Prove that κ satisfies conditions (i)–(iv) of Theorem 3.4. (κ is called the *cofinite topology* on S.)

3.41 A subset C of a topological space S with topology τ is called **closed** if C' is open, that is, $C' \in \tau$. Reformulate conditions (i)–(iv) of Theorem 3.4 in terms of the family $\sigma = \{C \subseteq S \mid C' \in \tau\}$ of closed sets.

3.42 The collection $\mathcal{T}$ of all topologies τ on a set S is a family of subsets of $\mathcal{P}(S)$ (hence, a subset of $\mathcal{P}(\mathcal{P}(S))$ and an element of $\mathcal{P}(\mathcal{P}(\mathcal{P}(S)))$!). Does $\mathcal{T}$ form a topology of $\mathcal{P}(S)$ or not?

From: Elements of Logic via Numbers and Sets. D.L. Johnson, Springer, 1998.

4 Relations

"*Lexicographer.* A writer of dictionaries,
a harmless drudge."
S. Johnson
Dictionary of the English Language

Various relations exist between things of the same kind. Thus, if $a, b \in P = \{$all living human beings$\}$, the relation σ of sisterhood may be expressed by writing $a \,\sigma\, b$ if a is a sister of b. Again, the relation $\mid$ of divisibility exists on the set $\mathbb{Z}$ of all integers: $a \mid b$ if a divides b. In general, a given relation ρ on a set S may or may not hold between two elements $a, b \in S$. Listing or otherwise describing the ordered pairs (a, b) for which it does hold defines the relation. This leads to the following definition, which is a nice example of how to attach a precise mathematical meaning to an everyday word.

Definition 4.1

A (binary) **relation** ρ on a set S is a subset of $S \times S : \rho \subseteq S \times S$. We often write $a \,\rho\, b$ instead of $(a, b) \in \rho$.

This very general definition encompasses two particularly important but very different special types of relation, equivalence relations and orderings, which we will study in turn in this chapter.

4.1 Equivalence Relations

We shall start by defining three properties that a particular relation ρ on a given set S may or may not have. Such a relation is called

$$\begin{array}{lll} \textit{reflexive} & \text{(R)} & \text{if} \quad \forall a \in S \quad a \,\rho\, a, \\ \textit{symmetric} & \text{(S)} & \text{if} \quad a \,\rho\, b \Rightarrow b \,\rho\, a, \\ \textit{transitive} & \text{(T)} & \text{if} \quad a \,\rho\, b \wedge b \,\rho\, c \Rightarrow a \,\rho\, c, \end{array}$$

where a, b and c denote elements of S.

To illustrate these general properties, we extend the meagre list of examples given above,

1 sisterhood on P,

2 divisibility on $\mathbb{Z}$,

by adding a few more.

3 Equality on any subset S is defined by the **diagonal subset**

$$\Delta = \{(s,s) \mid s \in S\} \subseteq S \times S;$$

$s = t \Leftrightarrow (s,t) \in \Delta$.

4 For $a, b \in \mathbb{R}$, write $a \leq b$ if $b - a$ is non-negative.

5 For $a, b \in \mathbb{Z}$, write $a \equiv b$ if $a - b$ is a multiple of 5.

6 For any set S and $A, B \in \mathcal{P}(S)$, write $A \nsubseteq B$ if A is not contained in B.

7 Let S be any set and π any partition of S. Then write $a \equiv b$ for $a, b \in S$ if b belongs to the same member P of π as a.

8 Given $(a,b), (c,d) \in \mathbb{N} \times \mathbb{N}$, write $(a,b) \sim (c,d)$ if $a + d = c + b$.

9 Given $(a,b), (c,d) \in \mathbb{Z} \times \mathbb{N}$, write $(a,b) \sim (c,d)$ if $ad = cb$.

10 Let $\mathbb{R}[x]$ denote the set of all polynomials in an indeterminate x with real coefficients. Then for $f(x), g(x) \in \mathbb{R}[x]$, write $f(x) \sim g(x)$ if $f(x) - g(x) = (x^2 + 1)h(x)$ for some $h(x) \in \mathbb{R}[x]$.

Table 4.1 shows which of these ten relations have which of these three properties. The first seven rows are more or less obvious, and the last three are exercises to which we shall return in Section 3 below. We shall also refer again to row 5 in the next section and to row 7 in a moment, but first, we will look at the main definition.

Table 4.1. Properties of same.

	relation	set	R	S	T
1	σ	P			✓
2	$\mid$	$\mathbb{Z}$	✓		✓
3	$=$	S	✓	✓	✓
4	$\leq$	$\mathbb{R}$	✓		✓
5	$\equiv$	$\mathbb{Z}$	✓	✓	✓
6	$\nsubseteq$	$\mathcal{P}(S)$			
7	$\equiv$	S	✓	✓	✓
8	$\sim$	$\mathbb{N} \times \mathbb{N}$	✓	✓	✓
9	$\sim$	$\mathbb{Z} \times \mathbb{N}$	✓	✓	✓
10	$\sim$	$\mathbb{R}[x]$	✓	✓	✓

Definition 4.2

A relation ρ on a set S that is reflexive, symmetric and transitive is called an **equivalence relation** on S.

It is pretty clear that any partition π of a set S determines an equivalence relation on S (in accordance with row 7 of Table 4.1, where it is written $\equiv$). Less obvious but more important is the converse of this statement, and we now begin to work towards the derivation of this fact.

So let $\sim$ denote a fixed equivalence relation on a given set S. Then for any $a \in S$ the set

$$[a] = \{b \in S \mid b \sim a\}$$

is called the **equivalence class** of a. Of course $[a]$ depends on $\sim$ as well as a, and $[a] \subseteq S$. We will prove two facts about equivalence classes. First, every element $a \in S$ belongs to at least one equivalence class: $a = a \in [a]$ because $\sim$ is reflexive. Second, no element $a \in S$ can belong to two different equivalence classes, that is, for $a, b, c \in S$,

$$b \in [a] \wedge b \in [c] \Rightarrow [a] = [c]. \tag{4.1}$$

This is proved using the symmetry and transitivity of $\sim$ as follows. First,

$$\begin{array}{rcl} b \in [a] & \Rightarrow & b \sim a, \text{ by definition, and} \\ b \in [c] & \Rightarrow & b \sim c \Rightarrow c \sim b \text{ by (S)}, \end{array}$$

so that $b \sim a$ and $c \sim b$, and $c \sim a$ by (T). Then, using (T) again,

$$d \in [c] \Rightarrow d \sim c \Rightarrow d \sim a \Rightarrow d \in [a],$$

and we have shown that every element d of $[c]$ belongs to $[a]$, that is, $[c] \subseteq [a]$. Finally, by reversing the roles of a and c in the above argument, we obtain $[a] \subseteq [c]$, so that $[a] = [c]$ as claimed.

The two facts we have just established respectively assert that every element of S belongs to at least one equivalence class and to at most one equivalence class, that is, to *exactly one*, and we have proved the following theorem.

Theorem 4.1

If $\sim$ is an equivalence relation on a set S, then the distinct equivalence classes

$$[a] = \{b \in S \mid b \sim a\}, \qquad a \in S,$$

form a partition of S. □

It turns out that if our equivalence relation $\sim$ comes from a partition π of S, then the resulting equivalence classes are just the members of π. Conversely, starting from an equivalence relation $\sim$, if π is the resulting partition into equivalence classes, then the equivalence relation determined by π is just $\sim$. We thus have a *one-to-one correspondence* between partitions of S and equivalence relations on S. (The notion of one-to-one correspondence, or bijection, will be made precise in the next chapter.) The point is that equivalence relations are easy to set up, whereas partitions are useful, so that Theorem 4.1 is important for practical reasons. Two such applications will be described in the next two sections.

EXERCISES

4.1 Given a set S, which of the properties (R), (S), (T) hold for the relation $a \neq b$ of inequality?

4.2 Which of the properties (R), (S), (T) hold for the relation $\subseteq$ of containment on $\mathcal{P}(S)$?

4.3 Prove that the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ given in Example 8 is an equivalence relation.

4.4 Do the same for the relation $\sim$ on $\mathbb{Z} \times \mathbb{N}$ in Example 9.

4.5 The same again for the relation $\sim$ on $\mathbb{R}[x]$ in Example 10.

4.6 What is wrong with following "proof" that property (R) of a relation ρ is a consequence of properties (S) and (T)?

First, $a \rho b \Rightarrow b \rho a$ by (S) . Then $a \rho b$ and $b \rho a \Rightarrow a \sim a$ by (T). Hence ρ is reflexive.

4.7 Any set S admits the trivial partition τ into singletons:

$$\tau = \{\{s\} \mid s \in S\}.$$

Describe the corresponding equivalence relation.

4.8 Describe the partition obtained in accordance with Theorem 4.1 from the equivalence $\equiv$ of Example 5.

4.9 For $x \in \mathbb{R}$, define the **integer part** $[x]$ to be the largest integer $\leq x$. (So $[\pi] = 3$, $[2] = 2$, $[-\frac{1}{2}] = -1$.) Prove that the relation

$$x \sim y \Leftrightarrow [x] = [y]$$

is an equivalence relation on $\mathbb{R}$, describe the equivalence classes and write down a transversal for them. [Note. There is ambiguity of notation here, which unfortunately is traditional. For the purposes of this question, use (x) for the equivalence class of x in $\mathbb{R}$.]

4.10 Write down an upper bound for the number of equivalence classes on a finite set with n elements.

4.11 Prove that the condition

$$a \equiv b \Leftrightarrow a - b \in \mathbb{Z}$$

defines an equivalence relation on the set $\mathbb{Q}$ of rational numbers. Find a transversal T for the equivalence classes.

4.2 Congruences

We focus attention on the relation $\equiv$ in Example 5 of the previous section. Since it depends crucially on the positive integer 5, we incorporate this into our notation and write it more precisely as follows: for $a, b \in \mathbb{Z}$,

$$a \equiv b \pmod 5 \Leftrightarrow 5 \mid (a - b),$$

where the left-hand part is pronounced "a is congruent to b modulo 5" and referred to as a **congruence** (modulo 5).

Let us illustrate Theorem 4.1 in the previous section by working out what the equivalence classes are (as in the solution of Exercise 1.8). For a given $a \in \mathbb{Z}$, divide a by 5 in accordance with Theorem 1.14 to get

$$a = 5q + r, \qquad 0 \leq r \leq 4.$$

Thus, $a \equiv r \pmod 5$ and so

$$a \in [r], \qquad 0 \le r \le 4,$$

and there are exactly five equivalence classes:

$$[0] = 5\mathbb{Z},\ [1] = 1 + 5\mathbb{Z},\ [2] = 2 + 5\mathbb{Z},\ [3] = 3 + 5\mathbb{Z},\ [4] = 4 + 5\mathbb{Z},$$

which is just the partition into residue classes modulo 5 (see Section 3.4). The fact that these five classes are pairwise disjoint is expressed mathematically as follows:

$$k, l \in \mathbb{Z} \quad 0 \le k, l \le 4, \qquad k \equiv l (\mathrm{mod}\ 5) \Rightarrow k = l.$$

It turns out to be possible to add and multiply these classes very much as if they were ordinary individual numbers:

$$[k] + [l] = [k + l], \qquad [k]\,[l] = [kl]. \tag{4.2}$$

But notice that there is something (rather subtle) here that requires proof. Take the first equation in (4.2). To define $[k] + [l]$, we *choose* elements k, l from each class, add them up, and take the residue class of their sum. But if we made different choices, say $k' \in [k]$ and $l' \in [l]$, how do we know that the result $[k' + l']$ is the same as $[k + l]$? What has to be checked is that the operations in (4.2) are *well-defined*, that is, independent of the choice of representatives from $[k]$ and $[l]$.

That this is indeed the case is expressed mathematically as follows:

$$k' \in [k] \wedge l' \in [l] \Rightarrow [k' + l'] = [k + l] \wedge [k'\,l'] = [k, l],$$

or, more conveniently in terms of congruences,

$$k' \equiv k (\mathrm{mod}\ 5) \wedge l' \equiv l (\mathrm{mod}\ 5) \Rightarrow k' + l' \equiv k + l (\mathrm{mod}\ 5) \wedge k'\,l' \equiv kl (\mathrm{mod}\ 5), \tag{4.3}$$

and we shall prove this now.

Since our hypothesis assert that $k' - k$ and $l' - l$ are both divisible by 5, we can write

$$k' = k + 5a, \quad l' = l + 5b, \qquad a, b \in \mathbb{Z}.$$

Then

$$k' + l' = (k + l) + 5(a + b), k'\,l' = kl + 5(kb + la + 5ab).$$

Since these numbers differ by a multiple of 5 from $k + l$, kl respectively, the conclusion of (4.3) follows.

There is an obvious transversal $T = \{0, 1, 2, 3, 4\}$ for these classes. To avoid the tiresome square brackets, we sometimes replace each class by its representative in T. When this is done, the addition and multiplication tables in

Table 4.2. Addition and multiplication of integers modulo 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	1	0
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

arithmetic modulo 5 are as shown in Table 4.2. Thus, the entries in the $(2, 4)$ places respectively assert that

$$2 + 4 \equiv 1 \pmod 5, \quad 2.4 \equiv 3 \pmod 5.$$

All that we have said so far generalizes nicely from the case $n = 5$ to that of an arbitrary positive integer n (assumed greater than 1 to avoid triviality). In particular, the formulae in (4.2) can be taken as the definition of the sum and product of the residue classes $[k], [l]$ modulo n, $0 \le k, l \le n - 1$. Thus, we can take $T = \{k \in \mathbb{Z} \mid 0 \le k \le n - 1\}$ as a transversal and then the definitions of addition and multiplication modulo n take the form

$$k + l = r, \qquad kl = s,$$

where r, s are the remainders $0 \le r, s \le n - 1$ on dividing $k + l$, kl respectively by n. Independence of choice of representatives is checked in the same way as for $n = 5$ above (see Exercise 4.1) and the resulting set of n residue classes is denoted by $\mathbb{Z}/n\mathbb{Z}$, the "integers modulo n":

$$\mathbb{Z}/n\mathbb{Z} = \{[k] \mid 0 \le k \le n - 1\}.$$

Here $[k]$ denotes the residue class of k modulo n, often abbreviated to k for convenience. We can now state the following theorem, whose proof is left to the exercises (Exercises 4.12–4.16).

Theorem 4.2

(i) The operations of addition and multiplication modulo n are well defined.

(ii) The set $\mathbb{Z}/n\mathbb{Z}$ forms a commutative ring-with-1 under these operations.

(iii) $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. □

What this theorem means in practical terms is that residue classes modulo n can be treated in much the same way as individual numbers in arithmetic. Congruences play the role of equations and are manipulated in a similar way.

The resulting theory of congruences forms an important part of elementary number theory.

To conclude this section, we observe that the type of partition just described can be generalized from $\mathbb{Z}$ to any group G, where the role of $n\mathbb{Z}$ is played by an arbitrary subgroup H of G. The members of the corresponding partition are called **cosets** in this context, and they play a fundamental role in group theory. A word of caution, however, is appropriate in this general case. While the cosets always partition the group, they do not always inherit the group operation. If G is abelian, the natural multiplication of cosets is well defined, but if it isn't the subgroup H needs to be of a special kind, namely, a *normal* subgroup.

EXERCISES

4.12 Show that the sum and product of residue classes $[k], [l]$ modulo n are well defined by the formula (4.2).

4.13 Prove that $\mathbb{Z}/n\mathbb{Z}$ inherits from $\mathbb{Z}$ the five universal laws:

$$(a+b)+c=a+(b+c), \quad a+b=b+a,$$
$$(ab)c=a(bc), \quad ab=ba, \quad a(b+c)=ab+ac,$$

in the eight axioms for a ring-with-1.

4.14 Prove that $\mathbb{Z}/n\mathbb{Z}$ satisfies the three existential laws:

$$\exists \text{ additive identity, } \exists \text{ multiplicative identity,}$$
$$\exists \text{ additive inverse for every element,}$$

in the eight axioms for a ring-with-1.

4.15 Show that if n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

4.16 Use Theorem 1.15 to show that $\mathbb{Z}/n\mathbb{Z}$ is a field when n is a prime.

4.17 Let $[a]$ be a residue class modulo n, $0 \leq a \leq n-1$. Show that $[a]$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if and only if a and n are coprime, $(a,n)=1$.

4.18 What are the residue classes modulo 2 better known as?

4.19 Let A be the residue class of 1 modulo 3 and B that of -1 modulo 4. Prove that $A \cap B$ is a residue class modulo 12.

4.3 Number Systems

In the previous section, an equivalence relation was used to construct a new number system from an old one: the relation on $\mathbb{Z}$ of congruence modulo n led to the construction of $\mathbb{Z}/n\mathbb{Z}$. We continue this theme now, but with the difference that the new systems we construct will be *bigger* than the old ones. In each case, the new system will contain the old one and will enjoy the advantage of containing the solutions to more equations than did the old one. We shall construct three number systems using Examples 8, 9, 10 from Section 1 in turn.

Recall Example 8, where the equivalence relation $\sim$ is defined on $\mathbb{N} \times \mathbb{N}$ by

$$(a,b) \sim (c,d) \Leftrightarrow a+d=c+b. \tag{4.4}$$

The old number system here is $\mathbb{N}$, and the new one consists of the equivalence classes $[(a,b)]$ of this relation, which we will abbreviate to $[a,b]$ for the sake of convenience.

First notice that we can subtract any $k \in \mathbb{N}$ from both a and b to get an equivalent pair, provided $k < \min(a,b)$:

$$(a,b) \sim (a-k, b-k).$$

It follows that every class $[a,b]$ contains a special pair, that is, one in which at least one of the components is equal to 1. Moreover, there is only one such pair in each class:

$$(1,b)=(1,d) \Rightarrow b=d, \ (a,1)=(b,1) \Rightarrow a=b, \ (a,1)=(1,b) \Rightarrow a=b=1.$$

The special pairs thus form a transversal,

$$T=\{(1,n+1) \mid n \in \mathbb{N}\} \cup \{(1,1)\} \cup \{(n+1,1) \mid n \in \mathbb{N}\}. \tag{4.5}$$

Next, attempt to define the addition of classes in a natural way:

$$[a,b]+[c,d]=[a+c,b+d]. \tag{4.6}$$

As in the previous section, we need to check for independence of representatives (Exercise 4.20) in order that this operation be well defined. The effect of this operation on the members of T works out as follows.

$$\forall (a,b) \in \mathbb{N} \times \mathbb{N}, \ [a,b]+[1,1]=[a+1,b+1]=[a,b] \tag{4.7}$$

so that $[1,1]$ is an *identity* for this $+$. Next,

$$\begin{aligned} [m+1,1]+[n+1,1] &= [m+n+2,2]=[(m+n)+1,1], \\ [1,m+1]+[1,n+1] &= [2,m+n+2]=[1,(m+n)+1]. \end{aligned} \tag{4.8}$$