An Introduction to

Abstract Algebra

Volume I: Group Theory

by

Steven Roman
www.sroman.com

To Donna

Preface

The Philosophy of This Book

First, a word about the philosophy of this book. The current trend in mathematical education is to motivate abstract concepts by introducing *applications* as quickly as possible, in an effort to satisfy those students whose overriding question is "of what use is this material?"

On the other hand, while I certainly respect the views of those whose main concern is whether or not the subject matter at hand has applications to the real world, I have chosen to take a more abstract approach to the subject at hand. I am a pure mathematician and appreciate mathematics as an *art form*, as well as the cornerstone of all science and technology.

Merriam-Webster defines art as follows:

> something that is created with imagination and skill and that is beautiful
> or that expresses important ideas or feelings

What could possibly fit this description more accurately than mathematics!?

Thus, while there will be plenty of *examples* to motivate the concepts, there will be few if any applications of the subject matter to other areas of mathematics or the sciences. I hope that my readers can appreciate the material *for its intrinsic beauty*, just as one might appreciate a Shakespeare play or a Beethoven symphony.

The Details

Now, as to the details of this book. There are several multi-volume series in abstract algebra, but as far as I am aware, they are all intended for the graduate student. I grew up with two such series, which were classics even in my early days—the three-volume series by Nathan Jacobson and the two-volume series by Bartel Leendert van der Waerden, both of which require considerable experience before undertaking and neither of which were an easy read by any means.

So why not a multi-volume series in abstract algebra for those who are have less experience but are nevertheless interested in undertaking a *serious course* in abstract algebra?

This is the first volume in the series. It is devoted to group theory. Subsequent volumes will be devoted to rings, fields, vector spaces and modules.

I come now to another point of apparent controversy. In my opinion, every student new to abstract algebra should be given a *short* dose of order theory (partially ordered sets, maximal and minimial elements, meets and joins) *at the beginning* and so Chapter 3 of this book is devoted to this subject. (Chapter 1 is a teaser and Chapter 2 is devoted to preliminaries.)

There will be many critics who say that this material is distracting and unmotivated. I can only say that the basic ideas of order theory are ubiquitious in abstract algebra and are essential to an understanding of many concepts throughout algebra. Also, since the approach of this book is abstract, I will assume that the readers of this book are able to appreciate the small amount of order theory as an art form as well. I will also say to those who are anxious to plunge immediately into group theory that a little patience will pay dividends later. Of course, those who are familiar with the basic concepts of partially ordered sets and lattices (not much beyond the definition) may feel free to skip Chapter 3 and refer to it later as needed.

I have kept the prerequisites for this book to a reasonable minimum, namely, a grasp of elementary linear algebra, as is usually taught in a first course on the subject. We will not have much need for linear algebra per se until later volumes, but the oft-mentioned *mathematical maturity* that such a course provides will be extremely helpful in making one's way through the present series.

I believe it is somewhat customary at this point to summarize the topic coverage of the volume for which this is the preface, but I will simply (and respectfully) ask you to examine the table of contents for such a summary.

Why?

For some readers, this book may be a first experience with a serious course in *abstract* mathematics, having perhaps had only calculus, discrete mathematics, elementary differential equations and the aforementioned elementary linear algebra prior to undertaking this course.

Accordingly, along with a first exposure to serious abstract mathematics comes a first exposure to serious abstract *thinking*. This raises the issue of how best to *think while reading*. If I were to give my readers only one single piece of advice, it would be to *constantly question*. If you are not saying to yourself “why is this statement true?” several times an hour, then you are probably not as involved with the subject matter as you should be.

To help with this, you will find the phrase "(why?)" liberally sprinkled throughout the text. This is a hint for you to pause a moment to make sure that you understand why the accompanying statement is true. On the other hand, recognizing that these insertions may become annoying, I have not included nearly as many I could have done. (This is a hint.)

If I were allowed the luxury of giving some additional advice to my readers, I would offer the following two pieces:

1) Practice, practice, practice. That is why the book has exercises. The more exercises you attempt, the more easily you will absorb the material. Along with trying the exercises, whenever you read the statement of a theorem, you should pause a few moments to see if you can construct a proof before reading my proof. Who knows, perhaps you can come up with a better proof than mine—It has been done before.
2) The most important practical thing you can do while reading is to

   immediately memorize all definitions as they appear in the text before reading on.

   After all, the definitions form the *vocabulary* of the subject, and who can learn any subject without memorizing its vocabulary?

   I know that memorization is not a fun thing to do, but after a while, it will become easier. To this end, I have in many cases avoided the common practice of introducing definitions at the start of a discussion, at which point they are essentially impossible to motivate. I find that a little motivation makes it much easier for me to remember a definition and I am sure that I am not alone in this. I believe that *generally speaking*, the best time for a definition is when it is *needed* and not before it is needed.

   This advice applies not only to formal definitions (using the heading "Definition") but also to all terms that appear in bold face within the text, since these are what you might call "in-line definitions" and are equally important.

Index of Symbols

There is an index of symbols at the back of the book, in case you encounter a symbol that you do not recognize. Also, we will use the following symbols often:

1) $\mathbb{N} = \{0, 1, \dots, \}$, the natural numbers, which *do* include 0,
2) $\mathbb{Z} =$ the integers,
3) $\mathbb{Z}^+ = \{1, 2, \dots \}$, the positive integers,
4) $\mathbb{Q} =$ the rational numbers,
5) $\mathbb{R} =$ the real numbers,
6) $\mathbb{C} =$ the complex numbers.

Greek Alphabet

It seems that mathematicians never have enough symbols. In particular, the usual Roman alphabet does not supply enough symbols to denote variables of different types. Accordingly, mathematicians find it necessary to reach out to other alphabet systems.

Some of the older classic abstract algebra textbooks (notably by Nathan Jacobson) that this author used as a student employ the **Fraktur** alphabet shown below.

𝔄𝔅ℭ𝔇𝔈𝔉𝔊ℌℑ𝔍𝔎𝔏𝔐𝔑𝔒𝔓𝔔ℜ𝔖𝔗𝔘𝔙𝔚𝔛𝔜ℨ
𝔞𝔟𝔠𝔡𝔢𝔣𝔤𝔥𝔦𝔧𝔨𝔩𝔪𝔫𝔬𝔭𝔮𝔯𝔰𝔱𝔲𝔳𝔴𝔵𝔶𝔷

However, as much as I enjoyed the added confusion that this alphabet provided while trying to learn algebra, I will not use it in this book. (For example, compare the upper case A ($\mathfrak{A}$) with the upper case U ($\mathfrak{U}$).)

It is fair to say that all mathematicians (and most mathematics books) make extensive use of the Greek alphabet, shown in the table below. If you intend to study mathematics seriously, knowledge of this alphabet is essential.

A α alpha	H η eta	N ν nu	T τ tau
B β beta	Θ θ theta	Ξ ξ xi	Υ υ upsilon
Γ γ gamma	I ι iota	O o omicron	Φ ϕ phi
Δ δ delta	K κ kappa	Π π pi	X χ chi
E ϵ epsilon	Λ λ lambda	P ρ rho	Ψ ψ psi
Z ζ zeta	M μ mu	Σ σ sigma	Ω ω omega

Good luck and thanks for reading.

Contents

Chapter 1: Introduction: The Big Picture, 1
What is Mathematics?, 1
What is Algebra?, 2
What Are Algebraic Properties Like?, 2
Common Themes Throughout Algebra, 5

Chapter 2: A Few Preliminaries, 11
Finite, Countable and Uncountable Sets, 11
Relatively Prime and Pairwise Relatively Prime Integers, 11
Congruence Modulo, 12
Words, 12
Cartesian Products, 13
Binary Relations, 15
Equivalence Relations and Partitions, 15
n-Ary Operations, 18

Chapter 3: Order, 23
Partially Ordered Sets, 23
Exercises, 34

Chapter 4: Groups, 41
The Definition, 41
Examples of Groups, 43
The Set Product, 50
Exponents and the Order of a Group Element, 51
The External Direct Product of Groups, 55
Symmetric Groups, 59
The Exponents of a Group, 62
Conjugation, 64
Homomorphisms of Groups, 68
Why Symmetric Groups Are the Most Important Groups, 70
Exercises, 72

Chapter 5: Defining a Group, Subgroups, Finitely-Generated Groups, 81
Defining a Group, 81

Group Templates, 83
Subgroups, 92
The Lattice sub, 95
Hasse Diagrams, 96
The Center of a Group, 97
Subgroup Generated by a Subset, 97
Three Similar Concepts, 99
Finitely-Generated Groups, 100
The Set Product of Subgroups, 105
Cosets and Lagrange's Theorem, 107
Euler's Formula, 110
Exercises, 110

Chapter 6: Special Families of Groups, 117
Cyclic Groups, 117
The Quaternion Group, 124
The Dihedral Groups, 126
The Additive Rationals, 129
Exercises, 133

Chapter 7: Cosets, Index and Normal Subgroups, 139
Cosets and Index, 139
Quotient Groups and Normal Subgroups, 140
The Normal Closure and the Normal Interior of a Subgroup, 145
The Set-Product Decomposition of a Group, 146
Monster Subgroups of a Finite Group, 154
Cauchy's Theorem, 155
Finite Abelian Groups, 161
The Center of a Group, 162
The Normalizer of a Subgroup, 164
Groups of Small Order, 166
Exercises, 168

Chapter 8: Homomorphisms and Cayley's Theorem, 175
Homomorphisms, 175
Kernels and the Natural Projection, 177
The Isomorphism Theorems, 178
The Correspondence Theorem, 180
Multiplication as a Permutation: Cayley's Theorem, 183
An Historical Perspective: Galois-Style Groups, 184
Exercises, 186

Chapter 9: Symmetric Groups, 195
The Definition and Cycle Representation, 195
Parity, 196
Generating Sets for S_n and A_n, 198
Subgroups of and, 199
The Simplicity of A_n, 199

Normal Subgroups of S_n, 202
Exercises, 203

Chapter 10: Group Actions, 209
Group Actions, 209
Translation by G on G/H, 215
Conjugation by G on the Conjugates of a Subgroup, 217
Conjugation by G on G, 218
Exercises, 219

Chapter 11: Sylow Theory, 227
Sylow Subgroups, 227
Normal Sylow Subgroups, 228
The Sylow Theorems, 228
The Search for Normal Subgroups; Simple Groups, 232
Groups of Order, 237
More Groups of Small Order, 243
Exercises, 246

References, 251
References on the Burnside Problem, 252

Index of Symbols, 255

Index, 261

Chapter 1
Introduction: The Big Picture

Perhaps the best place to start a discussion of any branch of mathematics is to first examine the "big picture" as it were. We begin with an overall view of mathematics in general.

What is Mathematics?

Mathematics can be thought of as the study of *sets with structure*. To illustrate, consider the following list, which suffers from some rather gross oversimplifications, but nonetheless makes the point.

- **Mathematical logic** is the study of sets with a deductive structure.
- **Combinatorics** is the study of (generally) *finite* sets, with a size structure.
- **Graph Theory** is the study of (generally) finite sets with a relationship structure.
- **Set theory** is the study of arbitrary sets with a size structure and possibly an order structure.
- **Number theory** is the study of the integers—a set with an incredibly rich order and arithmetic structure.
- **Order and lattice theory** is the study of sets with an order structure.
- **Point set topology** is the study of sets with a continuity structure.
- **Algebraic topology** is the study of sets with a continuity structure and a related algebraic structure.
- **Mathematical analysis** is the study of the sets $\mathbb{R}^n$ with a differentiability structure.
- **Differential geometry** is the study of general sets with a differentiability structure.
- **Probability** is the study of sets with a likelihood structure.
- **Measure theory** is the study of sets with a structure imposed by a general measure.
- **Euclidean, affine and projective geometry** is the study of sets with an axiom structure stemming from the notions of angle, parallelism and invariance under certain types of transformations.

Last but certainly not least, we come to the subject of this series

- **Abstract algebra** is the study of sets with an *algebraic* or *arithmetic* structure.

Of course, these areas of mathematics overlap considerably and the boundaries between areas are not at all well defined.

What is Algebra?

An algebraic structure is given to a set by defining one or more *algebraic operations* on the set. With the exception of the operation of scalar multiplication in modules and vector spaces, all of the algebraic operations that we will study are either nullary, unary or binary operations on the set. Let us define these terms.

1) A **nullary operation** on a nonempty set A is simply an element of A.
2) A **unary operation** on A is a function $u\colon A \to A$.
3) A **binary operation** on a nonempty set A is a function $f\colon A \times A \to A$ that takes an ordered pair (a, b) of elements of A and produces another element of A. there are two commonly used notations for binary operations. When **additive notation** is used, we write the image of (a, b) under the operation f as

$$a + b$$

in which case the operation is called **addition**. When **multiplicative notation** is used, we write $f(a, b)$ in any of the following ways

$$ab \quad \text{or} \quad a * b \quad \text{or} \quad a \cdot b$$

in which case the operation is called **multiplicaton**. The first of these multiplicative notations ab is the most common and is called **juxtaposition**.

When a set has two binary operations defined on it, we generally use addition for the stronger (the operation that has more properties) operation and multiplication for the weaker operation.

It might seem to you that defining a nullary operation on A as an element of the set A is more trouble than it is worth. Why not just simply say "an element of A?" Well, many mathematicians do, but there is a point in making this definition. Simply put, we want to be able to refer to the algebraic structure as the collection of all algebraic operations on the set, without needing to mention specific elements of the set. Put another way, the nullary and unary operations are just as important as the binary operations and so should have "equal status" as operations. While this discussion may not seem entirely clear at this point, we will clarify the discussion with a concrete example when we define groups, later in the book.

Algebraic operations can be very general. For example, for the set

$$X = \{a, b\}$$

we can define an operation called addition by setting

$$a + a = a, \quad a + b = a, \quad b + a = b, \quad b + b = b$$

Admittedly, this is not very useful, but it demonstrates the point that any nonempty set can

be given an algebraic structure. Obviously, abstract algebra is the study of *useful* algebraic structures.

For example, you undoubtedly know that functions on the real numbers can be added and multiplied. Thus, the set

$$\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is a function}\}$$

of all functions on $\mathbb{R}$ has two binary operations, called addition and multiplication, defined for $f, g \in \mathcal{F}$ by

$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

We can also take the negative of any function f, defined by

$$(-f)(x) = -(f(x))$$

The map $f \mapsto (-f)$ is a unary operation. The zero function $0(x) = 0$ and the identity function $f(x) = x$ are nullary operations worth singling out because of their nice properties. Of course, by definition, any element of $\mathcal{F}$ is a nullary operation, but the other elements don't have such nice algebraic properties.

Because of the properties of these binary, unary and nullary operations, which we will discuss at the appropriate time, this structure is an example of an algebraic structure known as a *ring*.

Abstract algebra can be divided into several different subareas, based on both the *number* of algebraic operations defined on the set and on the *properties* of these operations. Here is a partial list of the different types of algebraic structures that algebraists study. We will study the structures shown in bold in some detail.

- Semigroup (1 binary)
- Monoid (1 binary, 1 nullary)
- **Group** (1 binary, 1 unary, 1 nullary)
- **Ring** (2 binary, 1 unary, 1 or 2 nullary)
- **Integral Domain** (special types of ring)
- **Field** (2 binary, 1 unary, 2 nullary and one unary *partial* operation)
- **Module** (1 binary, 1 unary, 1 nullary and one non-operation called scalar multiplication)
- **Vector Space** (1 binary, 1 unary, 1 nullary and one non-operation called scalar multiplication)
- **Lattice** (2 binary)
- **Boolean Algebra** (2 binary, 1 unary, 2 nullary)

As you no doubt know, in the case of vector spaces (and modules), one of the operations, called *scalar multiplication* is not a true operation. For example, if V is a vector space over the real numbners $\mathbb{R}$, then scalar multiplication is a function

$$f: \mathbb{R} \times V \to V$$

which is not a binary operation. We will discuss this further at the appropriate time.

What Are Algebraic Properties Like?

Algebraic operations in themselves are of little value unless we require that they satisfy some *properties*. To get a feel for the types of properties that we will study throughout this lecture series, here is a list of the properties of addition and multiplication for the real numbers $\mathbb{R}$.

1) (**Associativity**) For all $a, b, c \in \mathbb{R}$,

$$(a+b)+c = a+(b+c) \quad \text{and} \quad (ab)c = a(bc)$$

2) (**Commutivity**) For all $a, b \in \mathbb{R}$,

$$a+b = b+a \quad \text{and} \quad ab = ba$$

3) (**Distributivity**) For all $a, b, c \in \mathbb{R}$,

$$(a+b)c = ac+bc \quad \text{and} \quad a(b+c) = ab+ac$$

4) (**Nullary Operations–Identity Elements**) There exists an element $0 \in \mathbb{R}$, called the **additive identity** or **zero element** of $\mathbb{R}$ for which

$$0+a = a+0 = a$$

for all $a \in \mathbb{R}$. Also, there exists an element $1 \in \mathbb{R}$, called the **multiplicative identity** (or sometimes just the **identity**) for which

$$1a = a1 = a$$

for all $a \in \mathbb{R}$.

5) (**One Unary Operation and One Partial Unary Operation–Inverses**) For each $a \in \mathbb{R}$, there is an element called the **additive inverse** or **negative** of a and denoted by $-a$, for which

$$a+(-a) = (-a)+a = 0$$

For each *nonzero* element $a \in \mathbb{R}$, there is an element called the **multiplicative inverse** of a and denoted by a^{-1}, for which

$$aa^{-1} = a^{-1}a = 1$$

Because the set $\mathbb{R}$ together with the operations of addition and multiplication satisfies the properties listed above, it is an example of a *field*.

You might be wondering why we bother to study algebraic structures in the rather abstract setting of an arbitrary set *whose elements are unspecified* with a collection of algebraic operations having certain properties. Why do we not simply study the "important" algebraic

structures, such as the ones that come from numbers, functions, matrices, polynomials and so on?

The reason is actually quite simple. Every time we prove some fact about an *arbitrary* group for example, that fact applies at once to *all* groups. Therefore, we don't need to prove a version of that result for each important group separately. This is *husbandry* at its finest. Also, it tells us that the fact we proved does not depend on any specific properties of the *elements* of a group, such as numbers, functions or matrices, but rather it depends *only* on the defining properties of the group structure. This is a very useful piece of information.

Common Themes Throughout Algebra

Once you have studied various types of algebraic structures, such as groups, rings, fields and vector spaces, you will notice that there are a lot of *common themes* running throughout each subject. Rather than realize this after studying these algebraic structures, it makes more sense to realize this before studying these algebraic structures, to whatever extent this is possible. So let us take a general look at these themes now. Note that they may not occur in precisely the same order as we describe them here. Authors generally have some discretion in this matter.

Let us imagine an unspecified type of algebraic structure, called a **widget**. Thus, widgets could be groups, or they could be rings, or they could be fields or they could be vector spaces and so on.

The Definition of a Widget

When you study widgets, the first thing you will encounter is, of course, the definition of a widget. This will be followed by a few of the basic consequences of the definition. For example, one common consequence is the *uniqueness* of certain objects described in the definition. For instance, the definition of most widgets includes the existence of a special *identity element* (which is a nullary operation) for each binary operation. It is a consequence of the properties in the definition that identity elements are unique, so you are likely to encounter a small theorem to this effect soon after the definition.

Note that because uniqueness of the identity element can be *proved* from the definition of widget, the statement of uniqueness should not be (and never is) included as part of the *definition*. Definitions are supposed to be as lean as possible, that is, they are generally intended to contain exactly what is required *and no more*.

Subwidgets

The next theme you may encounter is the concept of a subwidget (sub*group*, sub*ring*, sub*field*, sub*space* and so on). The idea is simple: If W is a widget and S is a nonempty subset of W, it is natural to wonder whether the algebraic operations defined on W can be *restricted* to the subset S, making it into a widget as well. If so, then S is called a **subwidget** of W. Note that S may be a widget under *other* operations as well, but that does not make it a *subwidget* of W.

Making New Widgets from Old Widgets

One of the next themes you are likely to encounter is that of making new widgets from old widgets.

The Product of Widgets

One way is to do this that applies to many (but not all) algebraic structures is to use the cartesian product, since widgets are sets. If W_1 and W_2 are widgets, then the cartesian product $W_1 \times W_2$ is the set of ordered pairs of widget elements

$$W_1 \times W_2 = \{(s,t) \mid s \in W_1, t \in W_2\}$$

So if $*$ denotes a binary widget operation, then we can try to define the product of ordered pairs *componentwise*, that is, we can set

$$(s,t) * (u,v) = (s * u, t * v)$$

This product construction works for groups, rings and vector spaces, for example, but it does not work for fields.

Exponential Widgets

Another way to make new widgets from old widgets is to take *exponentials* (although not all mathematicians use this terminology). If W is a widget and X is a nonempty set, then the set of all set *functions* from X to W, denoted by W^X is often a widget. The key is that a widget operation on W can be performed on the *images* of the elements under the functions in W^X, which lie in W.

As a simple example, if $W = \mathbb{Z}$, the integers, then we can define the sum and product of functions in $\mathbb{Z}^X$ by

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

for all $x \in X$. Now, as we will see, the integers $\mathbb{Z}$ form a ring under the operations of ordinary addition and multiplication and so does the set $\mathbb{Z}^X$ under the operations defined above.

We should note that sometimes W^X is not quite a widget, but it is another "weaker" algebraic structure. For example, the real numbers $\mathbb{R}$ form a field under the operations of ordinary addition and multiplication, but the set $\mathbb{R}^X$ does not quite make it to a field—it is merely a ring, which is a weaker algebraic stucture.

Quotient Widgets

Another way to make new widgets from old widgets is to take quotients. *Quotient widgets* can cause quite some confusion when they are first encountered. Let us see if we can explain the general idea behind quotient widgets. Suppose that W is a widget. Of course, W is also a set. Now, we are interested in *partitioning* the set W into nonempty, nonoverlapping blocks

$$\mathcal{P} = \{B_1, B_2, B_3, \dots\}$$

as shown in Figure 1, in such a way that we can "lift" the widget operation(s) from the *elements* of W to the *blocks* of the partition $\mathcal{P}$.

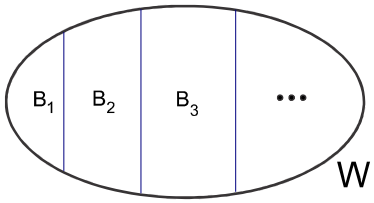

Figure 1

Let us assume that widgets have only one operation, which we will call the product (denoted by juxtaposition). There is one obvious way to try to perform this lifting process. Namely, we define the product B_iB_j of two *blocks* by taking one element from each block, say

$$a_i \in B_i \quad \text{and} \quad a_j \in B_j$$

taking their widget product a_ia_j and then finding the block that contains this product, say it is B_k. Then we *define* the product of these two blocks by

$$B_iB_j = B_k$$

Now we can ask whether this product of blocks satisfies the widget properties and so makes the set $\mathcal{P}$ of blocks into a widget as well.

However, there is a potential problem here. The way we defined the product of blocks is ambiguous. Do you see why?

Suppose someone else picks *different* elements from the blocks B_i and B_j, say $a_i' \in B_i$ and $a_j' \in B_j$. Then there is no guarantee that the product $a_i'a_j'$ and a_ia_j are in the same block of $\mathcal{P}$. If these two products are in different blocks, then this attempt at defining the product of blocks fails completely. Put more formally, the product is not **well defined**.

If we can resolve this potential issue, then the set $\mathcal{P}$ becomes a widget under this "lifted" operation and is called a **quotient widget** of W. Thus, we have quotient groups, quotient rings and quotient spaces. Quotient fields do not exist for reasons similar to those that cause the product construction to fail in the case of fields.

Functions Between Widgets

Another common theme in the study of algebraic structures is that of a *structure-preserving function* between widgets. If $h\colon W \to V$ is a function from the widget W to the widget V, then h is structure preserving if

1) For any binary widget operation (denoted by juxtaposition), we have

$$h(w_1 w_2) = h(w_1)h(w_2)$$

For example, for addition of real numbers, we require that

$$h(a + b) = h(a) + h(b)$$

2) For any unary operation $w \mapsto u(w)$, we have

$$h(u(w)) = u(h(w))$$

For example, for the unary operation of taking the negative of a real number, we require that

$$h(-w) = -h(w)$$

3) A nullary operation identifies a specific element in a widget. if that element is denoted by 1, then preservation of this nullary operation is

$$h(1_W) = 1_V$$

where 1_W is the specified element in W and 1_V is the specified element in V.

Many mathematicians would say that the concept of a structure-preserving function between widgets is almost as important as the concept of a widget itself. It is hard to appreciate why this might be true at this stage in the game, but suffice it to say that there is an entire branch of mathematics that attempts to make just this point! It is called **category theory**.

The structure-preserving functions between widgets are called **morphisms**. There are group morphisms, ring morphisms, field morphisms, vector space morphisms and so on. Each of these has a more specific terminology. For instance, group and ring morphisms are called **homomorphisms**. Field morphisms are called **embeddings** and vector space and module morphisms are called **linear transformations**.

Representations of the Elements of One Widget By the Elements of Another Widget

There is one final and *extremely important* common theme used throughout mathematics: that is the technique of *representation*. Specifically, often a great deal can be learned by representing one type of mathematical object as another type of mathematical object.

For example, a real number $r \in \mathbb{R}$ can also be thought of as (or represented as) a *function*, namely, multiplication by r, which we write as μ_r. Thus, μ_r is defined by

$$\mu_r \colon \mathbb{R} \to \mathbb{R}, \quad \mu_r(x) = rx$$

The function μ_r is *bijective* (one-to-one and onto) and is referred to in some contexts as **left translation** by r. Note that if we know μ_r, then we also know r, since

$$r = \mu_r(1)$$

As another example, in elementary linear algebra, we think of matrices such as

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

not just as rectangular arrays of numbers that can be added and multiplied together, but also as *linear transformation* (multiplication by M) from $\mathbb{R}^2$ to $\mathbb{R}^2$,

$$M\colon \mathbb{R}^2 \to \mathbb{R}^2, \quad M\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a + 2b \\ 3a + 4b \end{pmatrix}$$

In general, a representation of the elements in a widget A by the elements in another widget B is generally defined by a *function*

$$\lambda\colon A \to B$$

called the **representation map** for the representation. Thus, $a \in A$ is represented by the element $\lambda(a)$ in B.

Now, if the representation map is not injective (one-to-one), then there will be distinct elements a_1 and a_2 in A that are represented by the same element

$$b = \lambda(a_1) = \lambda(a_2)$$

in B. You might first think that this would ruin the representation, but there are in fact many important representations that are not injective, as we will see. When the representation map is injective, the representation is said to be **faithful**.

Representing one type of mathematical object by another type of mathematical object is an extremely important technique that we will employ to great advantage in this book.