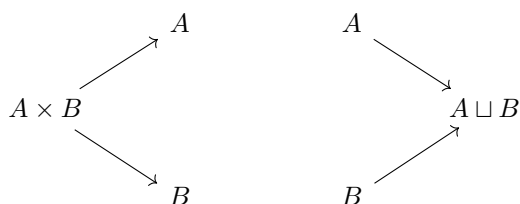


Algebra

Short Notes



I. Set Theory and Categories

1. Sets and Categories

1.1

Suppose that for any property, we can define a set whose members are items that satisfy that property. Then let $r = \{x : x \notin x\}$. Then $r \in r \iff r \notin r$.

In naive set theory and ZFC, this is avoided as the axiom schema of specification (for any property P and set S the set $\{s \in S : s \text{ satisfies } P\}$ exists) requires an existing set S . Also, a set of all sets cannot exist, as otherwise we can take S to be such a set.

1.2

Nonempty: any equivalence class $[a]$ contains a .

Disjoint: we wish to show that $[a] \neq [b] \implies [a] \cap [b] = \{\}$. Equivalently, $[a] \cap [b] \neq \{\} \implies [a] = [b]$. Suppose $c \in [a] \cap [b]$, and let $a' \in [a]$. Then $a' \sim a \sim c \sim b$, hence $[a] \subseteq [b]$. Similarly $[b] \subseteq [a]$.

Union is S : S contains the union as it contains every equivalence class by construction. Let $s \in S$. Then $s \in [s]$, hence the union contains S .

1.3

Define $a \sim b$ when there exists $p \in P$ such that $a \in p, b \in p$.

1.4

We count partitions. A partition will have 1, 2 or 3 parts. If it has 1 part it must be the whole set and if it has 3 parts it must be $\{[1], [2], [3]\}$. If it has 2 parts, exactly one part will have 2 items and the other 1 item, and we have 3 choices for the singleton part. Hence there are 5 equivalence relations.

1.5

For $a, b \in \mathbb{R}$ define $a \sim b$ when $|a - b| < 2$. Then $0 \sim 1$ and $1 \sim 2$ but $0 \not\sim 2$.

1.6

Reflexive: for $r \in \mathbb{R}$ we have $r \sim r$ since $r - r = 0 \in \mathbb{Z}$.

Symmetric: suppose $a \sim b$. Then $a - b \in \mathbb{Z}$. Then $b - a = -(a - b) \in \mathbb{Z}$, hence $b \sim a$.

Transitive: suppose $a \sim b, b \sim c$. Then $a - c = (a - b) + (b - c) \in \mathbb{Z}$.

Every class in \mathbb{R}/\sim is represented by a unique real number $r \in [0, 1)$, which is equivalent to all real numbers with that fractional part.

Every class in \mathbb{R}^2/\approx is represented by a unique pair of real numbers (r_1, r_2) with each $r_i \in [0, 1)$, which is equivalent to all pairs of real numbers whose fractional parts are the representative.

1. Functions between sets

2.1

$n!$

2.2

Let $f : A \rightarrow B$. We wish to show that f has a right-inverse iff it is surjective.

\implies : let $b \in B$. Suppose the right inverse is g ; then $f \circ g = id_B$ hence $b = f(g(b)) \in f(A)$.

\impliedby : we define $g : B \rightarrow A$ as follows. Let $b \in B$. Choose $a \in f^{-1}(b)$, which is nonempty since f is surjective, then set $g(b) = a$. Then g is a right inverse. Proof: for all $b \in B$ we have $f(g(b)) = f(a) = b$.

2.3

Let $f : A \rightarrow B$ be a bijection and f^{-1} its inverse. Since f^{-1} is a right inverse of f , we have $f \circ f^{-1} = id_B$ hence f is a left inverse of f^{-1} . By a similar argument, it is a right inverse as well; hence f^{-1} is a bijection.

Let $g : A \rightarrow B, f : B \rightarrow C$ be bijections. Then $(f \circ g) \circ (g^{-1} \circ f^{-1}) = id_C$, hence $f \circ g$ is surjective. By a similar argument, it is injective.

2.4

Reflexive: for any set A , $|A| = |A|$ since id_A is a bijection.

Symmetric: suppose $|A| = |B|$, that is, there is a bijection $f : A \rightarrow B$. Then $f^{-1} : B \rightarrow A$ is a bijection, hence $|B| = |A|$.

Transitive: suppose $|A| = |B|$, $|B| = |C|$ with bijections f and g . Then $f \circ g$ is a bijection between A and C .

2.5

A function $f : A \rightarrow B$ is an epimorphism (is epic) if for all sets Z and all functions $\alpha', \alpha'' : B \rightarrow Z$ we have $\alpha' \circ f = \alpha'' \circ f \implies \alpha' = \alpha''$. A function is surjective iff it is epic.

\implies : Let $f : A \rightarrow B$ be surjective and $\alpha', \alpha'' : B \rightarrow Z$ such that $\alpha' \circ f = \alpha'' \circ f$. Then f has a right inverse g and $\alpha' \circ f \circ g = \alpha'' \circ f \circ g$. Hence $\alpha' = \alpha''$.

\impliedby : Let $f : A \rightarrow B$ be epic and let $b \in B$. We wish to show that $b \in f(A)$. Let $Z = \{0, 1\}$ and suppose α' and α'' disagree only on b , that is, $\alpha'(c) = \alpha''(c) \iff c \neq b$. Then $\alpha' \neq \alpha''$. Suppose $b \notin f(A)$. Then for all $a \in A$, $\alpha' \circ f(a) = \alpha'' \circ f(a)$ (proof: $f(a) \neq b$, hence $\alpha'(f(a)) = \alpha''(f(a))$), which contradicts f is an epimorphism.

2.6

For any $f : A \rightarrow B$ define $\phi_f : A \rightarrow A \times B$ by $\phi_f(a) = (a, f(a))$. Then ϕ_f is a section (right inverse) of π_A . Proof: for all $a \in A$ we have $\pi_A \circ \phi_f(a) = \pi_A(a, f(a)) = a$. In fact every section of π_A corresponds to a unique function, since the $\pi_B(\pi_A^{-1}(x)) = B$.

2.7

For all $f : A \rightarrow B$ let $\phi_f : A \rightarrow \Gamma_f$ be given by $\phi(a) = (a, f(a))$. Then π_A is a left inverse of ϕ_f by exercise 2.6, hence ϕ_f is injective. Also ϕ_f is surjective. Proof: suppose $y = (a, b) \in \Gamma_f$. Then $b = f(a)$, hence $y = \phi_f(a)$.

2.8

The equivalence relation is: $r_1 \sim r_2 \iff e^{2\pi i r_1} = e^{2\pi i r_2} \iff r_1 - r_2 \in \mathbb{Z}$. Hence the surjection maps r to (the equivalence class represented by) its fractional part; \bar{f} maps $[r]$ to $e^{2\pi i r}$, with the unit circle as codomain; the injection is the inclusion map (of the unit circle in the complex plane).

2.9

Let the bijection between A' and A'' be f and the bijection between B' and B'' be g . Define a bijection $h : A' \cup B' \rightarrow A'' \cup B''$ as follows: $h(x)$ is $f(x)$ if $x \in A'$ otherwise $g(x)$. This is well-defined as exactly one of $x \in A'$, $x \in B'$ is true. The inverse can be defined explicitly similarly.

To form the disjoint union of A and B we produce disjoint copies; suppose we do this in one way to get A' and B' , and another way to get A'' and B'' . Since they are copies, $A' \cong A''$, $B' \cong B''$, hence the disjoint unions are isomorphic (as sets).

2.10

Any function from A to B is defined by the value of $f(a)$ for all $a \in A$; the choice for each a is independent, there are $|A|$ choices and for each choice we may choose $|B|$ ways, so there are $|A| \times |A| \times \dots \times |A|$ different functions.

For an explicit bijection, we can use the fact that any finite set can be well-ordered to order the elements of $|B^A|$ lexicographically on their valuations $(f(a_1), f(a_2) \dots)$.

2.11

A subset $S \subseteq A$ is determined uniquely by its indicator function $f_S \in 2^A$ given by $f_S(a) = 0 \iff a \in S$.

3. Categories

3.1

We compose two morphisms in C^{op} by composing the two underlying morphisms in C “the other way”. That is, suppose $f \in \text{Hom}_{C^{op}}(A, B) = \text{Hom}_C(B, A)$ and $g \in \text{Hom}_{C^{op}}(B, C) = \text{Hom}_C(C, B)$. Let composition in C be denoted by \cdot and composition in C^{op} by \circ . Then define their composition $g \circ f = f \cdot g$.

1. The identity homomorphism exists because $1_A \in \text{Hom}_C(A, A) = \text{Hom}_{C^{op}}(A, A)$.
2. We explicitly constructed the composition in C^{op} , hence it exists.
3. $(f \circ g) \circ h = h \cdot (g \cdot f) = (h \cdot g) \cdot f = f \circ (g \circ h)$.
4. $f \circ 1_A = 1_A \cdot f = f$; similar proof for left inverse.

3.2

$$|\text{End}(A)| = |\text{Hom}(A, A)| = |A^A| = |A|^{|A|}.$$

3.3

That means it is a left and right identity. Left identity means for all morphisms $f : a \rightarrow b$, $1_b f = f$. Proof that 1_b is a left identity: let $f : a \rightarrow b$. By our definition of composition, $1_b f = (a, b)$ (let $c = b$ on p21), which is identically f . The proof for right identity is similar.

3.4

No, since $n \not\prec n$, so $\text{Hom}(n, n)$ is empty.

3.5

\subseteq in 3.4 is the \sim relation in 3.3 (that is required to be reflexive and transitive).

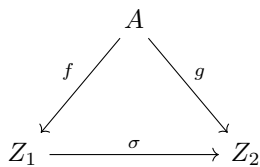
3.6

1. Let the identity in V be the identity matrix.
2. Let $f : x \rightarrow y, g : y \rightarrow z$. The composition gy is exactly the matrix product gy , which is the correct size ($gy : x \rightarrow z$ is a $z \times y$ matrix).
3. Associativity follows from associativity of matrix multiplication.
4. The identity matrix is an identity with respect to matrix multiplication.

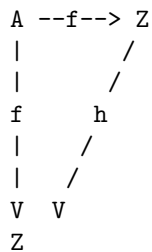
An object n of this category can be thought of as \mathbb{R}^n , and the morphisms $\text{Hom}(m, n)$ as linear functions $\mathbb{R}^m \rightarrow \mathbb{R}^n$. (Eg use the standard basis on \mathbb{R}^m and \mathbb{R}^n to convert a linear function to an appropriately sized matrix).

3.7

Let us denote this category as C^A . Then the objects of C^A are morphisms of C . Given two objects in $f, g \in \text{Obj}(C^A)$, suppose $f \in \text{Hom}_C(A, Z_1)$ and $g \in \text{Hom}_C(A, Z_2)$. Define a C^A -morphism from f to g to be a C -morphism σ such that the diagram commutes.

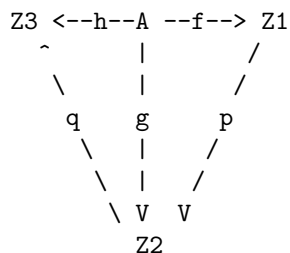


1. An identity C^A -morphism on the C^A -object f is a C -morphism h such that



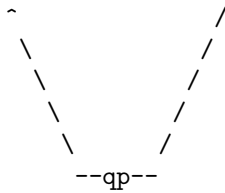
commutes; 1_Z does the job.

2. Suppose f, g, h are C^A -objects and p is a C^A -morphism from f to g and q is a C^A -morphism from g to h . Then the following diagram commutes.



By removing the vertical line and composing p and q ,

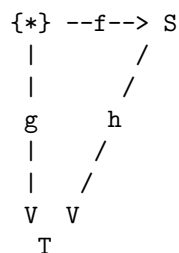




commutes; hence define composition in C^A as composition in C .

3. Associativity follows from associativity in C .

We will also verify the claim in example 3.8.



The requirement is that h commutes, that is, considered as set-functions, $g = h \circ f$. Since g is completely determined by its value on $*$, this means $g(*) = h(f(*))$, or $t = h(s)$.

3.8

The objects of C are infinite sets and the morphisms in C are set-functions between them (that is we define $\text{Hom}_C(A, B) = \text{Hom}_{\text{Set}}(A, B)$, forcing C to be a full subcategory of Set). Identity, composition and associativity all follow from Set .

3.9

WIP

A function maps between two sets; we must generalize this concept to allow for maps between two multisets. How we do this determines the structure of morphisms in MSet . (In all cases, though, members of $\text{Obj}(\text{MSet})$ will be pairs (S, \sim) where \sim is an equivalence relation on S).

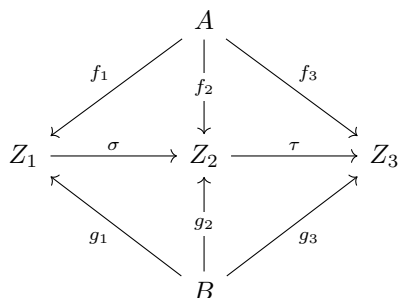
1. We can treat (S, \sim) as a partitioned set; then mfunctions between them will be functions between partitions.
2. We can simply inherit the morphisms from S , allowing morphisms to ignore \sim altogether. The downside is that mfunctions are now sensitive to which representative of a given element you feed it.
3. We can generalize functions to "multivalued functions" (eg the $z \rightarrow z^{1/3}$ operator on \mathbb{C}); TBD
4. We can generalize functions to "regular functions whose image contain elements with multiplicities"; for finite multiplicities this is like a regular function $x \rightarrow (y, n)$ where x, y are our conceptual domain and codomain and n is the multiplicity. A contrived example is: given a fixed function f over \mathbb{R} , we could map x to (y, n) where $y = f(x)$ and n is the algebraic multiplicity of the root of the function $f'(t) = f(t) - f(x)$ at y (hence n would mostly be 1, and at stationary points it would increase).

3.10

The object $\Omega = \{0, 1\}$ will do. A subobject (subset) A' of an object (set) A can be identified with a morphism (set-function) $f : A \rightarrow \Omega$ by setting $a \in A' \iff f(a) = 1$.

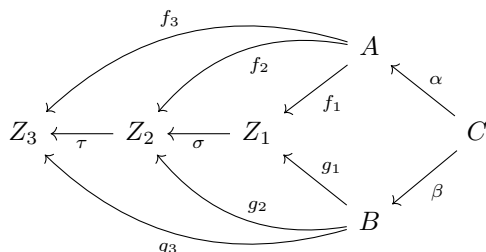
3.11 - $C^{A,B}$

A $C^{A,B}$ -object is a pair of C -morphisms (f, g) . A $C^{A,B}$ -morphism between (f_1, g_1) and (f_2, g_2) is a C -morphisms σ such that $f_2 = \sigma f_1$ and $g_2 = \sigma g_1$. Composition is inherited from C .



3.11 - $C^{\alpha,\beta}$

Let $\alpha : C \rightarrow A$ and $\beta : C \rightarrow B$. A $C^{\alpha,\beta}$ -object is a pair of C -morphisms (f, g) with a common target Z such that $f\alpha = g\beta$. A $C^{\alpha,\beta}$ -morphism between objects (f_1, g_1) with common target Z_1 and (f_2, g_2) with common target Z_2 is a C -morphism $\sigma : Z_1 \rightarrow Z_2$ such that $f_2 = \sigma f_1$ and $g_2 = \sigma g_1$.



4. Morphisms

4.1

Proof omitted.

4.2

They are relations which are also symmetric. Proof: let C be a category of this kind and let $A \sim B$, that is, $f \in \text{Hom}_C(A, B)$. By the groupoid property there exists a left inverse $g \in \text{Hom}_C(B, A)$, hence $\text{Hom}_C(B, A)$ is nonempty, hence $B \sim A$.

4.3

Let $\beta' \circ f = \beta'' \circ f$. Let g be a left inverse of f . Then $\beta' \circ f \circ g = \beta'' \circ f \circ g$, hence $\beta' = \beta''$.

TBD

4.4

As long as $Obj(C)$ is nonempty, the structure $C_{nonmono}$ constructed as such cannot work since the identity function is a monomorphism, hence not a homomorphism in $C_{nonmono}$.

4.5

TBD

5. Universal Properties

5.1

Let Z be final in C . Consider Z as an element of C^{op} and let Z' be any element of C^{op} . There is a unique C -morphism between Z and Z' , hence there is a unique C^{op} -morphism between Z' and Z .

5.2

0 is initial since for all sets S there is a unique function from 0 to S , the empty function. Let $T \neq 0$ be a set. Then T must have at least one element, say $t \in T$. Consider $Hom(T, P)$ where $P = \{a, b\}$ where $a = \{\}, b = \{a\}$ is a set with two elements. If $Hom(T, P)$ is nonempty, say $f \in Hom(T, P)$, then either $f(t) = a$ or $f(t) = b$; either way we can construct f' which differs from f in its value of t .

5.3

Let F be final. We show that there is a unique automorphism. This follows because F is final and an automorphism is $F \rightarrow F$.

Let F_1, F_2 be final. We show that there is a unique isomorphism between F_1 and F_2 . Since F_1 is final there is a unique morphism $f : F_2 \rightarrow F_1$. It suffices to show that f is an isomorphism. Since F_2 is final there is a unique morphism $g : F_1 \rightarrow F_2$. Then $gf = 1_{F_2}$ and $fg = 1_{F_1}$.

5.4

Let (I, i) be an initial member of Set^* . Then there must be exactly one morphism from (I, i) to any other object (S, s) . All singleton sets (that is, $(\{i\}, i)$) are initial, since given any (S, s) the unique morphism maps i to s . All non-singleton sets are not initial since there are at least two morphisms to (S, s) for $|S| > 1$.

Let (F, f) be a final member of Set^* . Then there must be exactly one morphism from any other object (S, s) to (F, f) . All singleton sets are final with the morphism mapping s to f . All non-singleton sets are not final (same argument as above).

5.5

We define the category C explicitly. A C -object is a Set-morphism $\sigma : A \rightarrow Z$ such that $a \sim a' \implies \sigma(a) \sim \sigma(a')$, and C -morphisms between σ_1 and σ_2 are Set-morphisms f such that $\sigma_2 = f\sigma_1$. The final

objects in this category are the Set-morphisms whose target are singleton sets.

5.6

Let m, n be objects of this category and let f be a final objects in $C_{m,n}$. Then $f|m$ and $f|n$. Furthermore, for all f' such that $f'|m$ and $f'|n$ we must have $f'|f$. Hence f is the gcd of m and n .

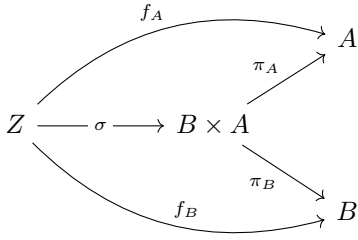
Let f be an initial object in $C^{m,n}$. Then $m|f$ and $n|f$. Furthermore, for all f' such that $m|f'$ and $n|f'$, we have $f|f'$. Hence f is the lcm of m and n .

5.7

The definition of $A \sqcup B$ given makes it a coproduct in Set , since it satisfies the universal property of coproducts.

5.8

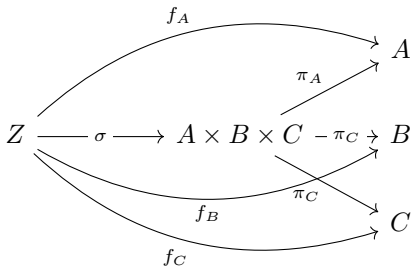
We need to show that a final object of $C_{B,A}$ is final in $C_{A,B}$. Let f be any final object in $C_{B,A}$, that is, f consists of an element $B \times A$ of C together with morphisms $\pi_A : B \times A \rightarrow A$ and $\pi_B : B \times A \rightarrow B$. Then f is final in $C_{A,B}$. Proof: let Z be any element of C and f_A, f_B be morphisms from Z to A and B respectively. By finality of f in $C_{B,A}$, there exists a unique morphism σ such that the following diagram commutes.



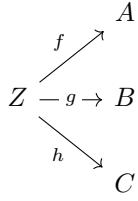
Hence f is final in $C_{A,B}$.

5.9

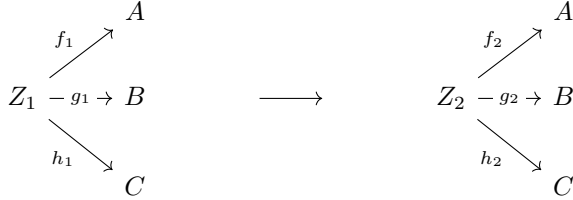
Let A, B, C be sets. Then the product $A \times B \times C$ is universal with respect to following property: for any Y and morphisms $f_A : Y \rightarrow A, f_B : Y \rightarrow B, f_C : Y \rightarrow C$ there is a unique morphism $\sigma : Y \rightarrow A \times B \times C$ such that the following diagram commutes.



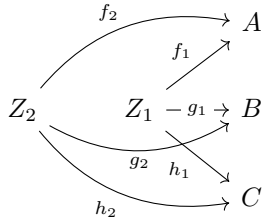
In other words, $A \times B \times C$ is final in the category $C_{A,B,C}$. We now define this category. Objects in this category are diagrams



in C , and morphisms



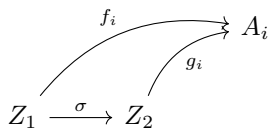
are commutative diagrams



We show that $(A \times B) \times C$ satisfies this universal property. The function σ defined by $\sigma(z) = ((f_A(z), f_B(z)), f_C(z))$ makes the diagram commute.

5.10

Let C be a category and $S = \{A_i : i \in I\}$ be an indexed set of objects of C . Define the category C_S as follows. An object in C_S consists of an object Z in C together with indexed morphisms $\{f_i : Z \rightarrow A_i\}$ where $f_i : Z \rightarrow A_i$. A morphism in C_S between $(Z_1, \{f_i : i \in I\})$ and $(Z_2, \{g_i : i \in I\})$ is a morphism $\sigma : Z_1 \rightarrow Z_2$ in C such that for all $i \in I$ the following diagram commutes.

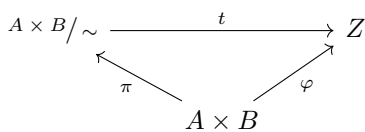


(If I is sufficiently small, we can convert this condition into the commutativity of a big diagram.)

5.11.1

check: <https://math.stackexchange.com/questions/242149/problem-1-5-11-in-aluffis-algebra-chapter-0>

The universal property says that for all ϕ, Z for which $(a_1, b_1) \sim (a_2, b_2) \implies \phi((a_1, b_1)) = \phi((a_2, b_2))$ there exists a unique t such that the following diagram commutes



Let $Z = A / \sim_A$ and φ be defined by

$$\begin{array}{ccccc}
 & & \varphi & & \\
 & \nearrow & & \searrow & \\
 A \times B & \xrightarrow{\pi_A} & A & \xrightarrow{\pi} & A/\sim_A
 \end{array}$$

where π is any representative-choice function $A \rightarrow A/\sim_A$ (such a function is included in the definition of A/\sim_A). By the above, there exists a set-function $A \times B/\sim \rightarrow A/\sim_A$.

5.11.2

Lemma. The representative-choice function has an inverse. Proof: by using the universal property of quotients,

$$\begin{array}{ccc}
 A/\sim & \xrightarrow{\exists!} & A \\
 \nwarrow \pi & & \nearrow id \\
 & A &
 \end{array}$$

Let the functions be labelled as such:

$$\begin{array}{ccc}
 & & A/\sim_A \\
 & \nearrow \pi_a & \\
 A \times B/\sim & & \\
 & \searrow \pi_b & \\
 & & B/\sim_B
 \end{array}$$

Note that this is an element of $Set_{A/\sim_A, B/\sim_B}$. Let the following be another element.

$$\begin{array}{ccc}
 & \frac{A}{\sim_A} & \\
 f_A \nearrow & & \\
 Z & & \\
 f_B \searrow & & \\
 & \frac{B}{\sim_B} &
 \end{array}$$

We wish to show that there is a unique $\sigma : Z \rightarrow A \times B/\sim$ such that the combined diagram commutes. Consider the following diagram.

$$\begin{array}{ccccc}
 & & f_A & \xrightarrow{\quad} & A/\sim_A \xrightarrow{\exists!} A \\
 & \nearrow & & \nearrow & \\
 & & \text{dotted line} & & \\
 Z & \xrightarrow{\quad} & A \times B/\sim & \xleftarrow{\pi_\sim} & A \times B \xrightarrow{\quad} B/\sim_B \xrightarrow{\exists!} B \\
 & \searrow & & \searrow & \\
 & & f_B & \xrightarrow{\quad} &
 \end{array}$$

By the universal property of $A \times B$, the dotted line is inhabited by a unique set-function. Its composition with π_\sim provides the required σ .

5.12

tbd. “pullback”.

2. Groups

1.4

It suffices to show that $ghg^{-1}h^{-1} = 1$ for all g, h . This is true because it is $(gh^{-1})^2$.

1.6

Let G be a group. We know $1 \in G$. Hence if $|G| = 1$ then $G = \{e\}$.

If $|G| = 2$ then $G = \{1, x\}$. The multiplication table is

	1	x
1	1	x
x	x	

The last spot must be 1.

If $|G| = 3$ then $G = \{1, x, y\}$. Suppose $x^2 = 1$. Then

	1	x	y
1	1	x	y
x	x	1	
y	y		

No choice is possible for the value of xy . Hence $x^2 = y$.

	1	x	y
1	1	x	y
x	x	y	1
y	y	1	x

Let $|G| = 4, G = \{1, x, y, z\}$. The table is

	1	x	y	z
1	1	x	y	z
x	x			
y	y			
z	z			

Either $x^2 = 1, y$ or z . The later two cases are equivalent by relabeling. In the first case,

	1	x	y	z
1	1	x	y	z
x	x	1	z	y
y	y	z		
z	z	y		

Either the remaining diagonal entries are 1 (giving us the table for $C_2 \times C_2$) or they are x (giving us the table for C_4).

In the other case,

	1	x	y	z
1	1	x	y	z
x	x	y	z	1
y	y	z	1	x
z	z	1	x	y

which is the table for C_4 .