Chapter 6. Number Theory

Note. The topic of number theory is a central part of mathematics! It is a pity that it is not a formal part of the ETSU (undergraduate or graduate) curriculum! Your only opportunities for an introduction to this area is in this class (Mathematical Reasoning, MATH 3000) and maybe in History of Mathematics (MATH 3040). The ETSU undergraduate catalog includes the class Elementary Number Theory (MATH 3120) with class description: "Introduces number theory, treating divisibility, congruencies, linear Diophantine equations, and quadratic residues. Some history of the development of the discipline also is included." We will not consider Diophantine equations nor quadratic residues in these notes, nor will will give much history. However, I have online notes for Elementary Number Theory which include the topics in the catalog description (and more), along with a moderate amount of history. Unfortunately, the Elementary Number Theory (MATH 3120) class has not been formally offered in my memory (my unreliable memory extends back to the beginning of the new millennium on this; the class may have been offered by one of my colleagues as an Independent Study in this time frame, but not that I recall). This might be an appropriate time to lament the total absence of a set theory class at ETSU, as well...

Note. Gerstein states (see page 278): "...in recent years [number theory] has been applied to problems associated with the transmission and encryption of numerical data. (Pure mathematics has become applied mathematics!) Number theory is unique in its abundance of appealing problems whose statements are accessible to elementary school students, but whose solutions have eluded mathematicians for centuries."

6.1. Operations

Note. In this section, we define a binary operation and some of its properties. We define the algebraic structures of group, ring, and field.

Definition 6.1. Let S be a nonempty set. A *binary operation* on S is a function $* : S \times S \to S$. A set on which one or more operations have been defined is an *algebraic structure*, *algebraic system*, or *binary algebraic structure*. We denote the image of $(a, b) \in S \times S$ under $*$ as $a * b$.

Definition 6.2. Let $*$ be an operation on S. Then

(i) $*$ is *commutative* if $a * b = b * a$ for every $a, b \in S$,

(ii) $*$ is *associative* if $(a * b) * c = a * (b * c)$ for every $a, b, c \in S$, and

(iii) An element $e \in S$ is an *identity element* of $*$ if for all $a \in S$ we have both $e * a = a$ and $a * e = a$.

Example 6.3. (a) Three binary operations on $\mathbb{R}$ are ordinary addition, subtraction, and multiplication: $(a, b) \overset{+}{\mapsto} a + b$, $(a, b) \overset{-}{\mapsto} a - b$, $(a, b) \overset{\cdot}{\mapsto} a \cdot b$. Notice that addition and multiplication are commutative, but subtraction is not. The additive identity is 0 and the multiplicative identity is 1; there is no subtractive identity. Notice that division is not a binary operation on $\mathbb{R}$, since division by 0 is undefined. We will define a "ring" below, and $\mathbb{R}$ along with addition and multiplication are an example of a ring (as are the $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{C}$). It is true that subtraction is a binary operation on these sets of numbers, but there is no such thing as subtraction (or division) when we consider the algebraic properties of these rings; there is only addition (though we can consider the addition of an additive inverse so that we have $a + (-b)$) and multiplication (though we can consider multiplication by a multiplicative inverse [other than the multiplicative inverse of 0] so we have ab^{-1}).

(b) If A is any set, then union and intersection are binary operations that are commutative and associative on the power set $P(A)$. The empty set is an identity for $\cup$ and A is an identity for $\cap$. (We'll see below that identities are unique.)

(c) Let Σ be a finite alphabet with the set of words Σ^* (see Section 4.5. Languages and Finite Automata). The concatenation of two words is the word obtained by following one word be the other. Concatenation is a binary operation on Σ^*. It is associative but not commutative, and the identity is the empty word ε.

(f) Let A be a nonempty set, and let $F(A)$ denote the set of all function from A to A. Then compositions of functions is a binary operation on $F(A)$. It is associative but not commutative and the identity map i_A is the identity.

Note. If set A is small of size n and $*$ is a binary operation (or simply an "operation," as Gerstein uses the term) then we can make a $n \times n$ "multiplication table" where we augment the matrix with a first column of the elements of A and augment is with a first row of the elements of A, as given below. We then put $a_i * a_j$ in the

(i, j) entry of the original matrix:

$$\begin{array}{c|ccc} * & a_1 & a_2 & a_3 \\ a_1 & a_3 & a_1 & a_2 \\ a_2 & a_2 & a_3 & a_1 \\ a_3 & a_1 & a_2 & a_1 \end{array}$$

Notice that the operation is not commutative (since the matrix is not symmetric) and there is no identity. When you are introduced to groups in Introduction to Modern Algebra (MATH 4127/5127), some small groups will be presented in this way.

Theorem 6.4. An operation has at most one identity.

Definition 6.5. Suppose the operation $*$ on S has identity element e, and let $a \in S$. If there is an element $b \in S$ satisfying $a * b = b * a = e$, then b is an *inverse* of a with respect to $*$.

Theorem 6.6. Suppose $*$ is an associative operation on S with identity e. If an element $a \in S$ has an inverse, then it has only one inverse.

Note. In Example 6.3(a), we see that the inverse of $a \in \mathbb{R}$ under addition is $-a$. The inverse of each nonzero $a \in \mathbb{R}$ under multiplication is $a^{-1} = 1/a$, and 0 has no multiplicative inverse. In Example 6.3(b), $\varnothing$ is the identity on $P(A)$ under $\cup$, but no nonempty set in $P(A)$ has an inverse. In Example 6.3(c), the empty word ε is the identity on Σ^* under concatenation, but no nonempty word has an inverse.

Definition. A nonempty set S with an associative operation $*$ is a *semigroup*. A semigroup with an identity element and such that every element has an inverse is a *group*. A *ring* is a nonempty set R on which two associative operations, usually denoted $+$ and $\cdot$, where R under $+$ is a group, $+$ is commutative, and $\cdot$ distributes over $+$. If $\cdot$ in a ring is commutative then R is a *commutative ring*. A commutative ring with a multiplicative identity and such that every non-additive-identity (i.e., nonzero) element has a multiplicative inverse is a *field*.

Examples. The natural numbers $\mathbb{N}$ under addition form a semigroup, but not a group under addition, since there is no additive identity and no additive inverses. The integers $\mathbb{Z}$ under addition are a group with identity 0 and the inverse of a is $-a$. The integers under addition and multiplication form a ring, but not a field since there are no multiplicative inverses (except for 1 and -1). The rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and $\mathbb{C}$ each form a field. These three fields differ, for example, in which equations can be solved. The equation $x^2 = 2$ has no solution in $\mathbb{Q}$, but does have a solution in $\mathbb{R}$ and $\mathbb{C}$. The equation $x^2 = -1$ has no solution in $\mathbb{Q}$ nor in $\mathbb{R}$, but does have a solution in $\mathbb{C}$. In fact, every polynomial equation has a solution in $\mathbb{C}$; that is, $\mathbb{C}$ is algebraically closed.

Revised: 2/14/2022