.11, pero hai moitos máis, entre os que cabe destacar a $C_2 \times C_2$, Q_8, A_4 ou os grupos libres de rango ≥ 2. Deste xeito, damos unha resposta á primeira pregunta da introdución.

Os casos de Q_8 e dos grupos libres escápanse completamente do alcance do traballo. A pesar diso, pódense consultar nas referencias [10] e [9] respectivamente. O nivel de complexidade dos casos $C_2 \times C_2$ e de A_4 é similar e adecúase máis ao traballo. Decidimos desenvolver coidadosamente o caso A_4 porque nos dá a oportunidade de empregar resultados probados nos capítulos anteriores, resaltando así a súa aplicabilidade.

Supoñamos que existe un grupo G que ten o mesmo retículo de subgrupos que A_4, isto é, $L(A_4) \simeq L(G)$. Como xa estudamos o retículo de subgrupos de A_4 na subsección 3.1.2, sabemos que $L(A_4)$ é da seguinte forma:



Consideremos os subgrupos H_1, H_2, H_3, H_4 que son maximais e minimais, e denotemos $\Gamma = \{H_1, H_2, H_3, H_4\}$. Definimos a aplicación $\varphi\colon G \longrightarrow S_4$ que a cada elemento $g \in G$, faille corresponder unha permutación $\varphi_g\colon \Gamma \longrightarrow \Gamma$ definida como $\varphi_g(H_i) = gH_ig^{-1}$. É inmediato comprobar que $\varphi_g \in S_4$, xa que os conxugados dos subgrupos maximais seguen sendo maximais e os conxugados dos subgrupos minimais seguen sendo minimais. Imos probar que φ é un homomorfismo de grupos inxectivo. É trivial comprobar que $\varphi_{g_1g_2}(H_i)$ é igual a $\varphi_{g_1}(\varphi_{g_2}(H_i))$ para todo $H_i \in \Gamma$, polo que φ é homomorfismo de grupos. En canto á inxectividade, veremos que $\mathrm{Ker}(\varphi) = \{1\}$. Sexa $g \in \mathrm{Ker}(\varphi)$. Entón, $\varphi_g = \mathrm{Id}_\Gamma$, polo que $\varphi_g(H_i) = H_i$ para todo $i = 1, \dots, 4$; noutras palabras, $gH_ig^{-1} = H_i$ para todo $i = 1, \dots, 4$. Lembrando a Definición 1.13, temos que $g \in N_G(H_i)$ para todo $H_i \in \Gamma$, polo que $g \in \bigcap_{i=1}^4 N_G(H_i)$. Dado que $H_i \subseteq N_G(H_i)$, vendo o diagrama, chegamos á conclusión de que $N_G(H_i)$ é H_i ou G. Temos dúas opcións mutuamente exclusivas:

1. Existen tres subgrupos $H_j, H_k, H_l \in \Gamma$, $j \neq k$, $j \neq l$, $r \neq l$, con $N_G(H_j) = G$, $N_G(H_k) = G$ e $N_G(H_l) = G$.

2. Existen $H_j, H_k \in \Gamma$, con $j \neq k$, tales que $N_G(H_j) = H_j$ e $N_G(H_k) = H_k$.

Comezaremos coa primeira opción. Se $N_G(H_j) = G$, entón $H_j \trianglelefteq G$, polo que G/H_j é grupo. Polo teorema de correspondencia (véxase Teorema 1.8), os subgrupos de G/H_j correspóndense cos subgrupos de G que conteñen a H_j. Vendo o retículo, os grupos de G que conteñen a H_j son G e H_j, que se corresponden en G/H_j con G/H_j e $\{1\}$. Por iso o retículo de subgrupos é unha cadea (de dous elementos), e polo Teorema 4.6 ou o Corolario 4.14, G/H_j é cíclico e polo tanto abeliano. Pola Proposición 1.15, $[G, G] \subseteq H_j$. Analogamente, $[G, G] \subseteq H_k$. Como $H_j \cap H_k = \{1\}$, a única opción é que $[G, G] = \{1\}$ o que equivale a que G é abeliano. Pero polo Teorema 5.3, isto implica que $L(G)$ é modular, e a súa vez que $L(A_4)$ é modular. Pero como xa dixemos na sección 3.1.2, $L(A_4)$ non é modular. Polo tanto, desbotamos a primeira opción. Terá que cumprirse a segunda opción. Temos que $\bigcap_{i=1}^4 N_G(H_i) \subseteq H_j \cup H_k = \{1\}$, polo que $\bigcap_{i=1}^4 N_G(H_i) = \{1\}$ e así, $g = 1$. Polo tanto, $\mathrm{Ker}(\varphi) = \{1\}$ o que equivale a que φ é inxectivo. Entón, G será isomorfo a un subgrupo de S_4.

Como fixemos anteriormente, utilizaremos SageMath para obter os subgrupos de S_4. No seguinte código mostramos a obtención dos subgrupos, e nas últimas liñas a orde dos subgrupos e a estrutura que teñen.

```
S4 = SymmetricGroup(4)
S4.subgroups()
```

```
Subgroup generated by [()] of (Symmetric group of order 4! as a permutation
```

```
group),
Subgroup generated by [(1,2)(3,4)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,3)(2,4)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,4)(2,3)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(3,4)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(2,3)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(2,4)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,2)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,3)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,4)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(2,4,3)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,3,2)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,4,2)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,4,3)] of (Symmetric group of order 4! as a
permutation group),
Subgroup generated by [(1,3)(2,4),(1,4)(2,3)] of (Symmetric group of order
4! as a permutation group),
Subgroup generated by [(3,4),(1,2)(3,4)] of (Symmetric group of order 4!
as a permutation group),
Subgroup generated by [(1,4),(1,4)(2,3)] of (Symmetric group of order 4!
as a permutation group),
Subgroup generated by [(2,4),(1,3)(2,4)] of (Symmetric group of order 4!
as a permutation group),
Subgroup generated by [(1,2)(3,4),(1,3,2,4)] of (Symmetric group of order
```

```
4! as a permutation group),
Subgroup generated by [(1,3)(2,4),(1,4,3,2)] of (Symmetric group of order
4! as a permutation group),
Subgroup generated by [(1,2,4,3),(1,4)(2,3)] of (Symmetric group of order
4! as a permutation group),
Subgroup generated by [(3,4),(2,4,3)] of (Symmetric group of order 4! as
a permutation group),
Subgroup generated by [(1,4,3),(1,4)] of (Symmetric group of order 4! as
a permutation group),
Subgroup generated by [(2,3),(1,3,2)] of (Symmetric group of order 4! as
a permutation group),
Subgroup generated by [(1,2),(1,4,2)] of (Symmetric group of order 4! as
a permutation group),
Subgroup generated by [(3,4),(1,3)(2,4),(1,4)(2,3)] of (Symmetric group
of order 4! as a permutation group),
Subgroup generated by [(1,2)(3,4),(1,3)(2,4),(1,4)] of (Symmetric group
of order 4! as a permutation group),
Subgroup generated by [(2,4),(1,2)(3,4),(1,4)(2,3)] of (Symmetric group
of order 4! as a permutation group),
Subgroup generated by [(2,4,3),(1,3)(2,4),(1,4)(2,3)] of (Symmetric group
of order 4! as a permutation group),
Subgroup generated by [(3,4),(2,4,3),(1,3)(2,4),(1,4)(2,3)] of
(Symmetric group of order 4! as a permutation group)
```

```
def subH(x):
    return subgrupos[x]

[subH(x).order() for x in (range(30))]
```

```
[1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4, 4, 6, 6, 6, 6,
 8, 8, 8, 12, 24]
```

```
[subH(x).structure_description() for x in (range(30))]
```

```
['1', 'C2', 'C2', 'C2', 'C2', 'C2', 'C2', 'C2', 'C2', 'C2', 'C3', 'C3',
 'C3', 'C3', 'C2 x C2', 'C2 x C2', 'C2 x C2', 'C2 x C2', 'C4', 'C4', 'C4',
 'S3', 'S3', 'S3', 'S3', 'D4', 'D4', 'D4', 'A4', 'S4']
```

Recordemos que SageMath non sempre denota os elementos da mesma forma ca nós, neste caso o código devólvenos `D4` como o grupo diédrico de 8 elementos, que usualmente escribimos como D_8. Polo tanto, os subgrupos de S_4 son: $\{1\}$, C_2, C_3, C_4, $C_2 \times C_2$, S_3, D_8, A_4 e S_4. No capítulo 4 vimos que os retículos de subgrupos de C_2, C_3 e C_4 son cadeas, polo que G non pode ser ningún destes grupos. Na sección 3.3 vimos que o retículo de subgrupos de $C_2 \times C_2$ é o diamante, e na subsección 3.1.1 o do grupo S_3, que claramente tampouco é isomorfo ao de A_4. En S_4 hai trinta subgrupos, mentres que en A_4 só hai dez, polo que tampouco pode coincidir o seu retículo de subgrupos. En D_8 temos dez subgrupos, igual que en A_4, pero como podemos ver polo retículo de D_8 na Figura 6.1 só tres son maximais, mentres que en A_4 temos cinco maximais. Polo tanto, chegamos á conclusión de que G ten que ser isomorfo a A_4.

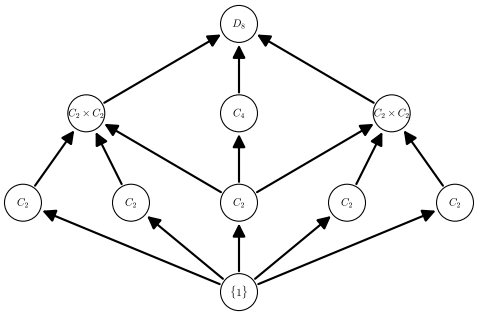


Figura 6.1: Retículo de subgrupos do grupo diédrico D_8.

Bibliografía

[1] Blyth, T.S., *Lattices and ordered algebraic structures*, Universitext, Springer-Verlag, London, 2005.

[2] Davey, B. A. e Priestley, H. A., *Introduction to lattices and order*, Second edition, Cambridge University Press, New York, 2002.

[3] Debreil, A., *Groupes finis et treillis de leurs sous-groupes*, Calvage & Mounet, Paris, 2016.

[4] Iwasawa, K., *Über die endlichen Gruppen und die Verbände ihrer Untergruppen*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I. 4 (1941), 171–199.

[5] Jez, A., *Subgroup Lattices That Are Chains*, Rose-Hulman Undergraduate Mathematics Journal, Vol. 7, Iss. 2, Article 4, 2006.

[6] Pálfy, P. P., *Groups and Lattices*, Groups St. Andrews 2001 in Oxford, Vol. II, 428–454, London Math. Soc. Lecture Note Ser., 305, Cambridge University Press, Cambridge, 2003.

[7] Pudlák, P. e Tuma, J., *Every finite lattice can be embedded in a finite partition lattice*, Algebra Universalis 10 (1980), 74–95.

[8] Roman, S., *Fundamentals of group theory. An advanced approach*, Birkhäuser/Springer, New York, 2012.

[9] Schmidt, R., *Subgroup lattices of groups*, De Gruyter Expositions in Mathematics, 14, Walter de Gruyter & Co., Berlin, 1994.

[10] Tarnauceanu, M., *A characterization of the quaternion group*, Analele Stiintifice ale Universitatii Ovidius Constanta Seria Matematica 21 (2013), 209–213.

[11] Viehweg, J., *Ore's theorem*, Theses Digitization Project, 145, 2011.

[12] Whitman, P. M., *Lattices, equivalence relations, and subgroups*, Bull. Amer. Math Soc. 52 (1946), 507–522.