Chapter 1
Complex Numbers

The Number Story

To express basic numerical facts of life (like "I have two horses", "he has four dogs") natural numbers are enough and people living in "primitive" societies were content with these. In time, the need to share necessitated introduction to the language words like *a half* and *a quarter*, that heralded the era of fractions. I have taught, over the years, students of different nationalities and they all confirm the presence of equivalents of *a half* and *a quarter* in their native languages. On the other hand, I have yet to come across a language containing a single word meaning *negative one*. It proves to me that positive rational numbers were used long before people realized the existence and usefulness of negative numbers. I believe, the concept of negative numbers appeared fairly late in history, with the development of trade and the idea of *credit* and *debt*. I don't know whether the ancient Greeks were using negative numbers, but they certainly knew about *irrational* numbers. They were the first to realize that square root of 2 cannot be expressed as a quotient of two integers. The climax of the ancient theory (and practice) of numbers was the invention of *zero*. Zero was invented several times, independently, in different parts of the world, and eventually was imported to Europe from India, by Arab merchants in the Middle Ages.

From today's point of view, we can look at the history of numbers as the constant effort to create more "complete" system in the sense that more and more types of equations become solvable. If we want all equations of the form x+a=b, where a and b are natural numbers to be solvable we must admit the existence of negative integers and of zero. To solve equations of the form ax+b=c, where a,b and c are integers we need the concept of fractions and, consequently of rational numbers. Notice that, once we admit rational numbers as solutions of our equations, we can also admit rational coefficients, without having to extend the set of potential solutions, i.e. all equations of the form ax+b=c with rational coefficients (and $a\neq 0$) have rational solutions. When it came to solving polynomial equations of higher degrees situation became more complicated. Even the construction of the set of real numbers was not enough to ensure solvability of all polynomial equations. We can easily construct a nonsolvable polynomial equation with integer coefficients and the degree as small as 2, for example $x^2+1=0$. It turned out that the solution is fairly simple. It is enough to admit the existence of just one more symbol, the *imaginary unit* i, with the property $i^2=-1$, and all polynomial equations become solvable. Of course, admitting the number i, we must also admit all the consequences i.e. all multiplicities of i and sums of real numbers and multiplicities of i.

Algebraic systems

Definition 1.1. A binary operation on a set X is function $f:X\times X\to X$. The word *binary* refers to the number of arguments of f.

Definition 1.2. An algebraic system or simply an algebra is a finite sequence $(X,f_1,f_2,\dots,f_n)$ where X is a set and $f_1,f_2, \dots, f_n$ are (binary) operations on X.

Traditionally, we use symbols like +,*,-,\ to denote operations and we place them between the arguments writing a+b rather than +(a,b). For any two arguments x and y, f(x,y) is called "the result of f on x and y".

The definition of an *operation* says that the result of the operation f for every two arguments x and y from a set X belongs to X We say then that X is closed with respect to the operation f or closed under f. For example **R** is closed under addition, subtraction and multiplication, which simply means that the sum, the difference and the product of any two real numbers is a real number. The set **N** of natural numbers is not closed under subtraction and is not closed under division.

Sometimes it may be necessary to consider operations of other "arities" – unary (one argument) operations, and in general n-ary (n-argument) operations.

An algebraic operation need not be anything as conventional as addition or multiplication. In fact it may be absolutely any function, even apparently wild and meaningless, as long as it assigns elements of X to pairs of elements of X.

Example 1.1. Consider the operation * defined on a set X as $(\forall x,y\in X)\ x*y=x$. The definition means that * assigns to every pair (x,y) the first element of the pair. It may not be very exciting but it is a perfectly legal algebraic operation.

Example 1.2. Another silly but formally correct example is a constant function & that assigns the same element of **Z**, for example 7, to every pair (x,y) from **Z**×**Z**, i.e. $(\forall x,y\in \mathbf{Z})\ x\&y=7$.

Example 1.3. The following definition "*whenever I am given a pair (x,y) I toss a coin and chose x if it is heads, or y otherwise*" is illegal because it may happen that presented for the second time with the same pair (x,y) you will chose differently, so your procedure does not define a function.

Example 1.4. Subtraction. It is an operation on the set of integers **Z**, but is not an operation on the set of natural numbers **N** because in the case of X=**N** the result of subtraction does not belong to X for some pairs of natural numbers (1–2=–1).

And now let us do something really wild.

Example 1.5. Arithmetic modulo *n*. First recall that *k* mod *n* denotes the remainder of the division of *k* by *n*. Let *n* be a positive natural number. Consider the set $\mathbf{Z}_n=\{0,1, \dots n-1\}$. For any two numbers a and b from $\mathbf{Z}_n$ we define their *sum modulo n* as $a\oplus_n b=(a+b)\bmod n$. Correspondingly, we define the *product modulo n* as $a\otimes_n b=(ab)\bmod n$. By the definition of the remainder of the division by *n*, both $a\oplus_n b$ and $a\otimes_n b$ are elements of $\mathbf{Z}_n$. Symbols $\oplus_n$ and $\otimes_n$ are a nuisance so whenever there is no risk of ambiguity we shall simply write ⊕ or ⊗. We must only remember that in $(\mathbf{Z}_7,\oplus)$ ⊕ denotes addition mod 7 and in $(\mathbf{Z}_5,\oplus)$ – mod 5. In these finite algebras we have all sorts of funny identities. Things like “*two plus two is zero”* or “*three times three is one*” are commonplace, as long as you do your arithmetic “mod 4”.

Example 1.6. Let ZOO={a cow, a dog, a frog}. We define an operation + on the set ZOO by means of the *operation table*

+	cow	dog	frog
cow	cow	dog	frog
dog	dog	frog	cow
frog	frog	cow	dog

This is another way of saying cow+cow=cow, cow+dog=dog, cow+frog=frog, dog+cow=dog and so on. Those poor darlings who ask now “But what does it **mean** that *a dog times a frog is a dog?*” are kindly requested to read this chapter again from the beginning, because it “means” nothing (and that’s the whole fun). On the other hand, some readers may notice, that our + operation is closely related to the operation ⊕ from Example 1.1, namely this is what we get if we put *n*=3 and identify 0 with the cow, 1 with the dog and 2 with the frog.

Example 1.7. Let $X=Y^Y$, i.e. X is the set of all functions mapping Y into Y. We will denote by ∘ the operation of composition of functions. The result of this operation is a new function $f\circ g$ from Y into Y, whose value on every $y\in Y$ is defined as $(f\circ g)(y)=f(g(y))$.

Example 1.8. Symmetric difference. For any set X, 2^X denotes the set of all subsets of X. In addition to the well-known set operations of union, intersection and set difference we will consider the operation of the *symmetric difference* defined as $A \div B = A \setminus B \cup B \setminus A$. Obviously, if A and B belong to 2^X then so do $A \setminus B$ and $B \setminus A$ and so does their union.

Fields

Definition 1.3. An algebra (G,*) is called a group iff

(a) $(\forall a,b,c \in G) a*(b*c) = (a*b)*c$ (* is associative)

(b) $(\exists e \in G)(\forall x \in G)\ e*x=x*e=x$ (G has the identity element *e*)

(c) $(\forall a \in G)(\exists b \in G) a*b=b*a=e$ (every element of G is invertible)

A group is called abelian (or commutative) if

(d) $(\forall a,b \in G) a*b=b*a$ (* is commutative)

Example 1.9. $(2^X,\div)$, $(\mathbf{Z}_n,\oplus)$, $(\mathbf{R},+)$, $(\mathbf{Z},+)$, $(\mathbf{R}^+,\cdot)$ are abelian groups. The dot in the last example denotes ordinary multiplication.

Example 1.10. $(\mathbf{R},\cdot)$ is not a group because 0 is not invertible under multiplication.

Definition 1.4. An algebra (**F**,#,*) is called a field iff

(a) (**F**,#) is an abelian group with the identity element e_0

(b) * is associative

(c) * is commutative

(c) * has an identity element e_1

(d) for every element x of **F**, such that $x \neq e_0$, there exists y in **F** such that $x*y=y*x=e_1$

(e) for every $x,y,z \in \mathbf{F}$ $x*(y\#z)=(x*y)\#(x*z)$

(f) **F** has at least 2 elements

It is easy to see that conditions (b)-(d) state that $(\mathbf{F}-\{e_0\},*)$ is a commutative group.

Fields are modeled on the set of real numbers with addition as the first operation (#) and multiplication as the second (*). Condition (e) is known as *the distributivity law*, we say that * is distributive with respect to #. In $(\mathbf{R},+,\cdot)$ multiplication is distributive with respect to addition but not the other way around, hence $(\mathbf{R},\cdot,+)$ is not a field.

Example 1.11. For every prime number p $(\mathbf{Z}_p,\oplus,\otimes)$ is a field.

Example 1.12. $(\mathbf{Q}(\sqrt{p}),+,\cdot)$ is a field for every integer p.

Example 1.13. ($R\times R,+,\cdot$) where + and $\cdot$ are defined "componentwise", i.e. (a,b)+(c,d) = (a+c, b+d) and (a,b) $\cdot$ (c,d) = (a$\cdot$c, b$\cdot$d) is NOT a field,since no element of the form (0,b) or (a,0) is invertible.

Example 1.14. ($R\times R,+,\cdot$) with componentwise addition and multiplication defined as follows: (a,b)$\cdot$(c,d) = (ac-bd,ad+bc) is a field.

Definition 1.5. The set of complex numbers is the set **C** of all expressions of the form a+bi, where a and b are real numbers and i is an object (not a real number) satisfying the condition $i^2=-1$. Symbolically, $\mathbf{C}=\{a+bi \mid a,b\in \mathbf{R} \wedge i^2=-1\}$. For a complex number z=a+bi, the two real numbers a and b are referred to as the *real part, Re*z, and the *imaginary part, Im*z, of z, respectively. We write then a=Rez, b=Imz.

There is no point in pondering the question "But what this *i* thing really is?". There is no more sense in this question than in "What the square root of 2 really looks like?". The concept of an irrational number was just as hard to grasp to our ancestors, accustomed to integers and ordinary fractions, as the concept of an imaginary number is to us. Our worry should rather be "Can we build a consistent theory of numbers (an algebraic system) that includes all real number and the imaginary unit i?". By "consistent theory" we mean a system that preserves all the basic properties of arithmetic operations on real numbers, such as commutativity of addition and multiplication, associativity and the like. The answer depends of course on how are we going to define addition and multiplication. Let us define those operations in the most natural way, as if "i" was the variable x in a binomial a+bx, only, whenever we come across i^2 we replace it with –1. Hence

$$(a+bi)+(c+di) = (a+c)+(b+d)i$$

$$(a+bi)(c+di) = ac+adi+bic+bdi^2 = (ac-bd)+(ad+bc)i$$

It can be easily verified that both operations are commutative and associative. Let us verify associativity of multiplication:

$$[(a+bi)(c+di)](e+fi) = [(ac-bd)+(ad+bc)i](e+fi) = (ace-bde-adf-bcf)+(acf-bdf+ade+bce)i$$

while

$$(a+bi)[(c+di)(e+fi)] = (a+bi)[(ce-df)+(cf+de)i] = (ace-adf-bcf-bde)+(acf+ade+bce-bdf)i$$

so the expressions are identical. Distributivity of multiplication with respect to addition can be verified in the same way. It is worth noting that every real number is also a complex number (whose imaginary part is equal to 0), hence the identity elements of addition and multiplication of real numbers (0 and 1) are members of **C**, and play the roles of identity elements here as well. The complex number (-a)+(-b)i is obviously the inverse of a+bi with respect to addition, while $\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i$ is the inverse of a+bi with respect to multiplication (if a+bi≠0). Hence the operations on complex numbers have all the basic properties of regular addition and multiplication, i.e. (**C**,+,·) is a field.