

Section 1.7. This section gives an algebraic view of the complex numbers. When you are interested in *solving equations*, the real numbers seem inadequate because they allow you to write the very simple equation

$$x^2 = -1 \quad (I)$$

that has no solution in real numbers. (The proof that it has no solution follows from the fundamental property that, for all real numbers x we have $x^2 \geq 0$.) The algebraic approach to this difficulty is to *imagine* that somewhere there is a quantity, usually called i , that satisfies (I), and to ask what else we need to have to have a system containing the real numbers and i that obeys reasonable rules of algebra (which will become the axioms defining a field later in the book). At the very least, we want operations of addition and multiplication, which forces us to have $a + bi$ for all pairs of real numbers (a, b) . We also declare that the only way to have $a + bi = c + di$ is $a = c$ and $b = d$. If addition is to be commutative and associative, and if multiplication by i is to distribute over addition, there is only one way to define addition. If we want a general definition of multiplication that obeys the

distributive law, then

$$(a + bi)(c + di) = ac + a(di) + (bi)c + (bi)(di)$$

If we also require commutative and associative laws of multiplication, the products in these terms can be rearranged to have all factors of i at the right. Finally, the factor of i^2 in the last term should be replaced by (-1) since we want i to *always* be a solution of equation (I). This leads an expression of the product of two complex numbers as a complex number. However, something important is missing: we do not yet know whether the number system we imagined exists.

Here is where abstraction comes to the rescue. The idea is to take a set we can construct and define operations on that set. We can then investigate whether these defined operations have certain properties. To make things truly abstract, we can define our operation on the set of ordered pairs of real numbers $\mathbb{R} \times \mathbb{R}$. The pair $(0, 0)$ is seen to be the identity element for addition and $(1, 0)$ is seen to be the identity element for multiplication. Proofs of the algebraic properties of these operations follow by expressing each desired

identity as an equation in the real numbers that are the components of the quantities in the identity. Each such equation can be shown to be an identity by the algebraic properties of addition and multiplication of real numbers.

For real numbers, we know that we have an operation of division. That is, if a and b are given real numbers, and $a \neq 0$, we can solve $ax = b$. It would be nice to know if we can do this for complex number, and if so, *how* to do it. Let's formulate the statement that we want to prove.

Given complex numbers (a, b) and (c, d) with

$$(a, b) \neq (0, 0),$$

there is a solution to the equation

$$(a, b)(x, y) = (c, d).$$

Here, $(a, b) \neq (0, 0)$ means that it is not true that both $a = 0$ and $b = 0$, i.e., $a \neq 0$ or $b \neq 0$. The product $(a, b)(x, y)$ is determined using our abstract definition of multiplication. Thus, division is interpreted as

solving

$$ax - by = c$$

$$bx + ay = d$$

and we know from linear algebra that this system of equations has a unique solution if $a^2 + b^2 \neq 0$. Since $x^2 > 0$ is $x \neq 0$ — the same property of real numbers that got us into this construction — this holds for all $(a, b) \neq (0, 0)$, as required. Indeed a solution can be given using only operations we know and division by this real number. In particular, the solution of

$$(a, b)(x, y) = (a^2 + b^2, 0)$$

is $(x, y) = (a, -b)$. This quantity, called the (complex) conjugate of (a, b) appears in many operations with complex numbers.

Abstract constructions like this mean that finding the roots of a polynomial is no *no big deal*. It is easy to modify this to enlarge any system of numbers to include a root of any polynomial, so the following (annoyingly difficult to prove rigorously) result, which

is called the “fundamental theorem of algebra”, plays no essential role in this course: Any polynomial with coefficients in the complex numbers has a root in the complex numbers.

The section ends with a concrete example of this “fundamental theorem”: a factorization of $z^n - 1$ into linear factors over the complex numbers.

Section 2.1 The systematic study of abstract algebra begins with our first structure, the **group**, which is an abstraction of the properties of $A(S)$ from Section 1.4. Groups are defined by saying that we have a set with one operation satisfying four properties: (1) closure, (2) associativity, (3) identity, (4) inverses. These are repeated often enough in the textbook, that I don’t need to write them here.

I feel (and I also feel that I have a lot of company in this) that closure is part of the definition of the operation and not property that needs to be tested after the operation has been defined. Older mathematics often treated formulas defining operations (or functions) as meaningful wherever they could be interpreted. When the interpretation is particularly far-fetched, it

is called “abuse of notation”. While this *abuse* is usually harmless and sometimes aids in the discovery or exposition of new results, it should not be part of the ideal proofs that our mathematical arguments aim to describe. In the ideal universe of contemporary mathematics, the domain and *codomain* of every mapping is part of the definition of the mapping. That is, the symbol describing a mapping should say not only what the mapping does, but where it is allowed to be applied and what kind of result is expected. In particular, although there is no difficulty restricting a domain or enlarging a codomain, these should be considered as composition with an inclusion mapping.

From this point of view, one should not be allowed to say that you have an operation on a set S until closure has been verified. The underlying set and the operation remain fixed while testing the remaining properties.

You may feel that it is a burden to require mappings to be defined so precisely, but it saves in other ways. For example, example 6 looks at the set of linear functions

$T_{a,b}$ for $a, b \in \mathbb{R}$ and $a \neq 0$, defined by

$$T_{a,b}(x) = ax + b.$$

An operation is defined by showing that the composition $T_{a,b} \circ T_{c,d}$ is an function of the same type. Throughout the discussion of this example, element of the group are denoted with a full size T that only serves to identify which example this is, while the numbers a and b that do all the work are subscripts written in a much smaller font. This is unfair! We should begin by stating clearly what group we are talking about, and choosing a notation that is an efficient description of the elements and operation in that group.

Purging useless symbols allows us to see much more quickly when two construction lead to the same group. If abstraction is our goal, this is a benefit. We should not need to carry a history of where our examples came from when they are used to illustrate abstract theorems, although interpreting the final result in the original model may be useful.

This use of subscripts should be thought of as a temporary device for using a familiar set S to label special

elements of a set of mappings $A(X)$ in order to define an operation on S that models composition in $A(X)$. This is particularly useful is X is infinite. Example 12 illustrates this with T_θ being rotation about the origin in \mathbb{R}^2 by an angle θ . Since $T_{2\pi} = T_0$, this informal description is hiding something that will need to be need to be made precise at some point. Since the subject demands that certain equations be verified, it is important to know when two elements are the same. In the case of the complex numbers ,this could be done by starting with unique names for all elements in the set. Until we decide what to do with rotations, this subscript notation is useful.

Since the assigned exercises refer to exercise 10, that should be discussed in class.

Section 2.2. This is devoted to simple properties of the identity and inverses. It is shown that the properties defining these quantities actually characterize *unique* elements whose *existence* is asserted in the axioms of a group. Since our systems are only rarely commutative, it is useful to note that the inverse of a product is always the product of the inverse *in the*

reverse order.

Instead of requiring two-sided inverses in a single statement, we could have independently required left and right inverses. This is no more general, the associative law shows that if $xa = i$ and $ay = i$, then $x = y$.