Septimiu Crivei

Bront.

**BASIC ABSTRACT ALGEBRA**

BCU Cluj-Napoca

MATEM 2002 00512 Casa Cărții de Ştiinţă Cluj-Napoca, 2002

ISBN 973-686-320-4

**To my family**

:512/C-89

**.**

© Copyright, Septimiu Crivei, 2002

**\*\*\***

420 KM

**\***

Director: Mircea Trifu Fondator: dr. T*.*A. Codreanu Corectura și tehnoredactarea computerizată aparțin autorului.

Tiparul executat la Casa Cărții de Ştiinţă 3400 Cluj-Napoca; B-dul Eroilor pr. 6-8 Tel./fax: 0264-431920 www.casacartii.com; e-mail: editura*@*casacartii.coni

.........

.

Contents

**Foreword**

**1 Relations**

1.1. Basic Definitions and Examples ....... 1.2 Operations for Relations, ... 1.3 Relation Classes .............. 1.4 Functions ................. 1.5 Left Inverses and Right Inverses ...... 1.6 Homogeneous Relations .......... 1.7 Equivalence Relations and Partitions ... 1.8. Factorization of Functions ......... 1.9 Partially Ordered Sets ........ 1.10 Lattices and Algebras ........... ........ 1.11 Order and Lattice Homomorphismas : ... 1.12 Boole Lattices and Boole Algebras .......... 1.13 Homogeneous Relations vs Bivalent Matrices ....... 114 Closure Systems and Operators ................

**2 Algebraic Structures**

2.1 Basic Definitions and Examples ............ 2.2 Semigroups ................ 2018 Free Semigroups ........ 2.4. Groups ............... 2.5 Subgroups ........................... 2.6 Group Homomorphisms ...*. 2*.7 Cyclic Groups . ..............

2.8 Normal Subgroups ...................... 94 7 2.9The Isomorphism Theorems for Groups .......... 100

**is**

. WIG

*CO*N*TENTS*

Foreword

patunk

2.10 Rings ............. 2.11 Boole Algebras vs Boole Rings ........... : . 109 2.12 Subrings .. ..... .........:.....

. 113 2.13 Ring Homomorphisms . .......

116 2.14 Ideals ........................... 2.15" Congruences Modulo *n ..*. 2:16 Polynomial Rings . ........

. . 130

hauend

Homemak

**"Algebra is generous: she often gives more** than is asked of ber"

***(*D'Alembert)**

**Vector Spaces**

**139** 3.1 Basic Definitions, Properties and Examples ...

.. 139 *3*.2 Subspaces .......................

: . 143 3,3 Linear Maps ...

.. 150 3.4 Linear Independence and Basis ..*..*

· 154 3.5 Dimension ......................... : . 162 3.6 Dimension Formulas ..*....*............... 168

The present textbook has crystalized in the period 1995-2002, when I have taught seminars and courses of Algebra at the " Babeş-Bolyai” Uni versity of Cluj-Napoca. It mainly addresses to first year students in Gomputer Science. But I consider it could be a useful tool for anyone looking for a minimal presentation of some essentials of Abstract Alge

bra.

**173**

**4 Matrices and Linear Systems**

4.1 Elementary Operations ......

173 4.2 Applications of Elementary Operations .....

.. 179 4.3 The Matrix of a Linear Map ............. . . 184 4.4 Change of Bases ............. 4.5 Eigenvectors and Eigenvalues...

.. 195 4.6 Linear Systems of Equations ................. 202

..... 190

The book contains basic topics presented in 5 chapters, starting with *Relations,* continuing with *Algebraic Structures, Vector Spaces, Matrices and Linear Systems* and ending with *Linear Programming.*

The first chapter studies binary relations, especially concentrating on functions, equivalence relations, partially ordered sets and (Boole) lattices,

The second chapter introduces the main algebraic structures with one and two operations, such as semigroups, groups, rings and fields. Important topics are: free semigroups, cyclic groups, Boole algebras and Boole rings, modular congruences and polynomial rings.

The third chapter deals with the key notion of Linear Algebra, namely the notion of a vector space. Subspaces, linear Ipaps, basis and dimension of a vector space are introduced and their main properties are established.

The last two chapters contain some important applications of the theory of vector spaces. By means of elementary operations, there are presented practical methods for computing the rank and the inverse of a matrix as well as the Gauss method for solving linear systems of equa

........

**5 Linear Programming**

**211** 5.1 Basic Notions .....

1.... 211 5.2 Formulation of the Problem . ...*...*

218 5.3 Solutions .............*...*....

226 5.4 The Simplex Algorithm ................

233 5.5 The Simplified Simplex Algorithm ............. 243

**References**

**249**

**English-Romanian Selected Notions Dictionary**

**251**

**Index**

255

vii

**SENY**

viii

*FORE*W*ORD*

Chapter 1

tions. The final part is just an introduction to Linear Programming, the main result being the Simplex Algorithm.

Besides an *Index* of notions and results, I added an *English-Romanian Selected Notions Dictionary,* as a help for comparing the present English textbook with some Romanian ones in the field.

Talking about the contents of this book, I would like to emphasize the strong relationship between these fields of Algebra and Computer Science. Undoubtedly, computers offer an extraordinary tool for mathe maticians in solving complicated problems. On the other hand, Mathe matics in general, and especially Discrete Mathematics and Algebra, are essential in the development of research in the world of computers. In this sense, I should mention that the main notions and results of this course are the roots of the mathematical basis in different fields of Com puter Science, such as Formal Languages, Abstract Data Types, Graph Theory, Parallel Computation, Cryptography etc.

Relations

This first chapter is dedicated to the study of relations, that may be seen, as far as a mathematician is concerned, as generalizations of functions. But numerous examples of relations are present in the daily life, even if we have not perceived them in the present form. Our goal is to formulate their algebraic definition and to study their various properties.

*A*cknowledgements

.

**t**

1.1 Basic Definitions and Examples

AC

i

**T**

Ter

e

I would like to thank Professors Ioan Purdea, Nicolae Both, Andrei Mărcuş and, for the chapter on Linear Programming, Dorel Duca for their helpful suggestions and comments, that improved the quality of the material.

I am grateful to Professor Iuliu Crivei and Gabriela Olteanu for nu merous challenging conversations on the topics included here, for the patience of carefully reading the manuscript and, in general, for their generous support.

Finally, I would like to thank my students, whose questions and in terest have been encouraging to write the present textbook.

**Definiti**on 1.1.1 A triple r = (*A, B, R)*, where A*, B* are sets and *RS AXB*, is called a *binary relation.*

The set A is called *the domain*, the set *B* is called *the codomain* and the set *R* is called the *graph* of the relation r.

If *A* = *B*, then the relation r is called *homogeneous.*

If *(a, b*) E *R*, then we sometimes write *arb*and we say that *a has the relation r to b or a and b are related with respect to the relation T.*

.

.

.

.

..

...

.

Septimiu Crivei

Cluj-Napoca, September 2002

*Rerarks*. (1) Usually, we will call binary relations simply *relations.* The first name is due to the existence of some generalizations of binary rela tions, namely *n-ary relation*s, that are not a subject of the present course.. They are defined as (*n* +-1)-tuples (A1,...,A4*,R)*, where A.1, ..., An are sets and *R*CA, X...x Ay

(2) Sometimes, when A and *B* are obvious, we will call relation the graph *R* of the relation r = (A*, B, R)*.

.

.

*CH*AP*TER 1. RELATIONS*

*1.1. B*A*SIC DEFINITIONS AND E*X*A*M*PLES*

(3) If A*, B* CR, then the graph of a relation r =(A*, B, R)* may be represented as a subset of points of the real plane R XR.

Example 1.1.2 (a) Let C be the set of all children and *P* be the set of all parents. Then we may define the relation *r = (C, P, R*), where

*(g*) Let A and *B* be two sets. Then the triples

*O*= (*A, B*,*0)* and *U*= (*A, B, A x B)* are relations, called the *void relation* and the *universal relation* respec tively.

*R=* {(c*,p) EC\*P*lc is a child of p}.

*(6*) Let S be the set of all world's independent states and all capital cities of the world's independent states. Then we may define

the set of the relation *= (*S*, C, R*) by

*(h*) Let A be a set. Then the triple A = (*1*, A, AA), where

AA = *{(a, a) a* € A}, is a relation called the *equality relation* on A.

*(i*) Every function is a relation.

Indeed, a function*s*: A d*e B* is determined by its domain A, its codomain *B* and its graph

*src*c

is the capital of s.

(c) The triple (R, R*, R*), where

*R =* {(*X, Y*) ER XR ! \* S*y*},

is a homogeneous relation, called the *inequality relation* on R.

(d) The triple (N,N, R), where

*Gr=* {*(x,y)* E AX*Bly = f(x*)}. Then the triple (*A, B,G*i) is a relation.

(6) Every directed graph is a relation. . Indeed, a directed graph (V,*M*) consists of a set V of vertices, say V = {1,...,n} and a set M of directed edges ("arrows") between ver tices. We may identify each directed edge with a pair in V XV, where the first and the second component are respectively the starting and the ending vertex of that directed edge. Denote by *P* the set of those pairs, Then the triple (V, V,*P*) is a relation.

For instance, the directed graph

*R=*{(x,y) € Nx N/x divides *y*},

**A**

**}**

is a homogeneous relation, called the *divisibility relation* on N.

Similarly, one can define the *divisibility relation* on Z. (e) The triple q = (R,R,*R)*, where

*R= {(x, y*) ER XR2 + *y*2 = 1},

is a relation, whose graph can be represented in the real plane as the circle with the center (0,0) and the radius 1.

*f*) On the set *D* of all lines in space, we define the relations = *(D,D,R*) and s*= (D, D, S*) by

darda e di || da,

- nii

di sda 5 di 1 dz. They are the *parallelism, relatio*n and the *perpendicularity relation* of lines in space respectively.

can be seen as the relation (A, A, *R*), where A = {1,2,3,4} and *R =* {(1,2), (2,3), (2,4), (4,3)}. Definition 1.1.3 Let = (*A, B, R*) be a relation and let A SA. Then the relation

q! = (A*, B, R*n (A' x *B)*) is called the *restriction o*f r to A' and is denoted by Tla.

.

*CHAPTER 1. RELATION*S

*1.2. OPERATIONS FOR RELATIONS*

102

*el* such that *0.17?; Q2*.

**Definition 1**.1.4 Let ri = (41, *B1, R*i) and r2 = *(A2, B2, R*2) be rela tions. Then we define the *inclusion* and the *equality o*f relations respec tively by

*jer*

Definition 1.2.2 Let r = (A*, B, R)* be a relation. Then we define the *invers*e of, to be the relation *p*o *= (B, A, R*), where

*r*i çrg

A1 = A2, *B1 = Bz* and *Ri SR2,*

r1 =*7*24A1 = A2, *B1 = B2* and Ri *= R2.*

•

*R*

*= {(b,* a) | *(a, b)* E R} .

*Remarks.* (1) 11 = 12 + 91 5ra and 73 571.

(2) Coc*u* for every relation t.

(3) Let 91 = (A*, B, R*i) and r2 = *(A, B, R*2) be relations. Then *r*i Craif and only if (or *iff* in short) for ever*y a* E A and *b E B,* we have *ar*i*bar2b.*

*Remark.* Notice that the symbol --1 is placed on the top of the relation and not in the right upper part of it. We will see a motivation for that a little bit later.

i

*(A, B, R) and s* = (*A, B, S) be relations*. &

1.2.3 *Let go*

**Theorem** *Then:*

1.2 Operations for Relations

**kez**

1.

On the one hand, since a relation is a triple of sets, we might think of having some similar operations for relations as those for sets. On the other hand, since we may see the notion of relation as a generalization of the notion of function, we might expect having some similar operations for relations as those for functions. Both ideas are actually present in what follows.

*(*ü) FUSE T'U *(ii) r*ns = gan ist; *(ii)* SS Sist

have the same *Proof. (ii*) Obviously, the relations r us and you domain *B* and the same codomain A, so that we have left to prove the equality of their graphs. But this follows since

**Defin**ition 1.2.1 Let (ribier be a family of relations, where r*i* = *(*A, *B, R*i) for each *i el.* Then we define the *intersection* and the *union* of the relations ri respectively by

**5**

"=(4,B*,*OR),

*(b, a) € R*US *(a, b) E R*US (*a,b) E R* or (*a, b*) ESF

> (*b,* a) E *R o*r (b, a) € *ŠE (6,* a) *e Rus.* The proof of the other properties is left to the reader.

*¿El*

*€1*

Ur; = (A, B, UR*i).* ie*r*

*i e* : We also define the *cornplement* of a relation qi

F = (A*, B*, A X *B\R*).

**Definition 1**.2.4 *Let r* = (A, *B, R) and s = (C,D,S) be relations.*

*Then we define the composition of s and r to be the relation*

(*A, B, R*) by

sor= (*A, D, SOR),*

*Where*

*Remark.* In the context of Definition 1.2.1, we clearly have

*SOR= {(a, d) € AXD*|3r E *BOC: (0, 2) E R and (c,d*) ES.

lai nri)a2

*VieI, Q*i*ri*az,

*CHAPTER 1. RELATIONS*

*1.2. OPERATIONS FOR RELATIONS*

*Remark.* If *BAC* = 0, then sor = (A*, D*,%), so that sor is a void relation.

Pr*oof*. Let p = (*A, B, R), S = (C,D,S*) and *t = (E,F,T*') be relations. We will show that

*(tos*) or=*to (s*or). Notice first that the left hand side and the right hand side relations have the same domain A and the same codomain *F*, so that we have left to prove the equality of their graphs. .

Notice also that *tos= (C,F,T*oS) and *sor*= (*A, D, SOR).* Then the result follows since

Example 1.2.5 Letr = *(*A*, B, R*) and s = *(C,D,* S) be relations, where A = {1,2,3,4}, *B* = {x*,y*,z), *C* = *{x,y, t}, D = {*7,8} and

*R* = {(1, 2), (2, x), (4,y),(4, z)},

*S = {(x*,7*), (4,*7), (t, 8)}. Then we have s or = (A*, D, SOR*) and ro*s = (C,B,*C), where

*So R* = {(1,7), *(*2,7), (4, 7)}. Example 1.2.6 Let r = (A*, B, R*) be a relation, where A = {1,2}, *B* = {1, 2, 3} and *R* = {(1,1), (1, 2), (3, 2)}. Then we have 7 *= (B,A, R*), por = (A, A, *R R.*), ro *v = (B,B, ROR*), where

*(a, f) € (T*O*S) OR*

3*2 E BOC:(2, 2*) E *R* and (*3, f) ET*OS IN E *BOC, EY E DNE: (a, X*) E*R*, (*2,Y)* E S and (*3, 1) ET*

\* *E DNE: (a, y) ESOR* an*d (y, f) ET*

(*2, S) ET (SOR).*

-1

*R = {*(1,1),(2,1), (2,3)},

v

*ROR=* {(1,1),(1,3), (3,1), (3,3)},

*Ro R* = {(1,1), (1, 2), (2,1)*,(*2, 2)}. Notice that ro 7 € 72 or, to 7? 86 and 7 or \*8A.

Theorem 1.2.8 *Let r* = (A*, B, R), S = (C,D, S) and t = (CD,T) be relations. Then:*

p*a (1)* ro(s U*t) =* (*ros*) Ur*ot)*;

*(ii) r*o(s n*t)* 5 (ro*s*) n (r (10); *(int) 5 Str*oss*r*o*t; (iv) s*ör=jos

*Rernark*s. (1) In general, the composition of relations is not commutative (see Example 1.2.6).

(2) If r = (*A, B, R*) is a relation, then we have

*Proof.* It is easy to see that each left hand side has the same domain and codomain as the corresponding right hand side.

*(1)* We have

HY

*To*da =*r*=*dBO*R,

cros U*t*))

€ AM*D:*(*s*ut) and *orb pr*omos

so that A and ob are kind of identity elements on the right hand side and on the left hand side respectively.

3x E AO*D :(*c*sr or ct*r) and *url*

(3) If r = *(*A*, B, R*) is a relation, then in general rom \* 8B and po *lepo* Da (see Example 1.2.6). We have now an explanation for the different notation r, justified by the fact that put is not an inverse element for you with respect to the composition of relations.

ar E *AND:*c*sx* and I*rb*) or *(ctx* and u*rb*)

S c(*r*os) b or e(r*ot)b* c(*(*ros) U (r o*t*)) b. *(ii*) We have

c(ro(s n*t*))6 x EAN*D:c*(*s n t*) x and *urb*s

3

Theorem 1.2*.7 The composition of relations is associative.*

*CHAPTER 1. REL*A*TIO*N*S*

*1.3. RELATIO*N *CL*A*SSES* 1.3 Relation Classes

.63 EAN*D:csx* and *ctx* and *urbe*

3x EA*D:(cse* and *urb*) and *(ctx* and *Irb*)

*c(*ros*) b* and c*(rot)b =*

*c((r*os

*ot))b.*

Definition 1.3.1 Let r = (, *B, R*) be a relation and let X SA. Then the set

T(X) = {*bEB* 137 E X:*rb*} is called the *relation class of X with respect to r.*

In particular, we define two special relation classes involving a rela tion *r*, namely the *first projection*

Notice that we have equivalences except for only one step in the proof.

*(iii)* We will use the equivalences

*3 St*

*SCT*

*S*U*T = TE*SU*t=t.*

Then by (i) we have

*prir = 7\*(B) "*

and the *second projection*

*rot=r*o(s U*t) = (T*O*S*) U (*rot*),

*prar =* r(A).

whence pos C*rot*.

(*iv*) We have

*d(507)2* = a (sor*)d*

*Remarks*. (1) We denote r <*I*>=r*{*{r}).

(2) Notice that

(X)= Ur<x>.

*P*EX Example 1.3.2 Let r = (R, R, *R*) be a relation, where

38 € *BOC:ar*i and r*sd*

30 *€ BOC:x*ia and *ds* =

*d*lzoshja.

*R= {(x,y*) ERXR*y=*2}

*Remark.* The corresponding properties for (*i*), *(ii*) and (*iii*) with the composition on the right hand side hold as well.

and let X = (-2,2). Then , <3 >= *q*uo <-3 >= {9}, r(X) = (0,4), *p*riru s R and prar = {0, +00) - R

Notice that *prir* and *p*ra*r* are obtained by geometrically projecting all the points of the graph *R*onto the axes *Ox* and *Oy* respectively. This fact justifies their name of projections.

**Example 1**.2.9 Let A = {1,2,3,4} and let r, s and *t* be the homoge neous relations on A with the graphs

A

.

*R =* {(1,2), (1,4), (2,3), (4,3), (4,4)},

Amung und

Theorem 1.3.*3 Let y = (*A*, B, R) be a relation and let* X,Y C *Then:*

*í () r*(XUY) =r(X) UT(Y);

*(ii) r(*

X Y) Cr(x) Or(Y); *(iii)* X CY= (X) Cr(Y).

puertory

**>**

***;***

**\*; et**

*A*N

S = {(1, 1), (2, 4), (3,4)},

*Proof. (*) We have

*T* = {(1,4), (4,4)}.

*ber*(XUY)

32 € XUV:2*7be*

Then

*RO(SAT) = 0* + {(1,4)} = *(R*O*S*) n (*R*o*T*).

Iz € X or Iz EY:z*rb membe*r(X) or *ber*(Y)

*CHAPTER 1. RELATIO*NS

*1.4. FUNCTIONS*

**I'LL**

*Proof.* We have

*de(s* 0T)(X)

x € X:(so*r) d*

A

*b*er(x) Ur(Y). *(ii)* We have

*Lb & r(*XoY) 4932 6 xnY: *zrbi*a B ize X and Iz € Y:zr*bb*er(X) and *b*er(Y)

*b*er(x) Ur(Y). Notice that we have equivalences except for only one step in the proof.

*(ii*i) Use the set-theoretic equivalence X SY XUY = Y and apply (i). QO

IX E X and 3*y € BOC:ry* and *ysd Jy Bnoiy Er*(X) and *ysdad E s*(r(X)).

.....

1.4

Functions

**Defini**tion 1.4.1 A relation r = (A, *B, R*) is called a *function (*or a *functional relation* or a *map* or a *mapping)* if

Va e A, lr<

>1=1,

**Theorem 1**.3.4 *Let r* = (*A, B, R) and s =* (*A, B, S) be relations and let X* CA. *Then:*

*(i) (r*us)(X) =r(X) Us(X);

*(ii) (r O*s(X) CT(X) ns(X); *: (ii) r C*sabay *n*(X) Cs(X)..

that is, the relation class with respect to*r* of every a E A consists of exactly one element.

*Proof.* Left to the reader.

*Remarks. (*1) If A is a set, then we denote by Al the *cardinal* of *A*, that can be identified with the number of elements of A provided A is finite.

**Example 1.3**.5 *(*a) Let A = {1,2,3}, *B =* {1,2,3,4}, X = {1,2} and Y = {2,3} and let r = (A*, B, R)* be a relation, where

*R*={(1,2), (1,4), (2, 3), (3,4)}.

Summer

*(*2) A relation r= (*A, B, R*) is a function iff *(1*) v*a €* Å, 3*5 € B:aró* (i.e., *Va* € A, 1r *<a>*11); *(ii) a € 4*,*5*,*6' EB, arb* and *arb'a b=t* (i.e., *Ha* € A, sr <a>51).

In other words, a relation *r* is a function iff every element of the dornain has the relation r to exactly one element of the codomain.

**Then**

*r*(XRY) = {3} + {3,4} = "(x) nr(Y).

*(6*) Let A = {1,2,3}, *B* = {1,2,3,4} and X = (*A, B, R*) and s = *(A,B*,S) be relations, where

{2,3} and let r =

*R =* {(1, 2), (1,4), (2,3)}, S = {(2, 1), (2,4), (3,3)}.

In what follows, if *j* = (*A, B, F*) is a function, we will mainly use the classical notation for a function, namely *f*: *A* - *B or* sometimes A *B.*

The unique element of the set *f <a*> will be denoted by (*a*). Then we have (*a, b) EFS f*(a*) = b*.

By Definitions 1.1.1 and 1.1.3, we get the following corresponding notions for a function.

**ri**

2. 1

Then

frn s)(x) = " + {3} = r(X) n s(X*)*.

**Theorem 1.3.6** *Letr* = (*A, B, R) and g = (C, D, S) be relations and let X* C*A. Then*

Definition 1.4.2 Let *f* : A - *B* be a function. Then A is called the *domain, B* is called the *codomain* and

.*:/* sor)(X)= ((X)).

*F= {(@, f(*a))|a € A}

12

*CHAPTER 1. RELATIONS*

ܡܡܕܼ

*1.4. FUNCTIONS*

is called the *graph o*f the function *f.*

If *f* = (*A, B, F*) and A' CA, then the relation *(A, B,F*nA' *B*)) is a function called the *restriction of f to* A', that is denoted by flar : ?

A *- B* and is defined by *f*al*a') f(a'), Va'* E A'.

*Proof.* By induction on *n. Remarks.* (1) The set *B*A, where A = *n*, can be identified with the set *B = B*X..\* *B.*

tiTM 会员

Using the definition of the equality of two relations and of the graph of a function, two functions *f* : A - *B* and *g:0 - D* are equal iff A = *0, B = D* and *Va* EA, *f(a*) *= g(a)*.

(2) Let us see what happens if we allow *n* or *m* to be zero, that is, A=*0 o*r *B=0.*

If A = 0, then *B*A *- BW = {*I*f :0 --B* is a function has a uniquc element, namely the inclusion function of 0 int*o B (*this is true even if *B=0*). Identifying *B* with *B*o, it follows that Bo has a unique element.

IF A*0* and *B =* 0, then *B*A = *0*A = {*f*l*f*: A-R is a function) bas no ele*m*ent.

**Example 1**.4.3 (a) Let A be a set. Then the equality relation (A, A, AA) is a function called the *identity function (map) on* A, that is denoted by 1A: A - A and is defined by 1A(a) = *a, Va* E A.

*(*6) Let *B* be a set and let A C*B*. Then the relation (*A, B,* AA) is a function called the *inclusion function of* A *into B,* that is denoted by *3* : A - *B* and is defined by *i*(a) *= a,* v*a* € A...

*(*c) Let *P*i : A, X A2 - Ai and *P*2 : A1 X A2 - A, be defined by *P1(01,0*2) = *a*1 and *Pz*(a1, *a*z) = *1*2, W*a*1,*02*) € A1 x A2. Then *p*i and *Pz* are called the *canonical projections.*

*(d*) Let A = {1,2,3), *B =* {1,2} and let r = *(*A*,B, R), S* = (A*, B,* S), *t* = (4,*B,T*) be the relations having the graphs

d

a

....

.

."

Definition 1.4.5 Let o*p*: A *- B* be a function and let X CA and YC*B*

We call the *image of X by* the relation class of X with respect to *f*, that is,

*f*(x) = *{b € B* | 3x € X : *236} =* {*}*() (2 € X}

We denote Im*f = f*(A) and call it the *image of f.*

We call the *inverse image (*or the pre*-image) of Y by f* the relation class of Y with respect to *s* , that is,

..

..

..

.

..

.

.

**A**

mer 1

.

.....

*f* (Y) = {*@* E A

*R=* {(1, 1), (2, 1), (3, 2)),

S = {(1,2), (3, 1)},

*T =* {(1,1),(1, 2), (2, 1), (3, 2)} . Since *r <a*> = 1 for every *a* € A, the relation r is a function. But s and t are not functions, because, for instance, we have s <2> =0 and t<1>1 = 2.

*Y* EY:*y fa*}={0€ *Al(a*) EY}.

**7**

.

.

.

For the first tirne in this course, we are going to give a so-called *characterization theorem*, that is an equivalent (necessary and sufficient) condition to the definition of a certain notion. In general, characteriza tion theorems are given with the goal of having alternative (and usually simplor) possibilities for proving results.

Now we introduce a classical notation. Let A and *B* be two sets. Then we denote

**Theorem**

**1**.4.6 *A relation r* = (A, *B, R) is a function iff*

*BA - {j*

*s*

*: A* -

*B* is a function.

The notation is justified by the following nice result.

**K72**

AAC *ROR and ROR* C*AB.*

**Theorem 1**.4.4 *Let A and B be finite sets, say* |A1 = *n and B*I =*m (m,n* EN\**). Then*

|*B*A| = m” *= 1B*1141

TA

*Proof.* We will use the remark following the definition of a functioni.

On the one hand,

*Va* € A, 3*5 € B:arbe*id

i

**1**

14

**C*ADA***

*CHAPTER 1. RELATIONS* I

**U11**

.

*1.4*. FU*NCTIONS*

*Proof.* Since *f* and *g* are functions, we have *Va* e A,

*(gof*)<*a >= 9(*

*<a*>) = *9<f(a)* >= {*91.*

)

tae A, 35 *€ B : (a,b*) € *R* and *(b, a) E R*

avae A, (a, a) E *ŘOR SACROR."* and on the other hand,

la € A*, 6, 6' EB, arb* and ar*b=+b = b']* (0€ A, *B, B'E B, (a,b) E R* and (*2,6*') E*R= (5,6'*) € AB) = la € A*, b, b' E B, (b, a) e R* and *(a, b) ER=(5,6').*E AB)

= *[(5,6*") E*RO R=(5,6')* AB]

*ROR C*AB.

so that ligo*s*)<a> 1 = 1, *Va* e A, i.e., *go f* is a function. *Remark.* In order to avoid the extra condition put in the previous theo rem for assuring that the composition of two functions is still a function, in general we will consider functions *f*: A - *B* and *g:B. C.*

Definition 1.4.10 A function *f*iA - *B* is said to be;

(1) *injective (*or an *injection* or *one-to-one* or *moni*c) if

*2*1,22 € 4, X1 #*2*2 ==*> j (*1) *+ f(*x2).

(2*) surjective (*or a *surjection or onto* or *epi*c) if

Corollary 1.4*.7 Let f*: A--*B,* XC A an*d* Y *S B. Then*

*Vy e B*, 3x € A : f(*x) = y.*

(3) *bijective (*or a *bijectio*n) if *f* is both injective and surjective.

XC *F (F*(X)) an*d FC* (Y))CY.

f

**of**

**4**

**1X**

**U**

**h*e*re**

*W*

*W*

We recall here a few well-known characterizations of injectivity and surjectivity

We have already introduced some operations for relations. We might ask now if they are compatible with the notion of a function, that is, if an inverse (in the sense of a relation), complement, union, intersection or composition of functions is still a function or not.

In the case of the first four operations the answer is negative, as we can see in what follows.

Lemma 1.4.11 *Let f* : A - *B be a function. The follouring conditions are equivalent to the injectivity of f:.*

*(1) 21*,22 E A, f(iki) = *f(22*) = 21 = *12*; *(ii) Hy E B, the equation f(x) = y has at most one solution in* A; *If* A*, B*CR, *then we may add:*

*(921) Every parallel to the O2 aris passing through a point of B in tersects the graph of f in at most one point.*

(4, A, *F*) and *g =*

Example 1.4.8 Let A = {1,2,3} and let *f = (A*,A,G) be relations, where

*F* = {(1,1), (2,3), (3,1)},

*G* = {(1,2), (2, 1), (3,3)}. It is easy to see that *f* and g are functions. But since, for instance, we have *f* < 2 > 1 = 0, 1*1* <1> 1 = 2, 1U*g)* <1>1 = 2 and l*i*n*g)* <1>1=0, the relations*, f, fug* and *ing* are not functions.

Lernma 1.4.12 *Let f* : A - *B be a function. The following conditions are equivalent to the surjectivity of f:*

*(i) f*(4) - *B; (ii) Vy E B, the equation f(*x) *= y has at least one solution i*n A; *If A, B*CR, *then we may add:*

*(iii) Every parallel to the O2 auis passing through a point of B in tersects the graph of f in at least one point.*

-

1

.-.

"..---..

**Theorem 1**.4*.9 Let f= (*A*, B,F*) *and g - (C,D,G) be functions such : that f(A*) S*C. Then the relation go f = (A, D, GOF) is a function.*

Example 1.4.13 (a) Let *B* be a set and let A C*B*. Then the inclusion function *1* : A - *B* is injective (see Example 1.4.3).

**1**

***r***

**16**

*CHAPTER 1. RELATIONS*

**R*UA***

*1.5. LEFT INVERSES AND RIGHT IN*V*ERSES*

1

1.5

Le**ft Inverses and Right Inverses**

**VA**

. *(b*) Let *|* :R - R. be defined by *f*(r) = *32,* V*I* E R. Then *f* surjective.

*(*c) Let A be å set. Then the identity function 1A:A - A is a bijection.

Theorem 1.4.14 *Let f = (A, B, F) be a function. Then: T (i) f is injective iff* AA *= F OF;*

*(ii) f is surjective iff Fo F* = A*B*

We have just seen that every bijection has an inverse. What happens with injections or surjections? We are going to see that they have some partial inverses,

**Definitio**n 1.5.1 Let *f* : A - *B*. Then:

(1) *r:B*-A is called a *left inverse* of *f* if*rof=*1a; (2) *s: B*- A is called a *right inverse* of *f* is *fos*=1*8.*

*Remark.* Notice that is r is a left inverse of *f*, then *f* is a right inverse of r and if s is a right inverse of *f*, then *f* is a left inverse of s.

**ef**

**?**

**Theorem** 1.5.2 *Let A + 0 and let f :* A w *B. Then the following statements are equivalent:*

*(i) { is injective; (ii) f has a left inverse*; *(112) For every set C and every 9, h:0*-A,

*Proof.* Since *f* is a function, AAC *FOF* and *FoF* CAB by Theorem

1.4.6. V (i) = Now let (x, *y) € F*O*F*. Then 32 € *B* such that (2,7) *EF* and (2,*4*) *E F* or equivalently (1,2) *E F* and *(y*, z) € *F.* Hence *f(0*) = *f(y)*z. But *f* is injective, so that I*=y*. Then (*1, y)* € AA.

5. Let 21, 22 E A be such that *f*(21) = *f*(x2) = *y*. Then (21*,y),* (12*,y) € F* or equivalently (21*,y) E F* and (*y, 22*) € *F*. It follows that (21,22) € *FOF=*AA, whence 21 = 22. Therefore, *f* is injective.

(ii) The function *s* is surjective V*y E B,* Ix € A such that *f(x) = y a Vy EB*, 3*.1* € A such that (*y,x) € F* and (x,*y) EF Vụ C B, g, gỗ - Fo F <*> A*BC Fo F.* Corollary 1.4.15 *Let f : A B. Then:*

*(2) f is injective iff VX* CA, X = *f (F*(X));

*fog fohg=h.*

*Proof.* We are going to prove that (*i*) *(12*) 3 *(122*) (*i)*.

(i) (*i*i) Suppose that f is injective. We have 4+0. Then V*y e f*(A), Hrg € A (unique) such that *f(x) = y.* Now deline*r : B* - A by

ky i*f y* e*l(*A)

r(y) = 170 if y*€ B\J*(A)

*(ii) f is surjective iff VY SB, f(*

*(Y*)) =Y.

where 30 € A is arbitrary. Since

*Then f =*

Corollary 1.4.16 *Let f* = (A*, B, F) be a function. (B,*A,*F*) *18 « function iff f is bijective.*

*t*a EA, (ro *1*)(I*) = r(j* (x))= *2,*

1

*Proof.* By Theorems 1.4.6 and 1.4.14, *f* is a function iff A*B SHOF* and *F OF* CAA iff f is bijective.

it follows that *g*o*f=*1A, i.e., r is a left inverse *o*f*f.*

*(21) = (iii)* Suppose that *f* has a left inverse, say *r*. Let *g, h: 0 -* A be such that *fog = foh.* Then

**Corollary 1**.4.17 *Let s*: *A* --*> B be a bijective function. Then f is a bijective function, which is denoted by f-1 and is an inverse of f, i.e*.*,*

*f-10 f* = 14 *and fof=1*= 1B.

*fog=foh*o*lfog) =rofon*)

RY

=

*(rof)og (*ro*f)oh*

1A o*g*=1A o*hg=h.*

***1*8**

*CHAPTER 1. RELATIONS*

*15 LEFT INVERSE*S *AND RIGHT INVERSE*S

Morescu

where y*i E B* \ *{y*o} is arbitrary. Then *g*

*h* and VEEA,

*(iii) = (2*) Assume that (*iii*) holds and suppose that *f* is not in jective. Then 3:2 1,82 € A, 11 *+ 1*2, such that *f*(x1) = *f(*12*)*. Now let *C* = {x1} and define *g, ħ :C*-A by

*(90D) (2) = 9(S(x)) = f(t) = h{f(z*)*) = (ho D)*(x),

*9(9*1) = xi and *h(x*1) = 22. Hence *g h.* On the other hand,

*(fog)(x*i) *= f(g(*x1)) = f(*xi) = f(x2) = f(h*(*x*))) = *(f oh)(*x1),

so that *go f= hof*, which is a contradiction.

Assume now that A = 0. Since *B* Ø, there exist a set O and *gh:B* with *gth*. But since A = 0, we have *goj=hof*, which is a contradiction.

Therefore, *f* is surjective.

Using the constructions given in the proofs of Theorems 1.5.2 and 1.5.3, we are able now to give a few examples of left and right inverses for injective and surjective functions respectively.

so that *fog=foh.* But this is a contradiction, hence *s* is injective. O

**Theorem** 1.5.*3 Lei f* : A w*at B. Then the following statements are equivalent:*

*(i) f is surjective; (ii) f has a right inverse; (iii) For every set C and every g,h: B - C,*

*gof=hofag=. Proof.* Again we are going to prove that *(i*) = (*ii*) = *(iii)* = (*i*).

(*1*) = *(ii*) Suppose that *s* is surjective. Then V*y E B,* there exists an (but possibly many) I4 € A such that *f*(*xy) = y.* Now define s*: B*m A

Example 1.5.4 Let *f*:R - R be defined by *f*(x) = 6, *VI* ER and let *g*:R - 10,00) be defined by *g* ) = 22, *VI* ER. Then */* is injective and g is surjective.

A left inverse of *f* is a:R - R defined by

Jinx 30

if x > 0 if r <0

by

where to E R is arbitrary and a right inverse of j is e: 10,00) - R defined by

*s*(x) = *væ,* VI € (0,0). Another right inverse of *f* is s" : [0,00) - R defined by

*$(y)* = my, where I, is arbitrarily chosen among those 2 € A satisfying *f*(x) *== y.* Since

*Vy E B, (fo*s)*(y) = f($(y)) = f(xy*) *= y,* it follows that *fos* = 1B, i.e., s is a right inverse of *f.*

*(ii*) e *(izz*) Suppose that *s* has a right inverse, say s. Let *g, h : B - C* be such that *gof=hof*. Then

*$'(:1)* = -*VI, Vx* € (0,00).

We have just seen that even if they do exist, left inverses and right inverses are not unique in general. But they are unique in the case of bijections.

**WP**

**Corollary 1**.5.5 *A function f* : A - *B is bijective if s has both a left inverse and a right inverse, in which casc they are unique and equal to the inverse 1-*1.

*gof=hof (gof) o s= (hof)os =>go(fos) =ho (fos) go*l*B = ho*l*b= =}. (iii) = (i*) Assume that *(izi)* holds and suppose that is not sur jective. Then *B +*0. Also *yo € B (A*).

Assuine first that A +0. Now let *C = B* and define *g, h:B- B* by *g=*1*8* and

Jy if *y € B* \ {yo} *h(y)* =

if *y=y*os

*Proof. A*pply Theorems 1.5.2 and 1.5.3 to prove the equivalence.

Now assume that *f* has a left inverse and a right inverse, say *r :B* A and *s:B* - A respectively. Then *r*o*os) = y0*1p=*r* and on the other hand, *(*ro)0*3*1AO*S - 5*, hence *r* = s. But then we must have

20

*CHAPTER 1. REL*A*TIC*

The notions of left and right inverses allow us to prove properties on (injective or surjective) functions without working on elements. This idea is present in results of the following type.

**Corollary 1**.5.6 *Lets: A* - *B and g:*

*B C . Then: (1) f f and g are injective, then go f is injective; ♡ (ii) If f and g are surjective, then go f is surjective;*

*(iii) If gof is injective, then f is injective; (iv) If go f is surjective, then g is surjective. (V) If gof is bijective, then f is injective and g is surjective.*

**1**

*Proof. (i*) If *f a*nd *g* are injective, then by Theorem 1.5.2 they have left: inverses, say *ri: Bm* A and r2 : *0 m B re*spectively. Then:

(r10rz*) 0 (gof) = 7*70 (*120g) o f =r*10 1*8 of =*rlo*f*=1A,

.K.

.

i.e.*, gof*: A - C has a left inverse, namely *r*ior2:*0* - A. Then again by Theorem 1.5.2*, go f* is injective.

*(iv*) If *go f* is surjective, then by Theorem 1.5.3 *g*o*f*: Am C has a right inverse, say *s:0*- A. Then

(5) *I, Y* EA, *Xray S yrr;*

*artisymmetri*c if : (a) *X,Y* E A, *Iry* and *yI* = x= *y.*

These properties of rı may be characterized in terms of the graph R of r. The following easy lemma, whose proof is left to the reader, will allow us to prove properties on homogeneous relations without working on elements. Lemma 1.6.2 *Lets* = (A, A*, R) be a relation. Then:*

*(i)r is reflexive* AAC*R;*

*(11) r is transitive RORSR; . (117) 7is symmetric RCR R= R*;

. *(iv) r is anlisymmetric > RAR* CAA. *Remark.* One can prove that the four properties are independent, that is, none of them is a consequence of some of) the others. **Definition 1**.6.3 A relation r = (A, A, R) is called:

(1) an *equivalence relation* if r has the properties (r), (t) and (s);

*(*2*)* a *quasi-order* (or *pre-order)* (relation) if y has the properties (r) and (t);

(3) a *partial order* (relation) if r has the properties (r), (t) and (a). Example 1.6.4 (a) The equality relation SA on a set A has all the four properties, hence 8 A is both an equivalence and a partial order relation,

*(b)* The inequality relation ” ” on N, Z, Q or R has the properties (r), (t) and (a), hence it is a partial order.

(c) The divisibility relation on N has the properties (r), (t) and (a), hence it is a partial order, whereas the divisibility relation on Z bas only the properties (r) and (t), hence it is only a quasi-order. .

*(d*) The perpendicularity relation of lines in space has only the prop

· erty (s).

(e) Let *72*. EN and let po be the relation defined on Z. by

...

14 = *(gof*)os*=goos),*

**Iverse, Da**

**Orern**

i.e., g has a right inverse, namely *f*os:*0 + B.* Then again by Theorem 1.5.3, *g* is surjective.

*(i*i) and (i*i*i) can be proved analogously and they are left to the reader and (v) is an immediate consequence of (*iii*) and (*iv*).

**1.6 Homogeneous Relations**

Recall that a relation p = (A*, B, R*) is called *homogeneous* if *A = B.* This type of relations are the subject of several sections of the present chapter.

**Definition 1.6.1** A homogeneous relation r on A is called:

a *reflexiv*e if (r) *VE*E*A*, *ITE*; & *transitive* if (t) *I,y,*z EA, *ery* and *yr22T*z; \* *symmetric* if

*Pyny S zy* (mod n*u*), that is, *52* (*3 - y)* or equivalently for *n #*0, # and *y* give the same remainder when divided by n. Then *P*rı is called the *congruence modulo* n and it has the properties (r), (t) and (s), hence it is an equivalence relation. They on

MX

*CHAPTER 1. RELATIONS*

*1.7. EQUIVALE*N*CE RELATIO*NS *A*N*D PARTITIONS*

23

::

We denote by *E(*A) the set of all equivalence relations on a set A ind by O(A) the set of all partial orders on a set A. A first example: of an equivalence relation and of a partial order is given in the next proposition, other examples being discussed in the following sections.

*Proof. (i*) Since AAC*R* and A4 SS, we have AAC*RO*S and AA C*R*US. Hencerns and r Us are reflexive.

(*ii*) Since *RORCR* and So*S*CS, it follows that

**Lemma 1.6**.5 *Let* A *be a set. Then*

**0**

*E*(*A*) n

(A) = {8a}.

*(R*A*S)o(R*OS) Ś *(RoR)N (ROS)* n(*SoR*)n(SOS).

*SRN (ROS)n(SoR) SSRO*S. Therefore, rns is transitive.

*(*iii) Sinc*e RC R* and *SCS*, we have

**non**

**VE**

1

........

*R*OSC*ROS = A*

..

*Proof.* Obviously, we have 8A E *E(A*) NO(A), since it satisfies the four properties of homogeneous relations. Conversely, let p = (*A*, *A*, R) E *E*(A) nO(*A*). By reflexivity, AAS *R*. By symmetry*, R= R.*, hence by antisymmetry, *R = RORC*AA. Therefore, *y =* DA.

Equivalence relations and partial orders will be mainly studied in the next sections. For the time being, we will give some other properties of homogeneous relations.

---1

*R*USS *R*US *- R*U*S*.

**Theorem 1.6.6** *Let ro* - (A, *A, R) be a relation. If r is reflexive, tran sitive, symmetric or antisymmetric, then qe has the same property.*

(iv) Since *RN R C*AA and *S*A*S* SAA, it follows that

*(R*NS) (RNS) = *(R*O R)n(*s* ) CA*A*

--- )

Therefore, rns is antisymmetric.

.

..

..

*Proof.* Suppose that r is reflexive. Then A*A CR,* whence AA = A S *R*, i.e., ;? is reflexive.

Suppose that r is transitive. Then *RORS R.* It follows that -1 -

- 1 *R*O*R = RORC R,* i.e., quo is transitive.

...

\*\*\*

..

.........

Corollary 1.6.*9 Letr* (A, A, *R) and s=* (A, A, S) *be relations. If r and s are equivalence relations, quasi-orders or partial orders, then r*ns *has the same property.*

.

www

.....

.

**کيسية**

.termini

.....

..

.W

...

1.7

Equivalence Relations and Partitions

......

..

I SAL

.

..

.

.

.

Assume that r is symmetric. Then *RCR*, whence *RS = R,* i.e., p is symmetric.

Assume that r is antisymmetric. Then RO*R*CAA, whence Aa, i.e., z is antisymmetric. **Corollary 1**.6.*7 If r is an equivalence relation, a quasi-order or a par tial order, then it is.*

..

Recall that a relation r = *(*A, A, *R*) is called an *equivalence relatio*n if it is reflexive, transitive and symmetric. We have denoted by *E(A*) the set of all equivalence relations on a set A.

.

.

.

"

'

'

**.**

..

.

..

.

**v*e*rsal**

.

.

.

..

**Example 1**.7.1 The following rclations are equivalence relations:

(a) the equality relation 8A = (A, A, AA) and the universal relation (A,A, AXA) on a set A (see Example 1.6.4 (a)).

(b) the congruence modulo n on Z (see Example 1.6.4 (e)). (c) the similarity relation on the set of all triangles in the plane.

.

**Theorem 1**.6.8 *Letr =* (A, A, *R) and s =* (A, A, S) *be relations. Then:*

*(i) If y and s are reflexive, then r*ns *and r* U*s are. (ii) If r and s are transitive, then rn*s *is. (iii) If r and s are symmetric, then r*ns *and r* U*s are. (iv) If r and s are antisymmetric, then rns is.*

.

.

.

"

:

"

"

"*"*

\*\*

:*: CH*A*PTER 1. RELATIONS*

25

We have seen that the intersection of two equivalence relations is again an equivalence relation. The following two theorems offer new methods of obtaining equivalence relations, starting with either quasi orders or some other equivalence relations.

I.e., *r*os is symmetric.

Therefore, ros is an equivalence relation Definition 1.7.5 Let r *€ E(*A). The relation class *p* < 20 > of an element € A with respect to n is called the e*quivalence class of 2 with respect to ?.*

Then the element & is called a *representativ*e of the equivalence class que <*3 >*

**Theorem**

**1**.7.2 *Let r be a quasi-order on A. Then rnq € E(*A).

*Proof.* Since r is a quasi-order, r is reflexive and transitive, hence it has the same properties by Theorem 1.6.6. Moreover, we have

We are going to see that equivalence classes behave much better than general relation classes. For instance, we have the following important lemma.

1

*ROR - ROR R*O

Lemma 1.*7.*6 *Let r E E(*A) *and 3*1,22 E A*. Then*

so that r n got is symmetric. Thus, on gon is an equivalence relation. O

**i**

Example 1.7.3 Letr be the divisibility relation on Z. Then r is a quasi order on Z, hence rn is an equivalence relation on Z by Theorem 1.7 2. In fact,

*\*(*rn 7')*y* x1 = l*y*1. **Theorem** 1.*7.4 Letr, s E E*(4). *Then*

..!'

Wwe

*T*OS *E E(*A)

ro*ssor.*

**Dow 21**

*Proof. =*. Suppose that r*os € E*(A). Sinceros, r and s are symmetric, we have

*RO*S = *ROS* = S*ORSOR,*

*7*1 *r X2 g <3*1 > <*x* >. *Proof.* If 21% 22, then x2 €<>. Hence

5 Kg >Cr(r< 11 >) = (ror) <2><*r* <11 > by the transitivity of r. By the symmetry of r, we have *227 I1*, whence similarly we get r <21 >C*r<12*>

The converse is obvious. W e

We define now an important notion connected with that of an equiv. alence relation. **Definitio**n 1.7.7 Let A be a non-empty set. Then a family (Ailier of non-empty subsets of A is called a *partition* of A if:

(i) The family (Ailie*r* covers A, that is,

U Aj = A;

*LEI* (ii) The subsets A, are pairwise disjoint, that is,

*2,3 € 1,1 + j* a Ain Aj = *0.*

**i**

so that ros = *sor".*

YOY

C..!!.

. Now suppose that ro*s*=so*r*. Since *r* and s are reflexive, AAC*R* and AA SS. Then it follows that AA C*RO*S, i.e., *r*os is reflexive.

Since n and s are transitive*, R*O*RCR* and SOS CS. Then

**LIV**

.IL .. --

W HY

arruar

.P

*(ROS*) *(ROS*) *= ROSOR) OS = Ro(R*OS)*S="*

*= (RO R) 0(S*OS) S*ROS,* i.e., ros is transitive.

Since r and s are symmetric, *R =* R and *S = S*. Then

SH! Y

74.

**Example 1**.7.8 (a) Let A = {1, 2, 3, 4, 5) and 41 = {1,2,3}, Ag = {4}, A3 = {5}. Then (A1, A2, Ag} is a partition of A.

*(6)* Let Aj be the set of even integers and A2 the set of odd integers. Then (A1, A2) is a partition of Z.

(c) Denote Any (,+ 1) for every *n E*Z. Then the family (An)?26% is a partition of K.

SSE

-1 -- 1 - *RO*SE SO*R=SOR=R*os,

the

26

.:

*CHAPTER 1. RELATIO*N*S*

*1.7. EQUI*VA*LENCE RELATIONS AND PARTITIONS*

2. ***I*N**

*27*

**..**

**.**

because for ever*y Ey*e A,

A*/T* = {r << > 2€ A};

*3G(*A*/T)*

*y*

*a* EA:*1, y en ca*m*ery.*

For every *r= (*Ailier *€ P(A*), we have

which is the set of all equivalence classes of elements of A with respect to r, is called the *quotient set of A by r.*

*(FOG)(T*) = *A/G(*7) = {<>

€ 4} = *7,*

**TYY**

**2**

z

We denote by *P*(*A*) the set of all partitions on a set A. Usually, we will denote a partition by *T.*

The following theorem establishes the connection between equiva- lence relations and partitions.

because for every 2 € 4, the class of the partition A/*G*T) containing 2 is the same as the class of the partition containing 2. Indeed, let

e Ag. Then

"

.

.

..-

*Tm* <

>

*{*

c A } *TT g} - {s* E 4 | vc } = A, .

.\*\*\*

**1**

**Theorem** 1.7.10 *(i) Let r E E(A). Then*

*Alr =* {*r* <I> 3 E A} E *P(*A).

Thus, *GoF* = 1E(A) and *FoG*=1P(A), i.e.*, F* and G are bijections. I *Remark.* If t = (Aic*i € P(*A), then the corresponding equivalence relation t has the graph

*(tr) Let T* = (Aili*er E P(*A) *and define the relation t# on A by*

*ITFY*I E*I:1,*€ Ai,

*R*x=U(A; x A;).

-

Wi-X

Example 1.7.11 (*a*) Let A = {1,2,3} and let r and s be the homoge neous relations defined on A with the graphs

*Then , E E(A*).

*(iii) Let F : E(A*) - *P*(A) *be defined by F(*T) = A/*r, Van € E(A*). *Then F is a bijection, whose inverse is G:P(*A) – *E(A*), *defined by G*T) =*T, VI E P*(A).

.

**formeeste**

Pagame?

*R*= {(1,1), (2,2

S = {(1,1),(2, 2), (3, 3),(1,2), (2,3)}. Then r is an equivalence relation, but s is not. The partition correspond ing to r is

**FA V**

V

*YPR*INS

I

.....

.

..

.

.

...

....

.

....

.....,

.

..

...........

.

**{**

**1**

portes,

Format

pand sunny

.

(*6*) Let

............

mand

**}**

.

*Proof. (i*) Since r is reflexive, we have & € pro <3>, *Vx* e A, hence A CUca*r <*>. The converse inclusion is obvious. Therefore, A=UREA*T <I*>.

Now let m*y € A* and a E*r* << > or <*y>.* Then ä*ra* and *yra,* nence *xry* by the symmetry and the transitivity of *r*. Now by Lemma 1.7.6, it follows that r <>= *r <y*>. Hence the equivalence classes D A*/r* are pairwise disjoint. Therefore, *A/r € P*(A). .

*(ii*) It is easy to see that the relation rt is reflexive and symmetric. Now let *x, y, z* € A be such that *are y* and *Yr*rm. Then 3*i, je I* such that

*,Y* E Ai and *y,*z E Aj, henc*e y E*A O Aj, which implies that A2 == A. It follows that 1, 2 E Ai, hence *IT*72. Therefore, *r*m is transitive and consequently *my € E(A*).

(i*ii*) We will show that G*oF* = 15(A) and FoG= 1P(A). For every *r € E(A*), we have

....

..

**110**

.

..

a' = {{1,2}, {2,3},{4}}. Then r is a partition of A = {1,2,3,4), but ' is not. The equivalence relation corresponding to has the graph

*Rx* == {(1,1), (2, 2), (2, 3), (3, 2), (3, 3), (4,4)} (c) The congruence relation modulo *n* is an equivalence relation on Z and the corresponding partition is

*Z/Pn =* {*pn* <>l € Z} = {x + ri2/2 € Z} {2{ 2 € Z}, 12

**1**

..

..

.

.

.

*(GoF*)*(r) = G*(*A/r)=r*,

**2**

\*\*\*

28

.

*CHAPTER 1. RELATIO*N*S*

*1.8. FACTORIZATIO*N *OF FUNCTIO*NS

29

:

where an equivalence class is denoted by Î. For n > 2, we denote

\**\*\**\*

**1.8**

**Factorization of Functions**

-

Zn *= Z/n*Z = {0, Î, ..., n-1}.

Notice that for *n* = 0 and n-1 we get

*Z/po* ={{{z}} x € Z} and *Z/pı* = {Z},

The subject of this section is the following general problem: having an arbitrary function we would like to "factorize" it, that is, to write it as a composition of some other functions, that are called *factor*s*.* The motivation is that we might know few things on the initial function, but we can use the properties of its factors, that will be looked for to be injective or surjective functions. *Remark.* Notice the sünilar language as in the case of the factorization of a natural number in prime factors.

that are the two extreme partitions of Z.

We are going to see that we ma*y* associate an equivalence relation to every function and, viceversa, we may associate a function to every equivalence relation.

Composition of functions can be visualized in the so-called *commu tative diagrams*. If : A - *B* and *y: B aby C*, then *gof:A*- *C* makes sense and we may represent all these functions in a diagram of the following type:

**Definitio**n 1.7.12 Let *f*: A.-*B*. Then the homogeneous relation on

*A* with the graph

{(21,22) € AX Al*f(2*1) = *f(x*2)}

A\_

*B*

is called the *kernel* of f and is denoted by ker *s.*

*gof*

**Lemma 1**.7.13 *Let f: A* - *B. The*n ker *s E E(A*).

*Proof.* Left to the reader.

**Definition 1**.7.1*4* Let *ar € E(*A). Define *P*r : A

Such a diagram is referred to as a *commutative diagram.* That is because if we start with any element a € Á and we tracc it going along either of the two possible paths going from A t*o C,* we get the same result. Going right and then down we get *gif(a*)) and going diagonally we get (*gof*)*(a)*, which are the same.

We give now the first result on factorization of functions.

. *A/m* by

*Pr (2*) = *r <<* >, *V*E A.

Then *p*r is called the *natural projection.*

**Lennina 1**.8.1 *Every function can be written as a composition of an injection and a surjection.*

**Lemma 1**.7.15 *Let ir € E(*A). *Then the natural projection Pr* : A

A*/r is surjective and* ker p*r =r.*

→

*Proof.* The projection *p*r is clearly surjective. Now let x1,x2 E A. Using Lemma 1.7.6, we have

*Proof.* Let *f* : A - *B.* Also, let s : Am *f*(A) be defined by *s(a) = f(a), Va* e *A* and let *i : f*(A) *B* be the inclusion function, defined by *i(b) = b, Vb E F(*-4). Then clearly s is a surjection, i is an injection and

*f =j*os.

The following two theorems tell us when a function has a given sur jective or injective function as a factor.

\*1 (ker *pr*)22

*P*r (x1) *= pr*(22)

<31 >=*r <I*

>

*I*jr 22,

*C be surjective. Then*

hence ker *pr*

*t.*

Theorem 1.8.2 *Let f*: A - *B and let g:A*- B*h:0 - B such that f=hog iff k*erg C ker *s.*

.

i

.

*30*

*CHAPTER 1. RELATIO*N*S*

*1.8.*

*TION OF FU*N*CTIONS*

**1**

**TOV**

*If h does exist, then it is unique and h = f0s, where s : 0* - A *is a right inverse of g.*

si!

*Remark.* The theorem can be visualized in the following diagram, where the dashed arrow represents a function whose existence still need to be proved:

"

..

Notice that the arrows in this diagram are exactly the reversed arrows of the diagram in Theoren 1.8.2. *Proof. =* Assume that 3*h : B-C* such that *goh* Let *a € /(B*). Then 2*b € B* such that *i = f(b) = g(h(b*)), hence a *Eg(C*). Therefore, *f(B) Cg(0)*

B. Assume that *f(B) S 9(*C). Since g is injective, it has a left inverse, sa*y ?* : A-*C*, and we have *rog =* 10. Now choose *h =rof.* We need to prove that *go*ro*f= f*. Let *be B.* Then 3CE C such that

*$(6) = g*(c), hence we have

.

"

A*B*S

*gr((O*))) *= g(ro(*c))) = *g(*c) *= f(b)*.

*Proof.* Then

. Assume that *h:0 - B* such that *f=hog.* Let C1,C2EC.

Suppose now that *h*e does exist and let us prove its uniqueness. If there also exists *h' :B-C* such that *goh = goh',* we may simplify on the left hand side by the injection *g (*see Theorem 1.5.2) and we have *h = h'*

Theorem 1.8.4 *Letr € B*(A) an*d let f:* A - *B be such that r* 5 ker *s.*

"'"...

LYF

."

\*\*\*\*\*\*\*\*\*

*B*

A -

\*

..

......

Ci (ker g) *(41) = g(c*2) *h(90*1)) *= h(g(c*a)) =

*= f(0) = f(0*2) => ci(ker *f* )02, hence ke*rg* C ker *j.*

4. Assume that ker*g* C ker *f*. Since *g* is surjective, it has a right inverse, say *s:C*-A, and we have *gos*=1c. Now choose *h = fos.*

We need to show that *f = hog,* that is, *f*(*a) = (fos) (g(a)), Va* € A. For ever*y a* € A we have g(*a*) = *g(s(g(a*))), hence a (ker*g*)*(s(g(a)*)). Since ker*g* C ker *s*, it follows that a (ker )*(s(g(a*))), so that *f(a*) = *f((sog*)(a)). Consequently, J*h fos*:c*- B* such that *f =ħog.*

Suppose now that h does exist and let us prove its uniqueness. If there also exists *h':0 - B* such that *hog=f=hog,* we may simplify on the right hand side by the surjection g (see Theorem 1.5.3) and we have *h =h'.*

**Theorem 1**.8.3 *Let f:B + A and let g:0* - A *be injective. Then* 3*h: Bm C such that goh = f iff f(B) Sg(C*).

*Ifh does exist, then it is unique and h =q*o*f, where r*:*A*-*C is a left inverse of g. Remark.* The theorem can be visualized in the following diagram:

.

.

.

....

*Then:*

*(1)* 3!/: A*/p mot B such that the diagram is commutative, that is, js.* O*p = f, where p, is the natural projection.*

*(ii) If f is surjective, then for is surjective. (iii) If r* = ker *S, then fr is injective.*

.

.:

::

:: 6. W

::*.*

.

.

-

..

xr..

*Proof. (i*) By Lemma 1.7.15, *P*is surjective and ker *p*r. = my C ker*j.* Now by Theorem 1.8.2, there exists a unique *f*ri *A/ré B* such that *Š, OP, f*. Then *(r <a*>) = *f(a), Va* € A, hence *f*r is well-defined, in the sense that its definition does not depend on the choice of the representative in *r* <*a*>. This fact can be proved directly as follows:

.....

......

.

..

A<

*B*

*r<a>*=*r* <*a'* >= ae*r* c*a*

*ara*

T

WSwab

*=*

*a (*ker */) a'*

*f(a) = f(a*)

where *, c E* A.

-

*CHAPTER 1. RELATIONS*

*1.9. PARTIALLY ORDERED SETS*

Ww".

....

.

(*i*i) It follows by Corollary 1.5.6. *(iii*) Using Lemma 1.7.6 we have

*f*r (r <a>) = fr(r <a'>) *f(a) = f*(a') ==>

a(ker *f*)*a' ard'* =r<a >=r <a>, where *, a'* E A.

*Then:*

*(i)* 3*g : All'*1 any A*/ry surjection such that go Prı Prz, which is defined by*

*gr*i <*a*>) = rn <*a>, Va* E A. *(ui) 3!h : (A/*r1)/ ker *g --* A*/ra bijection such that h o P*ker*g = 9, which is defined by*

.'"\*7

ini

.

**Theorem**

**1**.8.5 *Let f*: A

*B.*

*h*((ker 9) *<1*1 <*a >*>) = 12 <*a>, Va E A*.

*Proof. (i)* Apply Theorem 1.8.4 for the natural projection Pr*ı*

(*ii)* Apply Theoren 1.8.4 for the natural projection Pker *o*.

***P*ke*r***

A*/* ke*r 5 -> $*(A*)*

1.9

Partially Ordered Sets

**i**

*Then there exists a unique bijection*

Recall that a relation r = (A, A, *R*) is called a *quasi-order* if it is reflexive and transitive and it is called a *partial order* if it is reflexive, transitive and antisymmetric. Let us give now the following definition.

*f : A/*ker *f -*

*f(A*)

**Definiti**on 1.9.1 A relation r = (A, A, *R*) is called a *total orde*r if it is a partial order and for every *a, b* E A, we have either *arb or bra.*

*such that the diagram is commutative, that is,*

*i*o *foPker 1 = f,*

*where i : j(4) Bis the inclusion function and P*k*ers*:A - A/ ker*f is the natural projection.*

*Proof.* Since ker *s E E(*A) and ker *P*ker f = ker *f*, we may apply Theorem 1.8.4. Then 3!*h* : *A/* ker*f - B* injection such that *h o P*ker *y = f.* We may write *h = į of* (see Lemma 1.8.1), where

*f(*(ker*s*)<*a*>) *= f(a), Va* € A.

Hence *f* is surjective. The injectivity of *f* follows also by Theorem 1.8.4. The uniqueness follows in the same way as in Theorems 1.8.3 and 1.8.2, since *i* is injective and Pker' f is surjective.

**Exampl**e 1.9.2 (a) The divisibility relation on N is a partial order, but not a total order. The divisibility relation on Z is a quasi-order, but not a partial order.

(b) The inequality relation on N, Z, Q or R is a total order..

(c) Let M be a set. Then the inclusion relation on the *power set P*(M) is a partial order. But if |M >2, then it is not a total order.

(d) The way of placing the words of a language in a dictionary defines a partial order "<" on the set W of all words of that language. It is defined by *w Sw*iff either *w* coincides with w' or *u* comes before *w*' in the dictionary. In fact, this relation is even a total order on W and it is called the *lexicographical order.*

Recall that we have denoted by *O(*A) the set of all partial orders on a set A. We have already seen methods of obtaining new partial orders, namely, ifr,s € *O(*A), then qe O(A) and ros e O(A) (see Corollaries 1.6.7 and 1.6.9). But it is also possible to obtain a partial order starting with a quasi-order. Recall now that if r is a quasi-order on A, then ro*pe E(A*) (see Theorem 1.7.2).

**Theorem 1**.8.6 *Let* ri,r2 *E E(A*) *be such that rı Sra.*

***P*ker *g***

A-3, A*/*11 Phers (A*/*r*ı)*/ker *g*

*Pr*a

V Ara

3*4*

*CHAPTER 1. RELATION*S

*1.9. PARTIALLY ORDERED SETS*

*35*

.

**Theorem 1.9.3** *Let r* = (A, A, *R) be a quasi-order and denote s* = ro*m. Then the relation p defined on A/s by*

..

<3*> os <y> A*rray *Dry.*

*is a partial order.*

*Remarks. (*1) If (A, <) is a poset (totally ordered set) and *B*C*A*, then *(B*, S) is again a poset (totally ordered set), where we have denoted by the same symbol the restriction of the relation " " to *B.*

(2) II (A, 5) is a poset and *a, b* E A we may have the following three possibilities:

(1) *ab*; (ii) *b <a*;

(iii) a and *b* are not comparable. In the case of a totally ordered set we may have only the first two situ ations.

!

In the sequel we give definitions of some remarkable elements in posets.

*Proof.* Every time when we have a definition on relation classes, it is necessary to show that the definition is independent of the choice of representatives. Thus, the first step of the proof is to prove that the relation is well-defined, that is, if n'es<> and *y' ES <y*>, then *$* < *>ps <1* >. Indeed, if x' E*S*< > and ye*s <y*>, then De *gout <<* > and y' E p *<y>,* hence c*'re* and *yry'.* But since we also have *wry*, it follows by the transitivity of r that *x' ry',* i.e., *$*<*>ps <y*>.

It is easy to check that p is reflexive and transitive using the fact that *r* has the same properties.

Finally, if *s* <2>*ps <y>* and *s <y> ps*< < >, then *xry* and *yra*, so that r*sy.* But since s *E E*(A), it follows by Lemma 1*.*7.6 that § << >=*<y>*. Thus, *p* is antisymmetric and consequently *p* is a partial order.

Definition 1.9,6 Let (A, 5) be a poset and a E A. Then a is called a:

(1*) least element* if

- *V*EE A, a 5*x.* (1') *greatest element* if

*Vr*e A, *a*

*2.*

(2) *minimal element* if

2 € A, I Sa=

\*=*a,*

Example 1.9.4 Let r be the divisibility relation on Z. Then by Exam ple 1.7.3, we have

2 (rn *7') y* = 12 = 1*3*1. Hence *Z/*T 7 *go*n) may be identified with N, so that *p* becomes the divis ibility relation on N, which is a partial order..

i.e., it does not exist any element less than a.

(2) *maximal element* if

I € A, 3 *> a. -*

*\** =

,

i.e., it does not exist any element greater than a.

In what follows, we will refer to pairs consisting of a set and a partial order defined on that set. Since the classical example of a partial order is the inequality relation" <" on numerical sets, we denote an arbitrary partial order by the same symbol " <". Naturally, we denote its inverse by the symbol " > ". We sometimes use the notation *a<b (or a > 0*) to denote the fact that *a sb* (o*r a > 0*) and *a \*b.*

*Remark.* The definitions (1), (1') and (2), (2') respectively are so-called

*dual* definitions, that are obtained one from the other by replacing the relations "S" and ">" one with the other. In the sequel, we will usually give results involving only one of the dual notions. The *dual r*esults hold as well.

**Definition 1**.9.5 Let A be a set.

If " 5 " is a partial order on A, then the pair (A, S) is called a *partially ordered set o*r simply a *poset.*

If” <” is a total order on A, then the pair (A, S) is called a *totally ordered set or* a *chain.*

**Theorem 1.**9.*7 Lei* (, 5) *be a poset.*

*(i) If there exists a least element in* A*, then it is the unique minimal element.*

*(ii) Let a* E A. *If either* A *is a finite set or* (*A*, ) *is a chain, then a is the least element iffa is the unique minimal clement.*

AP

36

*CHAPTER 1. REL*A*TIO*N*S*

*1.9. PARTIALLY ORDERED SET*S

*(5) refierivity and transitivity hold in Hasse diagrams. Remark.* Conversely, we may associate to each Hasse diagram its corre sponding poset. **Example 1**.9.9 Let A = {2,3,6,7,8,12, 18, 40,72) and let "|" be the divisibility relation on A. Then the Hasse diagram of the poset (A, I) is:

72

*Proof. (i*) Left to the reader.

*(ii)* Assume that *a* is the unique minimal element. Suppose first that *A* is finite. Let x € A. If x = 0*,* we are done, so that assume *2 #a.* Then we have three possibilities:

(1) *x* and a are not comparable; *(*2) a< *x;*

(3) *2* <*a* and we will prove that the first two cannot happen.

Take the case (1). Since I cannot be minimal, there exists 21 E A such that 21<x. Since x and a are not comparable, we have 21*+a,* so that there exists 22 E A such that x2 < 1 < *x.* Again 22 *\*a* and repeat the procedure to construct an infinite chain -1 < 22 < 21 < x, which contradicts the fact that A is finite. Hence this case is not possible.

Take now the case (2). Since a is minimal, we have 2 = 0*,* which is a contradiction.

Therefore, we must have & <*a.* Consequently, *a* is the least element. If (A, 5) is a chain, then the conclusion is immediate.

9

12

**Exampl**e 1.9.8 Let n be the relation defined on R by

*ary*

(x +*0+ y* and x S*y)* or (*x = y=*0),

Notice that there does not exist the least or the greatest element. The minimal elements are 2, 3 and 7 and the maximaal elements are *7*, 40 and 72, hence the element 7 is minimal and maximal in the same time.

where" < " is the usual inequality relation on R. Then O is the unique minimal (and also maximal) element of R, but there does not exist the

least (or the greatest) element.

At this point, we discuss an intuitive way of representing (finite) posets by some diagrams, usually called *Hasse diagrams.* In this way, it will be possible to "see" easier special elements in posets.

We associate to each (finite) poset its Hasse diagram by the following rules:

*Remark.* A poset may have no minimal (maximal) element, finitely many or even infinitely many minimal (maximal) elements. **Exampl**e 1.9.10 For instance, (Z, S) has no minimal dement, the poset in Example 1.9.9 has 3 minimal elements and (N\{1}, D) has as minimal elements all the prime numbers.

*(1) the elements of A are usually represented by dots (or by them selves or by both) and are placed on levels;*

*(2) comparable elements are placed on different levels, the least ele ment on an inferior level;*

*(3) two comparable elements a, b* € A *are connected by a line segment (usually called edge) iff there does not exist any C*E *A such that a <C<b or b<c<a;*

*(4) non-comparable elements are placed on the same or on different levels and are not connected;*

**Theorem** 1.9.11 *Let (4*, 5) *be a poset. Then the following statements are equivalent:*

*(1) Every non-empty subset of A has at least one minimal element; (ii) If the following conditions hold for B*CA:

*(1) B contains all minimal elements of A,*

*(2) a € A and 2* EA <a C*B O E B; then B* = A;

*(231) Every strictly decreasing sequence*

| *3*1 > 0) > > *n* > ... *of elements of A is finite.*

--.

38

*CHAPTER 1. RELATIO*N*S*

*1.10. LATTICES AND ALGEBRAS*

.. .--.

.

*Proof.* Apply Theorem 1.9.11 for (N) (0,1}, D. Take *B* to be the set of all elements in N\{0,1} having a decomposition in prime numbers. Then 2 € *B.* Moreover, if *a* € N and every factor of a has a decomposition in prime numbers, then clearly *a* has one. Now by Theorem 1.9.11, *B* == N.

*Remark.* The three conditions given above are called the m*inimality condition*, the *inductivity condition* and the *strictly decreasing sequences condition* respectively. *Proof. (*i) *(*ii) Assume (i). Let *B* C A be such that the conditions *(*1) and (2) hold. Suppose that *B \** A. Then A *B* has a minimal element, sa*y a.* By *(*1), *a* is not minimal in *A*. Now if I E A and I <*a,* then we must have I E *B* (otherwise E *A B, <a* and a minimal in A *B* imply \* =*a,* a contradiction). Then by (2), we have *a EB,* which is a contradiction. Hence (*71*) holds.

*(ii)* = *(iii)* Assume (*ii)*. Let B be the set of all elements a E A such that any strictly decreasing sequence starting with a is finite. Then the conditions (1) and (2) hold for *B*, henc*e B --* A. Therefore, (*111)* holds.

Definition 1.9.14 A poset (A, S) is called *well-ordered* if every non empty subset of A has a least element.

**Example 1.9.1**5 The poset (N, S) is well-ordered, whereas (Z, <), . (Q,5), (R, 5), (N, 1) and *(P(*M*)*, 5) (for some set M with M > 2) are not.

**+**

*Remark.* Since any least element is minimal, Theoren 1.9.11 allows us to use the induction principle for well-ordered sets. In this case, we call it t*ransfinite induction.*

**?**

**t**

**.**

*(iii*) => *(i*) Assume *(iii)*. Suppose that there exists a non-einpty subset *B* of A having no minimal element. Let bi E *B.* Since *b*y is not minimal, there exists *b2 E B, 62 < 6*1. Now repeat the argument to obtain an infinite strictly decreasing sequence *bi > 02* >..., which is a contradiction. Hence *(*i) holds.

Theorem 1.9.16 *(1) Every well-ordered set is totally ordered.*

*(ii) Every totally ordered set satisfying the minimaliły condition is well-ordered.*

..

...

..---

-

-

----

---.

**Corollary** 1.9.12 (The noetherian induction) *Let B*CN *be such that:*

*(1) OEB;*

*(2) a* EN *and {{* EN <a} C *B aE B; then B*N.

*Proof. (1*) Let (A, S) be a well-ordered set and let *1,4€ A*. By hypoth esis, the set {x,*y*} has a least element, so that we have either x S*y o*r *y St*. Hence (.A, 5) is totally ordered.

*(ii*) It follows by Theorem 1.9.7.*.*

.

"

""

!

!

"

,

**Exampl**e 1.9.17 We have just seen that the posets (Z, 5), (Q, S) and (R, S) are not well-ordered. But clearly they are totally ordered.

"W

".

.

*Proof.* Apply Theorem 1.9.11 for (N, S). *Remark.* Usually, we would like to prove that a given property depending on a natural number holds for every natural number. Then we denote by *B* the set of all natural numbers satisfying that property, then verify (1) and (2) and finally, conclude that *B*=N. It can be shown that the result is still valid even if a weaker condition than (2) holds, namely

.

ponad

An important result in Set Theory, whose proof will be omitted, is the following one:

-

.

..

-

**Theorem 1**.9.18 *(*Zermelo, The Well-Orderin*g* Principle) *Every set can be well-ordered.*

-

*(2'*) a € A, *a* -1*EB*

*QEB.*

This is the case of the classical *(complete) induction principle.*

1.10

Lattices and Algebras

**Theorem 1**.9.13 (The Fundamental Theorem of Arithmetics) *Every natural number n* EN(0,1} *has a decomposition in prime numbers, unique up to a factor rearranging.*

This section deals with lattices, that are some special partially ordered sets. We need first some basic preliminary definitions.

ko

COBR*A*

**4**

**.**

40

*CHAPTER 1. RELATIO*NS

41

Let us now see if the classical posets are complete) lattices or not.

**Definition 1.1**0.1 Let (4,5) be a poset*, B*C A and a € A. Then *a* is called a:

*(*1) *lower bound* for *B* if

**Examp**le 1.10.3 *(a*) (N, 5), (Z, S), (QS) and (R, S) are lattices, but not complete lattices. More generally, every totally ordered set is a lattice.

*a sb, VbE B.*

(1'*) upper bound f*or *B* if

*a>b, WEB.*

*(2) greatest lower bound (9.1.b,* in short) for *B i*f a is a lower bound or *B* and *a > a'* for any lower bound *a'* for *B.*

(2') *least upper bound (l.u.b.* in short for *B* if a is an upper bound *or B* and *a sd* for any upper bound *a'* f*or B.*

Ne

V*otation.* We denote a g.l.b. for *B*CA by infA*B* or simply by inf *B* vben A is clear. We denote a l.u.b. for *B*CA by supA*B* or simply by

up *B* when A is clear. *Remark.* For a E A, we have:

Indeed, for any elements *a, b*, there exist

inf(x, *y*) = min(*x, y)* and sup(x,*y) = m*ax(*2,y).* But for instance, there does not exist sup N, bence (N, S) is not a com plete lattice.

*(b*) (N, ) is a complete lattice, Indeed, for any elements I*, y*EN, there exist

inf(*x, y) = (x, y)* and sup(*, y) =* 1*2,4),* where (c, *y*) and (*x*,*y*) denote respectively the greatest coromon divisor and the least common multiple of u and *y.*

Moreover, for any subset *B*, there exist inf *B* and sup *B. If B* is finite, they are the greatest common divisor and the least common multiple respectively, whereas if *B* is infinite, they are 1 and 0 respectively,

(c) *(P*(M), S) (for some set M) is a complete lattice. Indeed, for any 4,*BCM*, there exist

inf(A*, B)* = An *B* and sup(A*, B*) = AU*B.* Moreover, if (Ailier is a family of subsets of M, then there exist

inf(Ailie*r* = n A, and sup(Ajdier = UA.

*iel*

*j*e*r Remark.* In general, a latlice (4, 5) might have or not the least element, usually denoted by 0, or the greatest element, ueually denoted by 1 (see Example 1.10.3). But if they do exist, then infA A = 0, supa A = 1, infA0 = 1 and supAO = 0 (one can check them by the remark on page

(*i*) as*b, WEB* (ii) a' E A, *a' Sb, WEB-asa*

infA*B=2*4

supĄ*B =*

J(i) a*>0, WEB*

(*ii) a*' € A, a*'>b, Vb E B*

*a*

*' >a*

R*emark.* The greatest lower bound and the least upper bound are inique, if they do exist. This happens for any elements in special posets alled *(complete) lattices.*

**Definitio**n 1.10.2 A poset (*A*, <) is called a:

(1*) lattice* if for ever*y r, ye* A,

Finfa (x, y) and 3supa (*,y).*

40).

**Theorem 1**.10.4 *Every finite lattice is complete.*

!

n this case, infA *(x,y*) is called the *meet* of a and *b* and supa (*x, y*) is alled the *join* of a and *b*.

(2*) complete lattic*e if for every *B*CA,

infa *B* and supa *B.*

*Proof.* By the induction principle.

Actually, in order to prove that a lattice is complete it suffices to check a weaker condition, as we can see in the following result.

42

*CHAPTER 1. RELATIO*N*S*

*1.10. LATTICE*S A*ND ALGEBRAS*

43

- .

..

**Theorem** 1.10.5 *A lattice* (A, S) *is complete iff* Sinf *B, VB* S A *iff* 3 sup *B, VB* C A... :

**Definition 1.10.8** Let A be a set and n E N. By an *n-ary operation* on A we understand à map

6: An = *A*X-.XA - *A*.

Tu times

For *n* == 0,1,2,3, ... we get *a pullary, unary, binary, ternary* operation and so on.

*Proof.* We prove the non-obvious part of the first equivalence.

Let *B* C A. Denote by the set of all upper bounds for *B* in A, that is,

C={CE AV*EB, b*e}. Since infØ *EC,* we have *C +* 0*.*

Let a = inf*C.* We will show that a = sup *B.*

For ever*y b E B* and for every cE*C*, we have *b* <c, whence it follows that for every *b E B,* we have *b* <a, that is, a is an upper bound for *B.* Now let a' E A be an upper bound for *B.* Then a' e C, hence a <*a*

Thus, a is the least upper bound for *B* and consequently, *a* = sup *B*. o

*Remark*. See the remark on page 13 for the case n = 0.

Example 1.10.9 Examples of nullary, unary and binary operations are respectively: picking an element of set, associating the opposite of an integer, the sum of two natural numbers.

\* :

At this point, let us see what happens when we take a subset of a (complete) lattice. Is it still a (complete) lattice? The answer is negative in general, but positive for the so-called *(complete) sublattices.*

**Definitio**n 1.10.10 By a *universal algebra* (or simply *algebra*) we un derstand a set 4 together with some *n-*ary operations *(n*. E N*)* on A.

Let (*L*, S) be a lattice. Since for every *x,y EL,* 3 inf(x,*y*) and 3 sup(*x,y),* we may define two binary operations A, V*:LXL-L* by

**Definition 1.10**.6 Let (*A*, 5) be a lattice and let *B* C A. Then *B* is called a:

(1*) sublattice* of A if

I A*y*=inf(x, *y),*

*IVY* = sup(x*, y).* Then (*L,* A, V) is an algebra with two binary operations.

infA (*X,Y) E B* and sups (*V,y) EB, VE, Y EB.*

Moreover, if (*A*, S) is a complete lattice, then *B* is called a.

(2*) complete sublattice* of A if

infĄ *C E B* and supA*CEB, VCCB.*

**Theorem 1**.10.11 *Let (L*, S) *be a lattice and consider the two opera tions* A *and V defined as above. Then:*

*(1) IA(Y*A*Z)* = (*x Ay) Az,*

*IVY V* z) = *(1 Vy)* V2*, VX, Y, Z EL; (associative laws) (ii) 2 AY=y^x*,

*I Vy=Y VE, VI,Y EL; (commutative laus) (iii) x* A (*2V y) = x*,

*IV (*A*y) = 2, Vä, Y EL. (absorption laws)*

**Exampl**e 1.10.7 (a) Every subset of (N, 5), (Z, 5), (Q, S) or (R, S) is a sublattice.

*(6*) The set 2N = {2n | 7 € N} is a complete sublattice of (N, ). (C) Let N *C*M. Then *P(N*) is a complete sublattice of *(P(*M), 5).

*(d)* The set *B* = {1,2,3} S N is not a sublattice of (N, D), because, for instance, we have sup(2, 3) = (2, 3) = 6€ *B.*

*Proof.* We prove only the properties for ^, the others following by dual

ity.

*(i*) Denote a = *2*^ (*y*^ z) and *b =* (2 A*y)* A z. Then we have:

We are going to see that every lattice determines two operations and a structure called *algebra* and viceversa.

a <3 and *a <y* A*Z*

*A*

*5\*, <y* and a < 2

*CH*A*PTER 1. RELATIONS*

parsel

*1.11. ORDER* A*ND LATTICE HO*M*OMORPHISMS*

**V**

a < (a A*y*) and a <zua <(x A*y)* 17*,* hence *a sb*. Similarly, we get *b Sa*, so that *a = d.*

(*ii*) It is imrnediate by the definition. ,

*(222)* Denote c = \*^ ( *Vy*). Then c<x. On the other hand, 2 S*I* and : 5*.2 Vy,* hence *& SI*A (CV *y) =*c. Therefore, c=.

A converse of Theorem 1.10.11 holds as well, that is, we may associate a lattice to any algebra with two binary operations satisfying the laws in Theorem 1.10.11.

Let *2,4 € L* be such that I *<y* and *y < 2*. Then I V *y = y* and *YVES X*, whence x *= y.* Therefore, the relation is antisymmetric and consequently it is a partial order.

Let us now show that (*L,*<) is a lattice, and more precisely, that *V2,Y E L* we have

sup(x, *y) = IVY* First, by absorption and reflexivity we have

*X*V (*vy) = (x V 2) Vy=xVY,*

**Theorem 1**.10.12 *Let (L,*1,V) *be an algebra with two binary opera tions satisfying the associative laws, the commutative laws and the ab. sorption laws. Define a relation"* <” *on L by*

hence *<* < *\*Vy.* Similarly, we get *y S&Vy.*

Secondly, if I 5 z and y <%, then I V *z*=z and *y Vz*=z. We have

z = IV*2= IVY V z*) = *(*V*y) 17,*

*y*

*Ay=0*

*or equivalently by*

*2*

*y*

*3 Vy=y.*

*Then (L,* 5) i*s a lattice, where Vx, Y EL we have*

inf(*x, y) = x^y*

*and*

sup(x*, y) = IVý.*

*Proof.* For every *x, y € L,* we have by absorption and commutativity:

hence *x vy S*z.

Therefore, sup(*x,y) = x Vy, WI, Y EL.*

Consequently, *(L,* S) is a lattice. *Remarks. (*1) One can prove that:

*(1)* if we start with a lattice, apply Theorem 1.10.11 and then apply Theorem 1.10.12, then we get the initial lattice.

*(ii)* if we start with an algebra with two binary operations satisfying the associative laws, the commutative laws and the absorption laws, apply Theorem 1.10.12 and then apply Theorem 1.10.11, then we get the initial algebra.

(2) In what follows, we will see a lattice both as a poset and as an algebra with the two binary operations A and V. And from now on, we will usually denote

*T /A g = 1*

*+ 3y = g /* (*x y) = 4 V T - TV 4*

|

and also

*c V 4 =* ***g ==> T*** *= z /* (*+ y) = a f g .*

Consequently, a A*y=xHxVy=y.*

We prove now that " <” is a partial order on *L.* For every *2 EL,* we have by absorption

A*y=*inf*(*x*, y*) and *Vy =* sup(*x,y).*

.

*& V&=xV2*A *(@*VI) =*,*

**A**

1.11 Order and Lattice Homomorphisms

hence I <3, i.e., the relation is reflexive.

Let *1, Y, Z* E *I* be such that I <*y* and *y* < 2. Then *& Vy=y* and *Y V* 2 . It follows that

In this section we will discuss some special maps between posets and lat tices respectively. In order to simplify the notation, we will use somehow abusively the same symbol for partial orders on different sets.

*\*V2*=V*Y V* z) = (*IVY) VZ=y V2* = 2,

hence I <. Therefore, the relation is transitive.

**Definition** 1.111 Let (A,) and *(B*, S) be posets. Then a map *| :*

*A* - *B* is called an:

AV

**n**

*46*

*L*AT

4

**lause**

.

.-vr

..

(1) *order homomorphism (*or a *poset homomorphism* or an *increasing...:*:1. *map)* if

*X,Y E*A, *I Sy= f*(*x*) <*f(y). (*2*) order isomorphisın (*or a *poset isomorphism*) if f is bijective and both *f* and *f-*l are order homomorphisms.

....

*Remark.* We have seen that in the definition of an order isomorphism we have requested that the inverse is again an order homomorphism (see Definition 1.11.1). The next theorem on lattice isomorphisms shows us that the similar condition on the inverse is a consequence of the other two conditions.

.........

.......

*B.*

**Theorem 1**.11.5 *Let (*4, 5) *and (BS*) *be lattices and let f* : A - *B be a lattice isomorphism. Then f-1:B - A is a lattice tsomorphism.*

**Lemma 1.1**1.2 *Let* (A,) *and (B,* 5) *be posets and let f : A* = *Then f is an order isomorphism iff*

*(i) f is bijective; (ii) for every X, Y E* A, & S*y f (x) = f(y).*

\*\*

"'

*Proof.* Clearly, *f*-1 is bijective. Now let *bi, ta €* 14, Since *f* is surjective, there exist *21,*€ A such that *f*(aj) = *6*1 and *faz) = 62*. Then

.-

..

.

.

**نم**

.

.

*Proof.* Left to the reader.

Emipanning

.

.

...

.. Antylori

.....

.

**Exampl**e 1.11.3 (a) Let r = (A*, B, R)* be a relation and let *F : P(A)* - *P(B)* be defined by *F(*X) = f(x), VX E *P(*A). Then *F* is an order homomorphism between the posets (*P*(A), S) and *(P(B)*, 5).

*(6*) Let A = {*x,y*} and *D =* {1,2,3,6). Define *f:D - P(A*) by *f(*1) = 0*, $(*2*)* = {x}, *f(*3) = *{y*} and *f*(6) = A. Then *f* is an order isomorphism between the posets (*D*, ) and (P(A), 5). . (c) The identity map IN is clearly bijective and an order homomor

phism between the posets (N, 1) and (N, S), but 18 = 1n is not an order homomorphism between (N, <) and (N, 1).

*f(aj 1a2) = f(01) Af(az) (/(aj AQ*2)) *= f'(*(*ai)*^*f(a*2))

s *aj 102 = $-1(61 A bz) F-'(h*z) *^ f-(62) = x-1(b1 Aba)*. Similarly, the dual property holds. Therefore, *f-* is a lattice issomor phism.

Let us now see the connection between order bom*o*morphisms and lattice bomomorphisms.

Theorem 1.11.6 *Let* (A, S*) and (B*, 5) *he lattices and f :* A + *B. Then:*

*(1) I f is a lattice homomorphism, then f is an order homomorphism. (ii) f is an order isomorphism iff f is a lattice isomorphism.*

... ...

\*-\*

.

.

.

.

*Proof (2*) Notice that for every *I, Y* € A,

..

......

.....

<*y*

*=&par*ente e *I VY=y.*

..

*Remark.* By Example 1.11.3 (c), it follows that the condition on the inverse to be also an order homomorphism is essential in the definition of an order isomorphism.

Let us now consider the case of lattices. Recall that we have denoted *Ay =* inf*(x, y*) and X*V y =* sup(x, *y*). By the usual convention, we wil use the same symbols A and V even in different lattices.

...

ira-

Now let 2,*4 €* A. Since f is a lattice homomorphism, we have

sewwi!

*2*

*y =*

*Ay =* I*=*

*f(AY) = f*(x).

"

**Definiti**on 1.11.4 Let (*A*, S) and (*B*, S) be lattices. Then *f* : A - *B* is called a:

(1*) lattice homomorphism* if V*r, y* E A we have

........

....

=> *[(x) A f(y) = y(x) = f(z) </(y).* The dual property follows similarly. Thus, *f* is an order homomorphism. ol (ii) By Theorem 1.11.5 and by (i), if f is a lattice isomorphism, then

*f* is an order isomorphism.

Conversely, suppose that *f* is an order isomorphism. Then *f* is bijec tive and both *f*and *f*-1 are order homomorphisms. Now let *y, y* € A. We will show that

*f(x Ay) = f(3*) A*f(y),*

.

.

.

....

*f(2* A*y) = f() A f(y),*

*f(XVY) = f(x) V f(y). (*2) *lattice isomorphism* if *f* is a bijective lattice homomorphism.

.

*.-*..

-

4.

v

*1.12. BOOLE LATTICE*S *A*N*D BOOLE* A*LGEBR*AS

49

48

*CHAPTER 1. RELATIO*NS

· WA

proving that *f(B*A*Y*) is the greatest lower bound for *f(x*) and *f*(*y*), that

is,

(1) *f(x Ay*) S*f*() and *f* (*x Ay) S f(y*); *(2) b E B, b<f(c*) and *b f(y) = f(x Ay*).

But (1) holds, since *z Ay* SX, *Ay Sy* and *f* is an order homo morphism. Assume further that b *E B, b = f*(x) and *b < f(y*). Since *s* is surjective, 3*a* E A such that *f(a) - b*. Then *f(a) = f(2*) and *f(a) f(y)*, whence *a* <x and *a <y*, so that a <*3 Ay.* Since *f* is an order homomorphism, it follows that *b= f*(*a) f*(A*y).*

Similarly, the dual condition holds. Therefore, is a lattice homo morphism, that concludes the proof.

**Example 1.12**.3 *(a*) Let M be a set. Then *(P(M*), ) is a Boole lattice and *(P*(M), n, U,*D, M,CM*) is a Boole algebra, where the least element is 0, the greatest element is M and a complement of A C M is the set-theoretic complementation CM*A*. mo*k (6*) The only chains that are Boole lattices are those having at most two elements. A*l*

(c) Let M be a set. For every NCM, let

X*N* : M - (0,1}, XN(x) =

if 3 EN 10 if EMIN

be the *characteristic function* of *N*. Recall tbat we denote (0,11M =

{*f*l*f:M* - (0,1}} (see page 13). Then

Example 1.11.7 There exist order homomorphisms that are not lattice homomorphismus. For instance, let r = (*A, B, R*) be a relation and let *F:P(*A) - *P(B*) be defined by *F*(X) = r(X), *VX E P*A). Then *F* is an order homomorphism, but not a lattice homomorphism, since in general we have *r*XnYr(X) nr(Y).

{0,1}M = {XN I*N* CM}

We define a partial order on {0,1M by

XA SXB AC*B. N:*

1.12 Boole Lattices and Boole Algebras

**.**

Then ({0,1}M, 5) is even a lattice, where for every *VA, BCM,*

**1**

XA AX*B* == XAN*B,*

We are going to introduce now a type of lattice that plays an important part in Computer Science.

**1**

XAVX*B* = XAU*B*. Moreover, ({0,1}M, S) is a Boole lattice, where the least element is Xb, the greatest element is XM and the complement of any XA is X*C*MA.

Definition 1.12.1 A lattice *(B*,) is called a *Boole lattice* (or *a booleun*

*lattic*e) if:

(a) *Wax, y, z EB, 2*A *(Y V* z) = (*x Ay) V*(x Az) (*distributive law)* (or equivalently *I VY* A ) = *(2* V*y) A* (2 V 2));

(b) *B* has the least element and the greatest element, denoted by 0 and 1 respectively;

(c) For every x € *B*, there exists I *e B,* called a *compleme*n*t* of ?, such that

*I*AI=0, IV*E*=1.

**Theorem** 1.12.4 *Let (B, S) be a Boole lattice and let (B,*A, *V*,0,1,1 *be its associated Boole algebra. Then:*

*(1) Every IEB has a unique complement; (ii)* 0 = 1 *and* 1 = 0; *(212) 3 = x,* V*x € B; (iv) 2 AY=VY,*

*EVY - TAY, VX, Y EB (De Morgan laws); (V) I SyÝ S*E*, VE,YE B.*

**Definition 1**.12.2 If we see a Boole lattice *(B*S) as an algebra *(B,*A, V,0,1,), where A and *V* are the binary operations induced by *inf.* and *sup,* 0 and 1 are nullary operations and - is the unary op eration of taking a complement, then it is called a *Boole algebra* (or a *boolean algebra).*

*Proof. (i)* Let 2 € *B* and assume *x* has two complements 21,2*2 E B.* Then x A*2*] = 0, *XVI*1 = 1, *x* A x2 = 0 and x *V x*2 = 1. It follows that

*X*1 = *2*111 = *%*11(x*V2*2) = (211*I) V(X*1122) = OV(211x2) = x112,

*CHAPTER 1. RELATIONS*

*1.12. BOOLE LATTICES* A*ND BOOLE* A*LGEBR*AS

51

Definition 1.12*.7* Let (*B,* 5) be a Boole lattice. An element *a € B* is called an *atom* if *a* 40 and

hence 21 522. Similarly we get x2 < xi and consequently 2] = *22*..

(ii) Clear.m e (*iii*) VE*EB* we have č A*r* = 0 and @V I = 1, hence z = I. *(iv*) Let us prove that *Vx, y EB, XAY = IVY*, that is, to show that

*(XAY)* A (A*VT*) = 0 and *(x Ay) V* (X*V y)*=1.

0<r<

I*=0,*

that is, a is a minimal element in *(B*\ {0}, 5).

Lemma 1.12.8 *Let (B,* S) *be a Boole lattice, let a E B be an atom and let 2, Y E B. If a SVy, then a* S*I or a Sy.*

*Proof.* We have

We have

*(AY)* A *(@V y) = (r* A *Y A2*) V *(@*A*Y AY) -*

*= (y4*0) V (

20) = OVO = 0, *(*\* A*y) V (@V 7) =*= (*VäVÝ) A (YVÈVT) =*

== (1 *VT) A* (TV 1) = 1 A1=1. *(1*) Using De Morgan laws, V*I, y € B*, we have

*a Sævy*

*a = a 1* (X*VY) = (a* A*x) V (a A y) =*=

A2 S*a* and *a Ay <a.*

Since a is an atom, we must have *a* 1*x = a o*r *a Ay = a*., that is, a <*3* or *a <y.*

. *. <y=*

*&AY= ?*

*AY= Í*

*I VÝ=i*

*Y*

*<*

*.*

Now we are able to characterize the finite Boole algebras.

We can define a special homomorphism between Boole lattices.

**Theorem** 1.12.9 *Let B be a finite Boole algebra and let A be the set of all atoms in B. Then there exists a Boole isomorphism between B and P(A*).

*Proof.* For every , E *B*, denote AT) = {a e Ala <3}. Now define

Definition 1.12.5 Let (*B*S) and *(B',* <) be Boole lattices. Then the map *f:BB* is called a *Boole homomorphism* if f is a lattice homo morphism and

*f(x) = f*(2), VI*EB.* The map *f* is called a *Boole isomorphism* if it is a bijective Boole homo morphism.

*F:B-*

*P(*4)

by

*F*(x) = A(I), V*I E B*

*.*

Let a € A and 2*, y € B.* We have

*a* € A2 A*y)*

<A*Y SI*SI and a S*ya* € A(x) n A*(Y),*

*Remark.* If*f:B-B*is a Boole homomorphism, then cicarly *f(0*) = 0 and f(1) = 1', that is, it takes the least and the greatest element of *B* to the least and the greatest element of *B'* respectively.

so that

*F(RAY) = F*(x) *F(y*). Since *a* is an atom, it follows by Lemina 1.12.8 that

*Q*E A(*XVY) Sao Vya* Sic or *a Sya*e AX) U A*Y*),

Example 1.12.6 (a) Let M be a set and let *F:P(*M) +0,11M be defined by *F(N*) = XN*, VN EP(M*). Then *F* is a Boole isomorphism (also see Example 1.12.3 (c)). .

*(6*) Let M *+*0 be a set and let N CM. Let *S : P(N*) *- P(*M) be defined by *f(A*) = A, VA E *P*(N). Then *f* is a lattice homomorphism, but not a Boole homomorphism, since the image of the greatest element N of *P(*N) is not the greatest element M of *P(*M) *(s*ee the previous remark)

so that

*F3 Vy) = F(*P) U *Fy).*

**NA**

Also

*a* E AD

TOTECA FA*GUI*

<a hr*ana* CLUB-VAPOCA

*O* E *A*

*A*()

52

*CH*A*PTER 1. RELATIONS*

CEN

Indeed, if a <*ī* and we suppose that *a* <a, then *a* S*I*A E = 0, which is a contradiction. Conversely, if *a* X X, since we have *a* < 1= x V I, it follows by Leinma 1.12.8 that a <i.

Consequently,

*F(a) = F(X*)

and thus *F* is a Boole homomorphism.

In order to prove the injectivity of *F,* we need to show first that every element of a can be written as a (finite) join of atoms. For let & *EB,* denote the elements of Ax) by al,*..., O*ne and take

*t=a1* V.*.. V b.gr*

n

**i**

1.13 Homogeneous Relations vs Bivalent

Matrices

e

w

!

..

...

.

.

.

.

.

---

-

**.**

**M**

e

Since each *od* 5\*, we have *t I*. Suppose that *t +* . Then *2 +*0, because otherwise, we also have 1 = *tVE* <*3 VË,* whence *z VI* = 1 and thus, a ' *t* (by the uniqueness of the complement), which is a contradiction. Let a S*E*A*T* be an atom. Then a € A(x) = {@1, ..., *d*ige}, whence *a <t*. It follows that a *= a* A*t S AĞAt = 0*, which is a contradiction. Thus, & *t=91 V*... V *an.*

Now let *2,Y E B* be such that *F(X) = F(y)*, i.e., *A*(2) *A*l*y*). Write *2 = a1 V... Van* as a join of finitely many atoms *ai 5 2*. Then each *di* E A(I) = *A(y*), hence each *ai Sy.* It follows that *I <y*. Similarly, we get *y* < x, so that x *= y.* Thus, *F* is injective.

Let *CE P*(4), say C = {(1, ...,Ck, and denote 2 = c *V...Voki* Clearly, *CCFE*) = A(x). On the other hand, if a *E F(x*) = A(Q), then *a* <x=c1 V..*. V ok*. By Lemma 1.12.8, it follows that a sci for some *i* € {1,...*, k*}. Then a = c*i E C*. Hence *F(x)* C*C*, so that *F*(x) = *C.* Thus, F is surjective.

Consequently, *F* is a Boole isomorphism.

• O *Remark.* If *B* is an infinite Boole algebra, it is not always possible to establish a Boole isomorphism between *B* and some power set *P*(M), but it can be proved that *B*-is Boole isomorphic to a Boole "subalgebra” of some power set *P(M*).

**ALARI**

Throughout this section A = {*Q*1*, ..*., Dog will be a finite set and *R*(A) will denote the set of all homogeneous relations on A..

Recall that we have defined the intersection, the union, the compo sition and the inverse of relations and we have denoted by o the void relation, by u the universal relation, by the equality relation and by the complement of a relation on A.

Then *(R*(*A*), n, 0,0,*0,4,8,*9,-) is an algebra, with 3 binary opera tions (the first three), 3 nullary operations (the next three) and 2 unary operations (the last two) (see Definitions 1.10.8 and 1.10.10). *Remark.* For the purpose of this section we are going to define the multiplication "\*" of relations by T \*s=sor.

Theorem *11*13.1 *(R(*A), nu,*0,0,*") i*s a Boole algebra, isomorphic to the Boole algebra (P*(A2), O, U,0, Aa, *CA) through F : R*(A) - *P*(A4) *defined by*

*F(r)= R, Vr* = (A, A, *R*) E R(A). *That is, F is a bajection and F*ros) = *F(T*) n *F(s), F(*TUS) = *F*(r) U*F(s), F(0) = 0, F(u)* = AP, *F(7*) = *C*A*PR, for every 7, S ER*(4).

**Corollar**y 1.12.10 *The number of elements of a finite Boole algebra B is of the form 2*n*, where n is the number of atoms in B.*

*Proof.* Notice first that *R*(A) and *P(*A2) have the same number of ele ments, that is, \R(A) = *P*(A) = 2(n“). Clearl*y, F* is a bijection. Re call that (*P(*42), , 0, 0, *A*2, CA2*)* is a Boole algebra by Example 1.12.3. It is easy to see that *f* satisfies the properties of an isomorphism. Con sequently, (R(4), O, U, *0, 4*, ) is a Boole algebra.

**Example** 1.12.11 Here we give the Hasse diagrams of the four non isomorphic Boole lattices with at most 15 elements.

54

*CHAPTER 1. RELATIONS*

*1.13. HOMOGENEOUS RELATIONS* V*S BIVALE*N*T* MA*TRICE*S 55

**Pand**

*(@j*) *(b*ij) = *(*cin), where Caj = V-1 (*cik Abki*),

*Remark. (R(*A), n, U) is an algebra with two binary operations n and U satisfying the associative laws, the commutative laws and the absorption laws (see also Theorem 1.13.1). Hence by Theorem 1.10.12, *(R*(*A*), S) ; is a lattice, where inf(r, s) = rns and sup(r; s) = ? U*s, V*r*, s* E*R(*A). .

We intend to establish an isomorphism between the algebra *R*(A) of homogeneous relations on a finite set A and an algebra of some matrices, that will allow us to compute easier operations on relations and to read **easi**er their properties.

In what follows, let V = 0,1). Let us endow the set V with an algebra structure, by defining the binary operations A,V:VXV-V and the unary operation : V-V by

(Gra*y)* = (@ij),

(Arij)\* = *(*aji*)*. Then (M,(V), A, V, 0, 0m, 19.*, In*,";) is an algebra. But we have even a stronger result.

**Theorem** 1.13.3 (Mn(V), A, V, Ore, 1.org ) *is a Boole algebra.*

*Proof.* By the definition of the operations, the distributive law and the property of the complement in Mn(V) reduce to the initial properties in

*\*Ay =* rin(x*,y*),

Theorem 1.13.4 *Consider*

*\* Vy =* max(*x,y),* 0=1, 1-0.

*$:R*(A) - M (V), *f(n*) = M*, ,*

*where the bivalent matrix* Mr *= (avij*) *is defined by*

**Theorem**

**1**.13.2 (V, A, V,0,1,-) *is a Boole algebra..*

*Change* = 14

*listi Qig.*

*Then f is an isomorphisın between the algebra*

*(*R(A), O, U, \*, *0,,8,*,-)

*Proof.* Left to the reader.

Let us now consider the set Mn(V) o*f bivalent matrices*, that is, matrices with entries only 0 and 1. Since any matrix *BE* M,(V) is in fact a map

*B*:{1,..., *n*} x {1,..., *n*} - V, it follows that the number of elements of Mn(V) is the number of func tions of the previous form, that is, Mg(V)] = 2 (na) (see Theorem 1.4.4).

We would like now to" transfer" the algebra structure of V to M,(V). For make the following notations of matrices in My(V):

*of homogeneous relations and the algebra*

(M,(V), A, *V*,0,0,0,1.97.,1927.,)

*of bivalent matrices.*

*That is, f is a bijection and*

On = *(@j*j), where *C*orting = 0, *Vij* E {1,..., ni}, | 1= *(*ai)), where dj = 1, *Vi, j* c{1,..., n},

*I*n = (*aij)*, where *dij*=16 *i*=*j.* Now define on Mn(V) three binary operations A, V and O and two binary operations - and t by

*f(7* 778) = *f*(r) A *f(s), I*(TU 8) *= f*(r) V f(*s)*,

*$(\*\*) = f*(r) o *f(s), f(*0) == On*f*(*u*) = In, *(8) = In ;*

$(7) = *f*("*), 5(72*) = *f*(r)', *for every r, S E R*(A).

(Q*ij)* ^ *(bij) = (aij Abaj),* (*Chij) V (bij*) = *(*@h*ij v bij)*,

56

*CHAPTER 1. RELATIONS*

*1.13. HOMOGENEOUS RELATIONS V*S *B*IV*ALENT MATRICES57*

V*AL*

IS

*Proof.* Clearly *f* is a bijection. By direct computation we get

*Proof.* Left to the reader.

\*\*\*\* \*\*\*\*\*\*

Mrris *= My* A M*g*, Mrus *= M, V Ms*, Mr\*s = M, O *M8* ,

*M*. = Or , My = 1m, *Mz = In,*

Mr = *Mr*, M\_1 *=* M, for every *r, $ € R(*A).

**da*n***

**Corollar**y 1.13.*7 Let f :*R(A) - Mn(V) *be defined by S(r) =* M*r, Vr E R(*A). *Then f is an order isomorphism. between (*"*R(*A), C) *and* (Mr(V), 5). *Proof.* By Theorem 1.13.4, *f* is a lattice isomorphism and consequently an order isomorphism by Theorem 1.11.6.

Let r = (A, A, *R)* be a homogeneous relation. Recall that:

r is reflexive AAC*R,* or is transitive *RORCR,*

**Examp**le 1.13.5 Letr and s be homogeneous relations on the set A= {1,2,3} having the graphs

ma is symmetric

*R=*

*R* == {(1, 1), (1, 2), (2, 3), (3,1)}, ..

S = {(1,2), (1, 3), (2, 1), (2, 3), (3, 1)}. Let us see how we could compute their composition in an easier pro grammable way. Their associated bivalent matrices are

*R.*

i is antisymmetric G *RORS*AA. Then by Theorem 1.13.4 and Corollary 1.13.7 we get the following theo rem, characterizing these properties in terms of associated bivalent ma trices.

1 1 0 M*r* = 10 0 11,

*1*0 1 11 *M*s = 11 0 11.

Since by Theorem 1.13.4 the bivalent matrix associated to S*oR* is

1 1 11 *Msor = Mr\*5* = M, *O Mg* = 11 001,

lo 1 *1*

it follows that

**Theorem** 1.13.8 *Letr* - (A, *A, R) be a homogencous relation. Then*

*go is reflexive In S*M,, *To is transitive* at M, OM, < Mr,

*p is symmetric* Mp=M,

*ya is antisymmetric* M, AM*, <ly.* **Example** 1.13.9 Let A = {1,2,3,4,5) and let y be the homogeneous relation on A having the graph

*R=*AA U{(1, 3), (1,4), (2, 3), (2,4),(4,3), (5,2), (5,3), (5,4)} . Then its associated bivalent matrix is

*1*1 0 1 1 0

*S*or= {(1,1),(1, 2), (1,3), (2, 1), (3,2), (3, 3)}.

We could proceed similarly in order to get the intersection and the union of *r* and s or their inverses.

promenade

permanę

Mr =

0

0

1

0

0

.

Theorem 1.13.6 *Define a partial order”* <” *on* Mn(V) *by*

*(dij) = (bij)* 6 *Wij bij, Vi, j* € {1,..., 8} . *Then* (Mn(V), 5*) is a latlice, where*

inf((d*ij), (bij)) = (dij) ^ (b*i*j)*, sup((a*ij), (bij))* = (*dij) V (bij*).

ponad pred

lo

1

1

1

1

Since we have *In <* M., M*., OM*, *M., M., AM <1*m and M+ M , it follows by Theorem 1.13.8 that r is reflexive, transitive, antisyrometric, but not symmetric.

58

.

*CHAPTER 1. RELATIONS*

*1.14. CLOSURE* SYS*TEMS* AN*D OPERATORS*

59

hay

**1.14 Closure Systems and Operators**

Recall that if M is a set, then *(P(M*), C) is a complete lattice, where inf(Ailier = nic Ai and sup(Ailier = Vier Ai, for any family (Ailie*r* of elements of *P(*M).

We will be interested throughout the present section in those families C of subsets of *P(*M) having the property that any intersection of subsets of *C* is again in C.

(also see Definition 5.1.6). The definition could be visualized geometri cally in the real plane by saying that any line segment determined by two points in C is again in *C.*

Let C be the set of all convex subsets of R XR. Then C is a closure system on RXR, since any intersection of convex sets is a convex set (see Theorem 5.1.9).

Theorem 1.14.3 *LetC be a closure system on a set* M*. Then (C*, S) i*s a complete lattice.*

**Definition** 1.14.1 Let M be a set and let *C* C*P(M*). Then C is called a *closure system on M* if

*M*(Ailier SC, n A EC.

*ier* . .

3.

*Proof.* For any family (Ailier of elements of C, there exists inf(Ailie*r ==* nie A, EC. Then by Theorem 1.10.5, (*C*, S) is a complete lattice.

Let us notice that by the very definition of *sup* in *P*(M) we have sup(Ailier = niceCIU ACC}.

*LEI* .

*Remark.* If *I =* 0, then Nie, As = M. This holds, because nie, Ai = info = M (see the remark on page 41). Therefore, if C is a closure system on *M*, then ME*C*.

**Example 1.1**4.2 (a) For every *n.* € N, denote *nZ = {n.*

k *k* E Z}. Also denote

Cz= {nZ in EN). Then Cz is a closure system on Z, since for any *I* S N we have nie, *niZ = InZ € C*z. Actually, if *I* is finite, then m is the least common multiple of *(Trial*ies and if *I* is infinite, then *m* = 0.

*(6*) Let A be a set and denote by *Ru*f(A)*, Ri*(A) and R$(A) the set of all reflexive, transitive and symmetric homogeneous relations on A respectively. Then *R* (A), *R*i(A) and Rs(*A*) are closure systems on AXA (the proof is similar to that of Theorem 1.6.8).

We mention that the set of all antisymmetric homogeneous relations on A is not a closure system. One can prove that if (ri)ier is a family of antisymmetric relations and *I #0*, then Nietiis again antisymmetric. But if *I =* 0, then the intersection is AX A (see the previous remark), which is not antisymmetric.

(C) A subset C CRXR is called *conve*r if

*VX,YEC,* VA € (0,1), «x + (1 - *aly e C.* If I = (21,22*), y = (y1, y2) E C* and a € (0,1), then ar + (1 - ab*y* is defined as

(Ax{ + (1 - a)*y*1, 6.12 + (1 ~ a)y2)

We are going to see that there exists a strong connection between the closure systems on a set M and some special maps fro*m P(*M) to itself. **Definition 1.1**4.4 Let M be a set. A map*) :P(*M) -*- P(*M) is called a *closure operator on* M if:

(1) X S*J(*X), V*X EP(*M); (2) X,Y *EP(M*), XCY *J*(x) < J(V);

(3*) J(J*(X)) = J(X), *VX EP(*M). *Remark.* Notice that if (1) and (2) bold, then *J(X*) C*J(J*X)), so that we could have asked in the definition of a closure operator the weaker condition (3) *J(J*(X)) CJ(X). Definition 1.14.5 Let *J : P(*M) - *P*(M) be a closure operator on a set M.

(1) J(X) is called the *closure of X.*

(2) A subset XCM is called a *closed subset i*f *J(*X) = X. Example 1.14.6 Let r = *(*M*,*M*,R*) be a quasi-order and let *j : PM - P(*M) be defined by *J(*X) = r(X), VX *E P(M*). Then *J* is a closure operator on M. Indeed, we have:

*q*ue reflexive AMC*R=*XC?*(*X), *VX* E*P(*M),

X,*Y E P(*M), X SY ?(X) Cr(y), *y* transitive *RORC R= (r*(X)) Sr(x), *VX E P(*M).

*CH*A*PTER 1. RELATIO*NS

*1.14. CLOSURE SYSTE*MS A*ND OPER*A*TORS*

because (see (i) and *(i*i))

Let us now establish the connection between the closure systems and the closure operators on a set. But first denote respectively by *CI(*M) and *Op(M*) the sets of all closure systems and the set of all closure operators on a set M*.*

| X 60 *=> '*(X) = X

= X*e CJc*.

For every *J E Op*M), we have

**Theorem 1.1**4*.7 (i) Let C be a closure system on a set M and let Jc :P(M) - P(M) be defined by*

*(FOG)(I) = F(*C1= *1c, = 1.*

*Jc*(X) = n(CECIXCC}, VX *E P(M).*

Indeed, for every X C*M,*

*J(*X) = X

JC,(X) = X.

But since I S*J(*X) and *J(J*X) = JX), it follows that

*JC,*(X) SJ*C)(J*(X)) = *3*(X).

*Then Je is a closure operator on M.*

*In fact,* Jc*(*X) *is the least subset in C containing* X.

*(ii) Let J:P(*M) *- P(M) be a closure operator on a set* M*. Then the set*

*Cj* = {X CM|)(X) = X} *of all closed subsets of M is a closure system on* M*.*

*(izi) Let F:CI(*M*)* - *Op(M) be defined by F(C*) *= JC,* V*C E CIM)*. *Then F is a bijection, whose inverse is G:Op(M*) - *CI(M*) *defined by G()*) = *C), VI E Op(*M).

Similarly, one can prove that f(x) < *Jci*(x) for every X SM, so that

*JC; =) Remark.* We have seen that if *C* C *P(*M) is a closure system on a set M, then *(C*,C) is a lattice (see Theorem 1.14.3). Then by Theorem 1.14.7, for every A, *B EC* we have

*Proof. (*i) It is easy to check the first two properties of a closure operator. In *o*rder to show the third, let us prove that

infc(*A*, *B)* = An *B*= infp(M)(A,*B*),

*Jc(*X) = XEXEC.

supe(A,*B) = Je(*AU*B)*

AU*B*= supp(M)(*A, B).*

**Example 1.1**4.8 We have seen that, for a set A, the sets Rq *(*A), *Ri(*A) and *R*:(A) of all reflexive, transitive and symmetric homogeneous rela tions on A respectively are closure systems on AX 4.

Let A = {1,2,3} and let p and *u* be the homogeneous relation on A with the graphs

*R* - {(1, 1), (1,3), (3, 1), (3, 2)},

*S* = AA U{(1,2), (2,3), (1,3)}. Then the closures of *R* in *R*(A), *R*t(*A*) and R (A) are respectively

Indeed, if Ic(X) = X, then X is the intersection of some subsets C*E*C, hence X EC by hypothesis. Conversely, if X EC, then X is one of the subsets of the intersection defining Jc(X), so that Jc(X) CX. But we also have X *CJc*(X), hence *J*C(X) = X.

Now since JC(X) E C by its definition, it follows that *JC(J*C(X)) = *Jc*(X). Therefore, *J*c is a closure operator on M*.*

*(i*i) Let (Ailiei be a family of elements of Cj and denote A = Pier Ai. Then V*i ET,* AC Ai, hence *J*(A) S*J*A) = Ai by the second property of a closure operator and by the fact that Ai EC). It follows that J(A) chic, A = *A*, whence J(*A*) = A, so that A EC*)*. Therefore, C*j* is a closure system on M.

*(iii*) We will prove that *GoF-*lc*i(*m) and *FoG*=10p(M). For every *CECI(M*), we have

Aman aman

1

)

*Jr(R)* = AA U{(1,3), (3, 1), (3, 2)}, *Jt(R)* = {(1, 1), (1, 2), (1,3), (3, 1), (3, 2), (3,3)},

*JS(R)* = {(1, 1), (1,3), (2,3), (3,1), (3, 2)},

--

*(GOF)(C) = G(JC) = Cje =* C,

-

*CHAPTER 1. RELATIONS*

that is, respectively the "least" reflexive, transitive and symmetric rela tion containing *R.*

The closures of S in Ry(A), *R*t(A) and Rs(A) are respectively

33

*J, (S)* = S,

*JI(*S) = S*,*

*J.(*S) = A x4, that is, respectively the "least” reflexive, transitive and symmetric re lation containing S. Notice that S is a closed subset in Rr(*A*) and in *Rt(*A).

Chapter 2

Algebraic Structures

The chapter deals with the basic algebraic structures with either one or two (binary operations, such as semigroups, groups or rings. Therefore, in addition to the study of sets and the relations between them discussed in the first chapter, we are interested now in operations defined on them.

2.1 Basic Definitions and Examples

One of the key ingredients in this chapter is the notion of an operation. Recall that by an *x-ary operation (n* E N) on a set A we understand a xnap

*6*; *A* = AX:.. XA - A.

*n* times Also, by a *(universal) algebra* we understand a set A together with some *72*-ary operations (n EN) on A (see Definitions 1.10.8 and 1.10.10).

In the sequel, we will be interested in some algebras with one or two binary operations. Since from now on all the operations that we deal with will be binary, we will omit this adjective and we will simply call them *operations.* Therefore, we have the following definition.

**Definiti**on 2.1.1 By an *operation* on a set A we understand a nap

6: AXA

A.

Usually, we denote operations by symbols like ., t, \*, so that *f(x,y)* is denoted by *\*y,* t*y, r\*y, V(*x, *y)* E AXA.

64

*CHAPTER 2. ALGEBRAIC STRUCTURES*

**7**

*2.1. BASIC DEFINITIO*NS *A*N*D EX*AM*PLE*S

**Example** 2.1.2. The usual addition and multiplication are operations, on N, Z, Q, R, C and the usual subtraction is an operation on Z, Q, R, C, but not on N. The usual division is not an operation on either of the five numerical sets, because of the element zero.

(ii) Suppose that a has 21,*0*2 € A as inverses. Then by the associative law, we may compute the product *az · 0, 0*, in two ways as

*a*z (*a.a*z)

01'e = ai

Let us now define some important laws for operations,

**Defini**tion 2.1.3 Let" 4" and "." be operations on an arbitrary set *A*. Define the following laws:

A*ssociative law*

**and**

(@1.a). *0*2 = 2.02 = *.*2 and we obtain aj = 2*2*.

Let us now discuss some special subsets of sets endowed with an operation.

(*x •y). z = r. (yoz), Vx, y, z* € A

@ *Commutative law*

**Definitio**n 2.1.5 Consider an operation y: AXA - A on a set A and let *B* C A. Then *B* is called a *stable subset of A with respect to y* if

*3 3 = 32, VT, gc* Á

*Vany EB,*

*12,Y) E B.*

*• Identity law*

In this case, we may consider the operation

Je E A:

*a. e*

*e*

*.a = a,*

*va* € 4

*' :B x B -*

*B*

*(*e is called an *identity element)*

*Inverses law*

o*n B* defined by

*Va* € A, 3a E A:

*'*(*x, y)*

*(2,4*)*,*

*(z,y) € B\*B,*

*a.a' =a.a*re (e is the identity element)

*(a'* is called an *inverse element for a)*

*© Distributive laws*

that is called the *operation induced by w in the stable subset B of* A.

When using a symbol "." for the operation 4, we will simply say that *B is a stable subset of (*A,.).

*. (y* + 2) *= 2 y+y:z,*

*Vx,y,z* E A

(*y* -f. 2). *I=y I* +2.*3, Vx,y,z* E A that is, "." is distributive with respect to " +".

*Remark.* Notice that the associative, the commutative and the distribu tive laws still hold in a stable subset (endowed with the induced oper ation), since they are true for every element in the initial set (only the universal quantifier W appears in their definition). But the identity ele ment and the inverse element do not transfer (their definition uses the existential quantifier ) as well).

**Lemma** 2.1.4 *Let"," be an operation on a set* A.

*(i) If there etists an identity element i*n A*, then it is unique.*

*(ii)* A*ssume further that the operation* "." is *associative and has identity elemente and let a* € A*. If an inverse element for a does exist, then it is unique.*

**Exampl**e 2.1.6 (a) The interval (0,1) is stable in (R,).

*(6)* The set of invertible *n x n*-matrices (*n* € N, *n* > 2) with real entries is stable in (Mn(R),-).

*Proof. (i*) Assume that €1,62 € A are identity elernents in A. Then by computing their product in two ways, we have ei ea = ei = ez.

Let us now define the algebraic structures (algebras with one or two operations) that we will study throughout the present chapter.

*66*

*CHAPTER 2.* AL*GEBRAIC STRUCTURES*

*URE*S

2.2*. SEMIGROUPS*

*Remark.* Other examples of semigroups, groups, rings and division rings will be given in the following sections, when we will discuss their prop erties in detail,

**Definition** 2.1.7 Let A be a set. Then (*A*) is called a .

(1) *groupoid* if” ." is an operation on A. (2) *semigroup* if it is a groupoid and the associative law holds. (3) *monoid* if it is a semigroup with identity element. (4) *group* if it is a monoid in which every element has an inverse.

If the operation is commutative as well, then the structure is called *commutative. A* commutative group is also called an *abelian group.*

2.2

Semigroups

***I*ce**

**Examp**le 2.1.8 (a) Define on N\* the operation "\*" by

Recall that a pair *(A*,) consisting of a set A and an operation "," on *A* is called a *semigroup* if the associative law holds and (A, ) is called a *monoid* if the associative law holds and there exists an identity elenient with respect to",". We usually denote the identity clement by 1.

Definition 2.2.1 If (A, :) is a semigroup, then the operation”," is associative, so that we may define Vx EA,

*m\*1 = m", m, n* EN\*. Since "\*" is not associative, (N\*, \*) is a grupoid, but not a semigroup.

*(b*) (N\*, +) is a serigroup, but not a monoid,

(c) (N, +), (N, ), (Z, :), (C, :), (R, :), (C, .) are monoids, but not groups.

(d) (Z, +), (Q, +), (R, +-), (C, +), (Q\*, :), (R\*, :) and (C\*,-) are groups.

*E*" *= 2.3.....*

*(n* E N\*).

*n*o times

If (*A*,) is a monoid, then the operation ",” is associative and has an identity element, so that in addition we may also define 20 = 1.

**f**

*Remark*. If the operation is denoted by".+", then we replace the notation x" by *123.*

We may now state some computation rules in a semigroup.

**Definition** 2.1.9 Let A be a set. Then a structure with two operations : (A, +, ) is called a:

(1) *ring* if (A, +) is an abelian group, (A,-) is a semigroup and the distributive laws hold (that is, " ," is distributive with respect to " +").

(2*) unitary ring* if (A, +,-) is a ring and there exists an identity element with respect to "."

The ring (A, +,-) is called*.commutative* if the operation "," is com mutative.

Lemma 2.2.2 *Let (A*,*) be a serigroup, let 2* É A *and let m, 12* E N\*,

*Then:*

*() e*n n = . *(ii) (m*m)" = *inn*

If(*A*, +, ) is a ring, then we denote the identity elements with respect to " ..." and "." respectively by 0 and 1. We will also use the notation A\* = A' {0}.

*Proof*. By the induction principle applied either on *m* or *ni.*

Let us now see some other examples of semigroups and monoids than those given in Section 2.1.

**Definitio**n 2.1.10 Let A be a set. Then a structure with two operations (A, +, ) is called a:

(1*) division ring (or skew field)* if (A, +,-) is a ring, IA > 2 and every EA\* has an inverse - EA\*.

"," *(2) field* if it is a commutative division ring.

Example 2.2.3 *(*a) Let R(A) be the set of homogeneous relations on a set A and let"0" be the composition operation on *R*(A). Then (*R*(4), o) is a monoid, where the identity element is A.

In particular, (A4, 0) is a monoid, where A4 = *{*

*f f* A} and

: 4. - the identity element is 1A.

*(b*) Let (4,) be a serigroup (monoid) and denote by Mg(4) the set of *n x n* matrices with elements in A. We may naturally define a

**Example** 2.1.11 (a) (Z, +,-) is a commutative ring, but not a field.

*(b*) (Q, +,-), (R, +. :) and (C, +,-) are fields.

.

*CHAPTER 2.* A*LGEBRAIC STRUCTURES*

2*.2. SEMIGROUPS*

\*\*\*\*

multiplication on Mn(A) using the multiplication on A. Then *(*Mn(A), :) is a semigroup (monoid).

(c) Let A,) be a semigroup (monoid). Define on *P(A*) a multipli-. cation by

*Remarks.* (1) In fact, the set of all subserigroups of the semigroup A is a closure system (see Definition 1.14.1) and the subsemigroup generated by X is the closure of X with respect to the associated closure operator (see Theorem 1.14.7).

*(*2) Notice that <0 >= Ø by Definition 2.2.6.

Let us now determine how the elements of a generated subsemigroup look like.

X Y = {*x•y*\*EX*, YE*Y}, VX,*Y E P*(A).

Then *(P*(A),-) is a semigroup (monoid). If e is the identity element in the monoid (A,), then {e} is the identity element in the monoid *(P*(*A*),-).

**Theorem** 2.2.7 *Let (*A;-) *be a semnigroup and let 0* + X CA*. Then*

«

X >= {2122 ...In

Die X, = 1,...*,71, n* E N\*},

**Definitio**n 2.2.4 Let (A,) be a semigroup and let *B* C A. Then *B* is called a *subsemigroup* if *B* is stable with respect to the operation ".", that is,

*Vä, y EB, YE B.*

*that is, the set of all finite products of elements of X.*

*Proof.* Denote by

the right hand side, that is,

*C* = {*4*122 ...In € X, *i* = 1,.*..,?h, n* EN\*}.

**Theorem 2**.2.5 *Let (A*, :*) be a semigroup and let (Bilier be a family of subsemigroups of (A*,.). *Then* Nie*, Bi is a subsemigroup of (*A, ').

*Proof.* Let *x,y*enic, *Bi*. Then *2, y E Big Vi E I.* Since each *Bi* is a subsemigroup of (A, ), we have *x y € Bi, Vi el*, hence *r.y*e Niej *Bi.* Therefore, sie*r Bi is* a subsemigroup of (A,').

Let us discuss now a very important construction. Given a semi group, in general a subset is not a subsemigroup. The question is how to "complete" it in a minimal way such as it becomes a subsemigroup. This is the motivation for the following definition. It is worth to be mentioned that this idea is more general and it will appear again for the other algebraic structures and substructures we will define.

We are going to prove that C is the least subsemigroup of A containing

X, that is, to show the following 3 properties:

(i) C is a subsemigroup of A; (ii) X C*C"*; (ii) If *B* is a subsemigroup of A and X C*B,* then CC*B.* Let us discuss them one by one.

(i) It follows since the product of two finite products of elernents of X is a finite product of elements of X.

(ii) Take n = 1 in c. (iii) By hypothesis, any finite product of elements of X S *B* is in *B.*

**Corollar**y 2.2.8 *Let (*A,*) be a semigroup and let 3* € A*. Then*

**Definition** 2.2.6 Let (A, :) be a semigroup and let X Ç*A*. Then we denote

<>= {x" | n € N\*}.

<X >= *N{B* CA*B* is a subsemigroup and X C*B}*

**Examp**le 2.2.9 The subsemigroup generated by 2 in (N\*, +) is

< 2 >= {2*n* | n EN\*} = 2N\*.

and we call it the *subsemigroup generated by X.*

In fact, <x> is the "least" subsemigroup of A containing X. Here X is called the *generating set* of <x>. If X = {x}, then we denote <>=< {2}>.

Let us now define some special maps between semigroups. Recall that we denote by the same symbol operations in different arbitrary structures.

*CHAPTER 2. ALGEBRAIC STRUCTURES*

2.3*. FREE SEMIGROUP*S

*B.:*

**Definition 2.2.10** Let (A,) and *(B*,) be semigroups and *f*: A Then *f* is called:

(1*) (semigroup) homomorphism* if :

*f(x y) = S*(*I): f(y),*

*Vx, y* A.

*f*(1) *== f(*1) *f(x*) *= f(*1.x) = *f*() =E*,* hence *f*(1) = 1' is the identity element of A.

(ii) Since

.2.2-1 = 3-1.=1 *5(*x-2-1) = *f*(x-1.2) = *f*(1) =

*> f*(x)• *f* (x-2) = *f*(*x*-1*). S*(x) = 1', it follows that *(f(*x))-1 *= f(x*-1).

*(*2) *isomorphism* if *f* is a bijective homomorphism.

(3) *endomorphism* if *f* is a homomorphism and the semigroups A and *B c*oincide.

*(*4*) automorphism* if *f* is an isomorphism and the semigroups A and *B* coincide.

2.3 Free Semigroups

S A. Recall that the subsemi

Let (A,) be a serigroup and let 0 € group generated by X is

**Exampl**e 2.2.11 (a) Let (4,-) be a semigroup. Then the identity map 1A: A - A is an automorphism of A.

*(6*) Let (A,) be a semigroup and let *B* be a subsemigroup of A. Define *i :B* - A by i*(x)* = *2,* VE *E B*. Then *i* is a homomorphism, called the *inclusion homomorphism.*

<X >= {*x*1.22 ... Imami E X, = 1,..*.,n,n*e N\*},

**Th**eorem 2.2.12 *(i) Let f* : A - *B be a semigroup isomorphism. Then f-1:B - A is a semigroup isomorphism.*

*(ii) Let f*:*A*-*B and g: B C be semigroup homomorphisms. Then gof:* A-*C is a semigroup homomorphism.*

that is, the set of all finite products of elements of X (see Theorem 2.2.7).

In general, the writing of an element of < X > as a finite product of elements of an *n*-tuple (31,.*.*., *I*n) e X” is not unique. This is due to the fact that some other laws than the associative law may also hold in a semigroup, for instance the commutative law in a commutative semigroup or some other relations between the elements of the generating set X.

For instance, take the sernigroup (N, :) and let X = {2, 4, 5, 10}. Then <X > is the set of all finite products of elements 2, 4,5 and 10, that is,

*Proof.* Left to the reader.

| Definition 2.2.13 Let (A,) and (A', .) be monoids with identity ele ments 1 and 1' respectively and let *f* : A- A'. Then f is called a *unitary homomorphism* if f(1) = 1'.

<X >= {24.4.5m. 107 | k*, l, m, n* E N\*} = {2k. 5m | k*, mn* € N\*}.

**Theorem** 2.2.14 *Let* (A,) *and (A'*,') *be monoids with identity ele ments* 1 *and 1' respectively and let f* : A - A *be a semigroup ho momorphism.*

*(i) If f is surjective, then it is unitary.*

*(ia) If f is unitary and x* € *A has an inverse element 21*€ A, *then f(I) has an inverse and*

We have 20 = 2 · 10, but also 20 =4.5.

In what follows, we start with an arbitrary (non-empty) set X and we will construct a semigroup gencrated by X for which only the associative law holds. It has many applications in Computer Science, in connection with the so-called *word problem.*

**Definiti**on 2.3.1 By a *word on* X we understand an 7h-tuple (nz EN)

*w = ($*1,.*.*., Xyz) E X

.

(*f {2))-*1 *= f(x*-2). *Proof.* (i) Let x' E A'. Then 3x € A such that f(x) = x'. Then we have

m*'. f*(1*) = f*(x*) + f*(1) *= f(*x - 1) = *f*(x) = x',

The natural number n is called the *length o*f the word *w* and is denoted by *l(w).*

*572*

*CHAPTER 2.* A*LGEBR*A*IC STRUCTURES*

***EBR***

......

*2*.3*. FREE SE*M*IGROUPS*

*X*

Ifn= 0, then Xo has a unique element (see page 13), called the *void word* and denoted by e.

If n= 1, for the sake of simplicity of writing, we will identify a word. (1) of length 1 by the element & € X.

*(i*i) Let *w El*S;*(*X), say *w =* (01,..., 29). Since we have identified *(x*) by x € X, we may write *u = x*1*22*.*..X*yz

If *w=t*s ... for some (I's, ...,) Xm as well, then

.

Let us now define the equality of two words on X and introduce an operation on X

w = (x',...,xim) = (11, ... , m*)*, so that *m =n* and Xi = x, V*i* € {1,...,*n*}. Therefore, the writing of an element of *S*,(X) as a finite product of elements of X is unique. O

**Definitio**n 2.3.2 Let *w* (81,..., Im) and w*'* . .... ) be words on X

The *equality o*f the two words is naturally defined by

*w =\*W 5 m* = 1 and Xi = t', Vi € {1,..., 82}.

**Corollar**y 2.3.4 *(i) If* |X1 = 1*, then we have a semigroup isomorphism between (S*P(X),) *and (*N, +). .

*(11) If* X > 1*, then the semigroup S*F(X) *is infinite and non commutative.*

The *product* of the two words, denoted by *w w'*, is defined by *juxta posing w* and *w'*, that is,

*Proof. (i*) Let X = {x}. For every w ES *(*X), we have

*w* = (*1*, ..., *3) =*

*I 2 = 2*

*w-w' = (2*1, .*..*, Eyn, 21,...,mm).

***7*2 times**

*n* times

*Remark.* If *w* and *w'* are words on X, then

for some *n* E N. Then an isomorphism is *f :*S (X) - N defined by *f(3) = 12.*

(i*i*) Clear.

*1{w • W') = 7(W) + llw'*).

Let us denote by SF(X) the set of all words on X.

**Definiti**on 2.3.5 The semigroup Sf(x) is called the *free serigroup generated by* X.

A semigroup (A, ) is called *fre*e if there exists a set X such that the sernigroups (S'(X), ) and (A,) are isomorphic.

**Theorem** 2.3.3 *(i) (S*/(X), ) i*s a semigroup with identity, where the identity is the void word e.*

*(ti) VW* € S (X), Sn € N *and there exists a unique n-tuple* (21,...,n) E X*such that*

**Exampl**e 2.3.6 The semigroup (N, +) is free by Corollary 2.3.4.

**Theorem** 2.3*.7 Let (A*,) *be a scrigroup with identity and let X be a set. Then for every map f:* X - *A, there exists a unique unitary semigroup homomorphism :*S(X) - A *eriending I, 2.€., s*x *= .*

**T**

**HIP**

*U = 11 1*2 ....*I*na *Proof.* () Let w = ($1,...,2m), w' = (21..., and w*" =* (x",..., me be words on X. Then

*wo (w.w"*) = (11, .., Xm)• (za,..., m, 2,...,2%) =

= (x1, ... Per mag, mens de ...,20) = = ($1,..., lim, &' ,. .. , en). (x",. .. ) = (w •w*'*).w". Therefore, (*S:*(X), ) is a semigroup. Clearly, the void word e is the identity element in *S*F(X).

*Proof.* Let us prove first the uniqueness. Suppose that we have an isomorphism *f:S*:(X) - A extending *f*, that is, *wx* E*x, f*(*x) = f(x*). Then V*w =* (21, ..., *I*nn) ESF(X), we have *w =* 1 X*2*:... "Igr. It follows that

*f (w) = f(x1*)*. F*(x2).*... 7 (*xx) = *f*(x1) · f(*x2). .... f*(xn),

hence *f* is uniquely determined by *f.*

*CHAPTER* 2. A*LGEBRAIC STRUCTURES*

*2.4. GROUPS*

2.4 Groups

Let us begin by recalling the definition of a group.

Let us prove now the existence. Define *F :S,*(X) - A by

*F(t) = f*(x1) · f(x2). .*... f*(In*)*, V*w* = (21, ... , pm) *S;*(X) for n #0 and

*I(e)* = 1, where 1 is the identity element of A. Then W*w =* (Il, *..*, In), *w' =* (, ... ) E *S*/(X), we have

*F(w*. v\*) *= F*((T1*,* ... , Im, tj,..., )) = *= f*(x1*). f(x*2)...*..* (Im): 5()· *f*(29) ..*.. S() = 5(w). F(w')*, hence f is a homomorphism.

**Definiti**on 2.4.1 A pair (G,-) consisting of a set G and an operation "." on G is called a *group* if it satisfies:

(1) A*ssociative law: (wy*). Z=*2(y•z*), *Vr,y,z EG, (*2) *Identity element:* 3e E*G: I.e*=e*1*= *x,* VEE*G,*

*Va EG*,5*xI*e*G: 2*.1--- 2-1.1=e. (3) *Inverse element:* If *(*G,) also satisfies

*(*4) *Commutative law: Iy=yx, Vany EG*, then it is called a *commutative group (o*r an *abelian group).*

**2**

*Remark.* We denote by 1 the identity element of a group *(G*, :) and by *3*1 the inverse of an element re*G*.

We have seen that in a semigroup it makes sense to talk about non zero natural powers of an element. In a group we will be able to define We negative powers as well.

**Corollar**y 2.3.*8 Let (A*,) *be a semigroup wrth identity and let X he a set.*

*(i) If 5,9 : Sf*(x) + A are *semigroup homomorphisms such that f*lx *= gx, then f = g.*

*(ii) If):*S(X) - S,(X) i*s a semigroup homomorphisin such that f*(x) = *x, VX* E X, *then f =* 15,(X). *Proof.* (1) By Theorem 2.3.7.

*(22*) Take A = *S:*(X) in Theorem 2.3.7*.*

8

**Definition** 2.4.2 Let (G,) be a group, let I EG and let *n* E N\*, Then we define

\* = *\* I .*.... ,

*1*2 times

.

**Theorem** 2.3.9 *Every semigroup with identity is the image of a homo morphism defined on a free semigroup.*

\* = (27?)". *Remark.* If the operation is denoted by " +", then we replace the notation

by *nr.* We may now give some standard properties of group computation.

Lemma 2.4.3 *Let (G,) be a group, let r EG and let m,n e Z. Then:*

*(i) m*m = min*; (ii) (z*n)n = *xmln*.

*Proof.* Let (A,) be a semigroup with identity and let X be a generating set for A. Such an X always exists, since for instance we may take X = A. Let i :X + A be the inclusion map, defined by *i*(*x)* = *x,* Wo e X. Then i can be extended by Theorem 2.3.7 to a homomorphism. *1:*S:(X) - A.

Let us prove that i is surjective. Let a € A. Since X generates A, *Q* can be written as a = I1 ...In for some 21,.*..,* e X and *n* EN Now take *w = (*201, ..., gr) = 21:..... Then

*i(w*) = i(x1).... .7(En) = 2(x1).... •2(x) = I1.... 2n = a, so that 7 is a surjection.

Thus, A is the image of the homomorphism i defined on the free semigroup *S/*(X).

*Proof.* Left to the reader.

**Lemma** 2.4.4 *Let (G*,) *be a group and let a,2,Y E G. Then:*

*(i) a3 = (y= =y,*

*IQ-ya* => *2 = Y (cancellation laws); (02) (*2-1)-1 = *E.*..commencerone *(iii) (xy*)--1=*Y-1*.2-1.

*CHAPTER 2.* A*LGEBRAIC STRUCTURES*

*2.4. GROUPS*

Pa das dade e

*Proof.* Left to the reader. *Il Remark.* A finite group may, be defined by its operation table, that specifies the result of any multiplication of two elements of the group. The operation table of a group has the property that every element appears exactly once on each row and each column.

Let us now see some other examples of groups than those given in Section 2.1.

Then *(G X G'*, ) is a group, called the *direct product* of the groups G and G'. The identity element is (e, e') and the inverse of an element *(9.9) EGXG*' is (*g-1,0*1).

If *(G*,-) and (G', ') are both commutative, then (GxG', ) is commu tative,

The example can be easily generalized for n groups.

*(9*) Let *K = {e, a,b,c*} and define an operation "." on *K* by the following table:

ea b c

**Example** 2.4.5 *(a)* Let {e} be a single element set and let ” ,” be the only operation on {e}, defined by *e*.e=e. Then ({e},) is an abelian group, called the *trivial group.*

(b) Let n E N, n > 2. Then (Zum, +) is an abelian group, called the *group of residue classes modulo n.* The addition is defined by

| a a eclb bbcie

+ *= x* + *, VẼ, gc l*à .

Then (K,) is a commutative group, called *Klein's group.*

*(h*) Let Q = {+1, *,* Ł*j, k*} and define an operation " ," on Q by the following rules:

(C) Let

*Un =* {2 € C1z\* = 1} (n €N\*). Then *(U*,, :) is an abelian group, called the *group of n-th roots of unity.*

*(d)* Let

*GL*n(R) = {*A* E Mn(R) det A +0}

\*

*(n* EN, *n* > 2) be the set of invertible *n x n-*matrices with real entries. Then *(GL*n(R), ) is a group, called the *general linear group of rank n.*

(e) Let M be a set and let

SM *= {f:*M

*+ M*

*f* is bijective}.

I is the identity element, $ 12 *= ja = k*o = -1, © *. j k j k = 1, k=, tj.;= -k, k.j = -1,ż · k = -1*,

\* The signs rule holds. Then (Q,-) is a non-commutative group, called the *quaternion group.*

(i) Let A*BC* be an equilateral triangle and consider the following geometrical transformations that transform the vertices *A, B* and C in themselves):

me is the identical transform *(*or the rotation counterclockwise of 360°),

a is the rotation counterclockwise of 600, \* *B* is the rotation counterclockwise through 1200,

a is the symmetry with respect to the axis *di*, passing through A and perpendicular t*o BC,*

o*b* is the symmetry with respect to the axis *d2*, passing through *B* and perpendicular to AC,

mc is the symmetry with respect to the axis *d*z, passing through C and perpendicular to *AB.*

Then (SM,0) is a group, called the *syirimetric group of M.* The identity element is the identity map lm and the inverse of an element*s* (which is a bijection) is *f-1*.

If|M| =*n*, then Sm is denoted by Sn and the group (S72, 0) is in fact the *permutation group o*f n elements.

*(f*) Let (G,) and *(*G”,) be groups with identity elements e anda respectively. Define on GXG' the operation "," by

*(91,9*1). (*92*,*9*2) = (*91 · 92:91.ga), 191,91), (92,93) EG*X*G.*

*CHAPTER 2.* A*LGEBRAIC STRUCTURES*

2.4*. GROUPS*

79

{

}

X d,

Example 2.4*.7 (a) U*(N, +) = {0}, *U*(N, :) = {1}, *U(Z*,-) = {-1,1}, *U*(Q) = Q\*, *U(*R, ) = R\* and U(C, :) = C\*.

*(6)* Consider the monoid (My(R),-) (n e N, n > 2). Then (see Example 2.4.5)

*GL*, (R) = *U(*M(R), :) is a stable subset of *(M*,2(R), ) and G*L*(R) is a group with respect to the induced operation.

(c) Consider M*M = f*i*siM -* M} for some set M. Then *(*M*M*,) is a monoid. It follows that (see Example 2.4.5)

SM *= U(M*M,0) is a stable subset of *(*MM*,*) and SM is a group with respect to the induced operation. **Theorem** 2.4.8 *Let (G*,) *be a non-empty semigroup. Then (G ) is a group iff the equations*

*Q.• 2 = 0 and y.a=b*

Denote

*D3* = {e, ai*, B, a,b*,*c}.* Define the product *x y* of two transformations r and *y o*f *D3* by perform ing first y and then 2. Then(*D*3,-) is a group, called the 3-*rd dihedral group*

Generalizing, we can define the n-th dihedral group *Drt* of rotations and symmetries of the regular *n*-gon, consisting of n rotations and n symmetries.

*have unique solutions in G for every a, b E G*.

**Theorem** 2.4.6 *Let (.A*,*) be a monoid. Denote*

*U*A,-) = {€A132-:\*1 = x-1.2=1},

*that is, the set of invertible elements of* A*. Then U(*A, :) *is a stable subset of* (*A*,) *and U*(*A*, ) *is a group with respect to the induced operation.*

*Proof.* Let x,*y E U(*A, :). Then 3x-1, *y-1* € A. Since there exists

*(*\*•*y) -1 = y-1.*2-EA,

*Proof.* Suppose that *(G*,) is a group and let *a: E G*. Since Ja-1 EG, it follows that I1 *= a-1.b* and *y1 = b.4*-1 are solutions of the above equations.

Assume now that iz EG is also a solution of the equation *a.x ==* . Then *a* 21 *= a · 1*2, whence *x1 ==* 12 by the cancellation law. Similarly, one can prove that the second equation has a unique solution.

Conversely, let *a* E G. The equations a*x = a* has a solution in G, say Ep. For ever*y b* E G, the equation *ya = b* has a solution in G, say c. Then

*| ber =* cae*r = c = 6.* Analogously, we get er E G such that for ever*y b E G, ezb = b.* Comput ing the product e*r*g in two ways, it follows that eg = e is the identity element in G. Let us denote it simply by e.

The equations *ya=*e and *ax =* e have solutions in G, sa*y* a' and *a"* respectively. Computing the product *a'aa*" in two ways, it follows thal *a' - a*' is the inverse of a. Hence every element of G is invertible.

Therefore, (G,') is a group. *Remark.* Notice that the uniqueness of solutions is not needed for the converse part of Theorem 2.4.8.

it follows that *• YE U(A*,-). Henc*e U*(A, ) is a stable subset of (A,).

Then clearly " ," satisfies the associative law. Since 1 *EU(A*,-), 1 is the identity element in *(U*(*A*, :), :).

Now let 3 E*U(*A,-). Then 3-E A. Since there exists

(7-1)-1 =XEA,

it follows that x-*EU(*A, -). Hence every element in *(U(A*,), ) has an inverse.

Consequently, *(U*(A, :), :) is a group.

80"

*CHAPTER* 2*.* A*LGEBRAIC STRUCTURES*

2.*5. SUBGROUPS*

2.5 Subgroups

*(*2) In the case of an additive group *(G*, +), the conditions *(ii*) and *(iii*) in Theorem 2.5.2 become

*(it') 2, Y E H = 9+ye H; (iii') IE HS*-I*E H.*

...

We turn now our attention to the study of a group inside another group. Recall that the associative law and the commutative law transfer in a stable subset, whereas the identity element and the inverse element do not in general. But we will see that they do transfer in a subgroup.

Theorem 2.5.*3 Let (G,) be a group and let HCG. Then HSG iff*

.

*(ii) 2, YEH*

*2.4-16H.*

**Definition** 2.5.1 Let *(G*,) be a group and let *HCG*. Then *H* is called a *subgroup of G* if:

*(*1) *H* is a stable subset of (G,-), that is,

*Vany EH, E H;*

*Proof.* By Theorem 2.5.2. *Remark.* In the case of an additive group (*G*, +), the condition (*ii*) in Theorema 2.5.3 becomes

*(ii') x, y € H=*E-*YE H.*

*(2) (H,*) is a group.

Let us now see some examples of subgroups.

We denote b*y HS*G the fact that *H* is a subgroup of G.

The following two characterization theorems provide two easy ways of checking that a subset of a group is a subgroup.

**Theorem** 2.5.*2 Let (*G,) *be a group and let HCG. Then HSG iff*

**Exampl**e 2.5.4 *(*a) Every non-trivial group *(G*,) has two subgroups, namely {1} and G, called the *trivial subgroups.*

*(b*) Z is a subgroup of (Q, +), (R,+) and (C, +). Q is a subgroup of (R, +) and (C, +). R is a subgroup of (C, +).

(c) The set

*Un* = {2 € C12" - 1} (n € N\*) 10 of the n-th roots of unity is a subgroup of (C\*,.). *; (d)* Let (G, :) be a group. Then the set

*(ii) x,y EH (iii) & E H =*

*.YEH;* - *EH.*

*Z*(G) = {\* EG\x*.g=g2,* V*g E G*}

*Proof.* . Suppose that *HSG*. Then *H* is group, so that *H +*0*. .*

Moreover, there exists an identity element 1' *€ H,* hence 1' == 1.2 = *, V*X *E H.* By multiplying by 2-1, we get 1' = 1 € *H.* Therefore, a subgroup must contain the identity element of the group.

Condition (ii) holds by the definition of a subgroup.

Now let € *H* and denote by r its inverse in the group *(H,)*. Then *& -I* = x' x = 1. But 2 € *HCG* has an inverse x-1E*G*. Then by multiplying by x-, we get r' = x-*EH.*

. Suppose that the conditions *(i)*, (*ii*) and *(iii*) hold. Then *H* is a stable subset of *(*G,.). Clearly, the associative law holds also in *H.* Take *& E H \**0. Then by (*iii*), 2-1*€ H* and by *(ii*), 1 = \*\**\*EH.* Hence 1 is the identity element in *H.* By *(iii),* every element of *H* has an inverse in *H.*

Consequently, *H* is a subgroup of G. *Remarks*. (1) The condition (i) can be replaced in Theorem 2.5.2 by the fact that 1 E*H.*

is a subgroup of G, called the *center of G*.

Notice that

*Z(G*)=

C *G* is abelian, hence the center of a group is a measure of "how close” of being com mutative is the group.

(e) Consider the group (Z, +). Then

*H <ZAH*

*= n*Z for some *n* eN.

Indeed, suppose first that *H = r*2 for some n EN. Clearly*, H +*0. For every *, y € H,* we have x *= nk* and *y = nl f*or some *k, l € Z*,

82

:

*CH*A*PTER 2.* AL*GEBR*A*IC STRUCTURES*

2*.5. SUBGROUPS*

\*\*\*

and we call it the *subgroup generated by X.*

In fact, <x> is the "least" subgroup of G containing X. Here X is called the *generating set* of <x>. If X = {2}, then we denote <2>=<{1} >.

whence 2*-y=nk - rl = n(k-1*) e*nZ = H.* Then by Theorem 2.5.3,

*H=n*Z<*Z*.

Conversely, suppose that *H <* Z. If *H* = {0}, then *H =* 0.Z and we are done. Assume now that *H \** {0}. Then *H c*ontains a positive element (if x *€ H* and 3 <0, then -*1E H* and --> 0).

Denote n = min*(H* N N\*). We will prove that *H = nZ*.

Since *n € H* and *H <* Z, it follows that nz *C H.* Now if *\* E H,* then by the Division Algorithm (see Theorem 2.15.3), there exist unique *9,*1 € 7 such that

*Remarks*. (1) We use the same notation for the subgroup generated by a subset as we did for the subsemigroup generated by a subset. .

*(*2) In fact, the set of all subgroups of the group G is a closure system (see Definition 1.14.1) and the subgroup generated by X is the closure of X with respect to the associated closure operator (see Theorem 1.14.7).

(3) Notice that < 0 >= {1} by Definition 2.5.7.

Let us now determine how the elements of a generated subgroup look like.

*=ng*+,

where

0 <*r <n.*

But then r - -- *nq E H* and r > 0. By the minimality of n, it follows that r = 0, so that x = *nq En*z, hen*ce H C*nZ. Therefore*, H = r2.*

**Theorem** 2.5.*8 Let (*G,:) *be a group and let* 0 + XS *G. Then*

For a group *(G*, :*)*, we denote by S(G,) the set of all subgroups of *G.*

We will see that the intersection is compatible with subgroups, whereas the union is not in general.

<X >= {2*142 ... I*gal *I; E* XUX-1, 1 = 1,...,*12*,1 € N\*},

**Theorem** 2.5.5 *Let (G,) be a group and let (Hilier be a family of learning subgroups of (G*, *:). Then* Nie, *Hi E S(G,.)*.

*that is, the set of all finite products of elements and inverses of elements in X*.

*Proof.* Denote by *H* the right hand side, that is,

*Proof. F*or each *i El, Hį €* S(G,-), hence 1 € *Hi.* Then 1 € nie*, Hit* 0. Now let , *y*enie*r Hi.* Then *I,Y E Hi, Vi E I.* But *Hi E S(G*,.), *Vi el*. It follows that r.*y-1 € Hi, Vi E I*, hence *2 .y-*) € nicy *Hi.* Therefore by Theorem 2.5.3, ni*cy Hi E* S*(G*,). .

*H =* {2132 ... E XUX“*, 1* = 1,.*..,n,n* EN\*}.

**Examp**le 2.5.6 In Example 2.5.4 (e), we have seen that

S(Z,+) = {*nZn* EN}. Take *H =* 27, K = 32 € S*(*Z; +). Then *HOK* = 27 37 = 6Z is a subgroup of *(*Z, +). But *HUK* =2ZU 3Z is not a subgroup of (Z, +), because, for instance, we have 2,3 E *HU*K, but 2+3 = 5*€ H*U*K*.

Therefore, in general the union of subgroups is not a subgroup.

We are going to prove that *H* is the least subgroup of G containing X, that is, to show the following 3 properties:

(i*) H <*G; (ü) X S*H;* (iii) If *K* SG and X SK, then *H C* K. Let us discuss them one by one.

(i) Clearly, we have *H* 0, because X *\** 0. Let 2*1x2*...m, *Y1Y2... You E H.* Then

*(*21X2 ... In*n) (y1y2 .. . Y*n*)!*=*m1*2 .*..Imyn... YzYTEH,*

This leads to the idea of the subgroup generated by a subset of a group.

**Definition** 2.5.7 Let *(*G

) be a group and let X CG. Then we denote

so that *H <G* by Theorem 2.5.3.

(ii) Clear.

(ii) If *K 5 G* and X SK, then X-1 5 *K* by Theorem 2.5.2. It follows that *HCK.*

< x >=

{H <G X C *H}*

DRR*A*

*CHAPTER 2.* A*LGEBR*A*IC STRUCTURES*

*CHAPTER*

*2.6. GROUP HO*M*OMORPHIS*MS

85

Corollary 2.5*.9 Let (G, :) be a group and let x EG. Then*

<\*>= {zk|*k*ez}.

**Y**

**.**

**5**

**1. LA**

**Example 2.5.10** Consider the group (Z, +) and let n e Z. Then

<*n>= {nk | k* € Z} = *nz.*

**Exampl**e 2.6.2 (a) Let (G,) and (G", be groups and let *f:G-G!!* be defined by *f(x*) = 1', *Va e G*. Then *f* is a homomorphisını, called the *trivial homomorphism.:*

*(*6) Let (G, :) be a group. Then the identity map 16:

G G is an automorphism of G*.*

(C) Let *(*G,-) be a group and let *HS* G. Define *`i : H - G* by *i*(n) = I, V*I € H.* Then *i* is a homomorphism, called the *inclusion homomorphison.*

(d) Letn E N and define *f : Z* - Z by *f(x) = nie,* V*I* E Z. Then *s* is an endomorphism of the group (Z, +-). never even .?

(e) The groups (R, +) and (R\*,) are isomorphic. An isomorphism is *f*:R - R defined by *f(3)* = ex, VIER.

"

**Theorem** *lattice.*

**2**.5.11 *Let (G,) be a group. Then (*S(*G*,), 5) *is a complete*

*Proof.* Let *(Hibi*er be a family of subgroups of G. By Theorero 2.5.5, Nie *Hi E S(*G,), hence

inf*(H;)ier* = n *H*i.

*LEI*

By the definition of the subgroup generated by a subset of a group, we

**Theorem** 2.6.3 *(1) Let f: G*- *G' be a group isomorphism. Then f-1:G' - G is again a group isomorphisın.*

*(ii) Let f :G- Gl and g: GP - G" be group homoinorphisms. Then gof:G +G" is a group homomorphisti.*

*g*et

sup*(H)ier* =< U*H;>.*

*ier* Therefore, (S*(G,* :), 5) is a complete lattice.

2.6

Gr*o*

**an ISOM**

Let us now define some special maps between groups. Recall that we denote by the same symbol operations in different arbitrary structures.

**Definiti**on 2.6.1 Let (G,) and (G',-) be groups and let *f:G* Then *f* is called a *(group) homomorphism* if

*t*

*G'.*

*Proof. (i*) Clearly, *1*-is bijective. Now let r*',Y'* E G'. By the surjec tivity of *f, , E G* such that *f*() = *x* and *f(y) = y'.* Since *I* is a homomorphism, it follows that *f-1*62*":y') = f-?($(z) • (y)) = 5-1(f*(*x+*y)) = x*y=1-12'). :-*().

Therefore, *f-*1 is an isomorphism. --> *(i*i) Left to the reader.

**Theorem** 2.6.4 *Let f:G-Gbe a group homomorphisin. Then:*

*(1) |(*1) = 1*;*

*(ii) (f(x*))-1 *= f(x*-1), *VEEG. Proof. (i*) We have *VR* EG,1·*2=1*:1 = r, so that *f*(1-1) *= f(*-1) = *f(*F). Since *f* is a homomorphism, it follows that

*f(1) f*(1) *= f(*x)*.* f(1) = *f(x)*, whence we get *f(*1) = 1' by multiplying by *(0)*)\*.

*(ii)* Let e € G. Since 2-1 = x-1*.*=), *f* is a homomorphisto and f(1) == 1', it follows that

*$*(*x) 5*(*x*-*2) = f*(x-1*). 5*() = 1'. x

*f (y) = f(t). f(y), VX,YEG.*

The notions of *(group) isomorphism, endomorphism* and *automor phism* are defined as usual.

We denote by G - *G*' the fact that two groups G and *G'* are isomor phic. Usually, we denote by 1 and 1' the identity elements in G and *G* respectively.

**80**

*CHAPTER 2. ALGEBRAIC STRUCTURES*

87

*2.6. GROUP HOMO*M*ORPHISMS*

Hence (*f*(x))-1 = 5(3-1).

Let us now define two important sets related to a group homomor phism, that will be even subgroups.

It is well-known that a group homomorphism (and even a function) *f:G- G*' is surjective iff Im*f = G'*. We have a similar characterization of injective group homomorphisms by their kernel.

Theorem 2.6.8 *Let f:G\_G" be a group homomorphism. Then*

*L*ive

**Definitio**n 2.6.5 Let *f*:*G* G*'* be a group homomorphism. Then the set

Kcr *f* = {TE*G*|*|*(x) = 1'} is called the k*ernel* of the bomomorphism */* and the set

In*f* = {*f*(x)/x E G}

is called the *image o*f the homomorphism *f.*

*Remark.* Notice the similar notation for the kernel of a function *f,* namely ker*s*, and for the kernel of a (group) bomomorphism *f*, namely Ker*f.* The first one is an equivalence relation (see Lomma 1.7.13), whereas the second one is a subgroup (see Theorem 2.6.6). There is a connection between them, but this is not a subject of the present **course.**

Ker *f* = {1} *f is injective.*

*Proof. =* . Suppose that Ker*f* = {1}. Let *x,y E G* be such that *f(x*) = *f(y*). Then (r*) (f(y)*)-1 = 1', whence it follows that *f(xy-1*) = 1', that is, *my-I* E Ker*f* = {1}. Hence *x = y.* Therefore, *f* is injective.

. Suppose that i*f* is injective. Clearly, {1} & Ker*f.* Now let 2 E Ker*f*. Then *f(x*) = 1*' = f(*1), whence I=1. Hence Kerf 5 (1}, so that Ker*f* = 1}.

We have seen that if *f:G- G'* is a group homomorphisin, then Im*f <G*ʻ. But we have a more general result.

Theorem 2.6.9 *Let f :G - Gbe a group homomorphism and let HSG and H' SGʻ. Then f(H) SG' and 1 (H') SG. P*r*oof.* For the first part, see the proof of Theorem 2.6.6. Since f(1) = l*'E H',* we have 1 *e f (H').* Now let 2, *y € f (H').* Then Ex", *EH* such that *f(x*) = rand *[(y) =y'.* But since *H' <* G' and *f* is a group homomorphism, we have

*f(xy*-1) = *5(x)f(y-*2) = *f*(x*)(f*(*y)*)-1 = t*'y- € H'.*

**Theorem 2.6.6** *Let fiG - G' be a group homomorphism. Then*

Ker*f SG and* Imf 5 *G'.*

D. Now let *2,*€ Ker*f.*

*Proof. S*ince f(1) = 1', we have 1 € Ker*f* Then *|(2) = f(y*) = 1'. It follows that

prog

*sity-) = f(x)f(y-2) = f(r)(*(*y)*)-1 = 1'.1' =1',

Hence xy=*€ 7 (H". C*onsequently*, f'(H') SG.*

hence *zy-*E Kerf. Therefore, Ker*f <G*.

Since 1*' = f(*1), we have 1' € In*f +*0. Now let z', *y'* E Im*f*. Then 3*x, y EG* such that *f(x*) = x' and *f(y) =y*. It follows that

**Theorem 2.6.10** *Let f :G* - *G' be a group homomorphism and let* X*CG. Then*

*f*(<x>) =< f(x) >.

*a'y-2 = f(x)(f(y))*-1 = *f(x)f(y-2) = f*(*xy*-l) e Im*j,* hence z'*y*-€ Im*f*. Therefore, Im*f SG'.*

*Proof.* If X = 0, the conclusion trivially holds. Assume X +0. By Theorem 2.5.8 we have

<X >= {2122 ...Til E XUX“, *i* = 1,...*,n,*EN\*}.

**Exampl**e 2.6.7 Let *f*:*Z*-Zy be defined by *f*(x) = *, V*a e Z. Then *f* is a homomorphism between the groups (Z, +) and (Z142, +). We have

Since f is a group bomomorphism, it follows that

Ker *f* = {r € Z î= } = rz.

*f*(< X >j *= f*({*2*1 ...| : E XUX-1, 1 = 1, ..., Nine N\*}) =

*CHAPTER 2.* A*LGEBRAIC STRUCTURES*

TRI

T

.

***A*U**

2*.7. CYCLIC GROUPS* 2.7 Cyclic Groups

**Play**

*=* {*f(x*1 ... In) SEE XUX-1,2 = 1, ...,*,1* € N\*} = = {}(x1)..*. f(*I*n)* | I; E XUX-?, i = 1, ...,*1,*n € N\*} =< *F(*X) >. En

Recall that if (G, ) is a group and I EG, then the subgroup generated by x is

<< >= {rk | k € Z} *Remark.* If (G, +) is an additive group, then

personne

<3 >= *{kx*|k € Z}.

Throughout this section we will study those groups that are generated by a single element. They are essential tools in Group Theory.

Definition 2.7.1 A group *(G*, ) is called *cyclic* if there exists *E G* such that G*=<\**>, that is, *G* = {*\*\** | *k*€ Z}.

.

*Remark.* Notice that every cyclic group is commutative.

*ative.*

example 2.7.2 (a) The group (2, +) is cyclic, because

Z=<1>=< -1>.

CM

Recall that if M is a set, then

SM = {*f:*M *- M f* is bijective) is a group with respect to the composition of functions, called the *sym metric group o*f M. If M = *n*, then Sm is identified with the permuta tion group of n elements and is denoted by Sm.

A very important result is the following theorem, that tells us that it is enough to study symmetric (permutation) groups in order to know the structure of any other group. Theorem 2.6.11 (Cayley) *Every group is isomorphic to a subgroup of a symmetric group. Proof*. Let (G..) be a group and consider the symmetric group Sc. For ever*y a EG*, define

*t*a: *G* + G by ta (I) = ax, V*x*EG. Let us prove that t*a e* SG, that is, ta is bijective. If 21,1% E G such that *ta* (21) = *ta(*12), then *ax*1 = *AX2*, whence x1 = 22. Thus, *to* is injective. Furthermore*, Vy E G*, 3.x = *a-ly EG* such that ta*() = ax = y.* Thus, *to* is surjective, so that *t*a is bijective.

We may now define

*f*i*G* - SG by *f(a) =ta, Va EG.* Let us show that *f* is an injective homomorphism...

If *a, b E G* such that *f(a*) *f(*b), then t*a = th.* It follows that *ta*(1*) = td*(1), that is, *a = b*. Hence *f* is injective.

Now let *a, b E G*. We have to prove that

*fla.b) = f*(*a) o f(b)* or equivalently

*tab = to* o *to.* But this holds since VX E*G*,

*tab(x) = (ab)x = a(bx*) *= ta(bx) = ta(to*(x)) = *(ta o tz)*(I). Therefore, *f* is a homomorphism.

It follows that G Im*f*. But Im*f* <SG, so that we are done. O

Gisa e il nu

*(*6) The group (Zay, +) (*n* EN, *n* > 2) of residue classes modulo *n* is cyclic, because

7=< î>.

(c) The group *(U*m, *(*neN\*) of *n*-th roots of unity is cyclic. Indeed, *Un = {*Z ECM - 1} has n elements, namely

*2km.*

2k7 wroom \*iSiN -

*Ek*

COS

=

*27*

. + i sin

=

*K* = 0,1,...*,*-

1.

Then

*U*n =< E1>.

= 1 and

**Defini**tion 2*.*7.3 Let (G,) be a group and let : E *G.*

Then x is said to have *finite order* if Im EN\* such that 2 *infinite order* otherwise.

If x has finite order, then the non-zero natural number

ord x = minín EN

r

= 1}

2*.7. CYCLIC GROUPS*

90

*CHAPTER 2. ALGEBRAIC STRUCTURES*

is called the *order* of the element 1.

If G is finite, then the cardinal Gl is called the *order* of the group G and is denoted by ord *G*.

**Theorem** *2.7.7 Let (G,) be a group and let I EG.*

*(1) If o*rd *x = n, ihen*

<< >= {1,8, 22, ...,xn-1}

*Remark*. If *(*G, +) is an additive group and x has finite order, then

*and* | << >1=*n.*

*(22) If or*d *x* = 0*0, then*

ord x = min{n EN\* | nx=0}

i, *je Z, 2 \*j*

*mode,*

*so that <a> is infinite.*

**Exampl**e 2*.*7*.*4 *(a*) Consider the group (R\*, -). Then ordl = 1 and every & ER\* with <#1 has infinite order.

*(*6) Consider the group *(*Z6, +). Then ord 0 = 1, ord 1=6, ord 2 = 3, ord 3 = 2, ord 4 = 3, ord 5 = 6 and ord Zo.6. **Lemma 2***.7*.5 *Let (G,) be a group. Then:*

*(i) The unique element in G of order* 1 *is the identity element* 1.. *(ii) Va* EG, ordx-1 = ord x.

*Proof. (i*) Let *me* Z. By the Division Algorithm, there exist unique *9,7* EZ such that m *= ng* tor, where 0 <r <*n.* Then we may write

*Proof.* (i) Obvious.

*(ii*) Let n EN\*. For every I EG, we have

(2-1)" =1% 2n=1

= .

for some r E{0,..*.,1* -1}.

Suppose further that r = *x* for some *1, j*e {0,...*,n*-1}, say *j <i.* Then *r\_j* = 1 and 0 s*i- jn.* Since ord x = n, it follows that *¿-j* = 0, hence *1 =j.*

Therefore, <I>= { k {0, 1, ...*,7* - 1}} and <I>1*n.*

(*ii*) Suppose that ? = for some *i,j E*Z, say *j <.* Then -9 = 1, whence *į = j,* because otherwise ord I would be finite.

It follows that VrE*G*, ord x-1= ord x. Notice that one of the orders is finite iff the other one is finite as well.

**Theorer** 2.7.*8 Every subgroup of a cyclic group is cyclic.*

**Theorem** 2.*7.*6 *Let (G,) be a group, let eG with o*rd x *=n and let m* E N\**. Then:*

*2* = 1 *nm.*

*Proof.= .* Assume that m = 1. Using the Division Algorithm (see Theorem 2.15.3) for *in* and n, there exist unique *q, r* EN such that

*|*

*m = 3q* + T ,

0 < *n* < *n .*

Then

*\** = 29-na - 2M () ? =1, so that r = 0, because the order *n* is the least non-zero natural riumber *k* such that k = 1. But then *m = ng,* i.e., *nlm.*

. Assume now that *nm*. Then 3k E N such that *m = ng.* It follows that

2. T = 29 = (x^)=1.

*Proof*. Let *(*G,:) be a cyclic group, say G=< # >, and let *HSG.*

If *H =* {1}, then *H=*<1> is cyclic and we are done.

In the sequel, assume *H +* {1}. Then *H* contains positive powers of 2, since if \* *E H*, then <- *€ H* f*or* k E Z.

Choose

*n* = min{k € N\* | \*\* *€ H}.* We will prove that *H =*< >

Since n E *H, i*t follows that < >*CH. C*onversely, let um *€ H* for some *m* e Z. Then by the Division Algorithm, there exist unique *q, r* EZ such that

*n = Tq* +*T*, 3 < < *1 .*

Then

= 20 m-789 = 2m

(3")-9.