CHAPTER 3 SUMMARY: THE INTEGERS $\mathbb{Z}$ (PART I)

MATH 422, CSUSM. SPRING 2009. AITKEN

1. Introduction

This is a summary of Chapter 3 from Number Systems (Math 378). The integers $\mathbb{Z}$ included the natural numbers together with negative numbers:

$$\ldots, -4, -3-2, -1, 0, 1, 2, 3, 4, \ldots$$

The integers are constructed as equivalence classes of ordered pairs of natural numbers, but we do not need to concern ourselves in this summary with particular method of construction as there are other approaches. In this summary we will focus on the properties of integers, not the construction.

2. $\mathbb{Z}$ as an abelian group

The first main result concerning $\mathbb{Z}$ is that it is an *abelian group* under addition. This is just a fancy way of saying that (i) $\mathbb{Z}$ has an addition $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ that is associative, (ii) that there is an additive identity (zero) element in $\mathbb{Z}$, and (iii) that every element $a \in \mathbb{Z}$ has an additive inverse.

The combination of properties mentioned above (associativity, identity, and inverse) is so common in mathematics, that there is a name for something that possesses them, a *group*. Forget the informal meaning of the word *group* used in everyday life; from now on it will be a technical term referring to a set with the combination of properties mentioned above.[1] If we throw the commutative law into the mix, we call the group *abelian* (after the famous mathematician Abel).

Definition 1. A group G is a set together with a binary operation

$$* : G \times G \to G$$

such that

(i) $*$ is associative: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

(ii) G has an identity element. In other words, there is an element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. (It is easy to prove that the identity is unique).

(iii) Every element of G has an inverse. In other words, if $a \in G$ then there is a $b \in G$ such that $a * b = b * a = e$ where e is an identity for G. (It is easy to prove that the inverse of a is unique).

Date: January 20, 2009.

[1]Mathematics majors typically study groups in more detail in an upper-division (abstract) algebra course.

Exercise 1. In many examples, $*$ is written $+$. Is $\mathbb{N}$ a group under $+$? What about $\mathbb{R}$ and $\mathbb{Q}$?

Definition 2. A group G is said to be *abelian* if the commutative law holds: $a * b = b * a$ for all $a, b \in G$.

Addition is extended from $\mathbb{N}$ to $\mathbb{Z}$ in such a way that $\mathbb{Z}$ is a group under addition. Addition is a binary operation $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. This extension can be described by the following four rules:
(i) If a and b are both in $\mathbb{N}$ we use the same addition as in $\mathbb{N}$.
(ii) If $a \in \mathbb{N}$ and $b = -m$ where m is positive and $m \leq a$, then $a + b$ is the natural number $a - m$.
(iii) If $a \in \mathbb{N}$ and $b = -m$ where m is positive and $a < m$, then $a + b$ is the negative integer $-(m - a)$.
(iv) If $a = -m$ and $b = -n$ where m and n are positive, then $a + b$ is the negative integer $-(m + n)$.

Theorem 1 (Associative law)**.** *If $a, b, c \in \mathbb{Z}$ then $(a + b) + c = a + (b + c)$.*

Theorem 2 (Commutative law)**.** *If $a, b \in \mathbb{Z}$ then $a + b = b + a$.*

Theorem 3 (Identity law)**.** *If $a \in \mathbb{Z}$ then $a + 0 = a$.*

If a is positive, then $-a$ is the corresponding negative integer. If $a = 0$ then $-0 = 0$. Finally if a is a negative integer, and $a = -n$, then $-a$ is n. With this we have the following:

Theorem 4 (Inverse Law)**.** *If $a \in \mathbb{Z}$ then $a + (-a) = (-a) + a = 0$.*

Theorem 5. *The set $\mathbb{Z}$ is an abelian group under addition $+$.*

Definition 3. If $a, b \in \mathbb{Z}$ then $a - b$ is shorthand for $a + (-b)$. In particular $a - a = 0$. This $-$ extends the subtraction of Chapter 2.

Remark 1. If G is a group, then the notation g^{-1} and $-g$ are both used for the inverse of $g \in G$. If the operation for G written '$+$', then $-g$ is usually used to signify the inverse (as we did in $\mathbb{Z}$ above).

Every abelian group satisfies the cancellation law.

Theorem 6. *Suppose $a, b, c \in \mathbb{Z}$, or more generally suppose $a, b, c \in G$ where G is a group under addition $+$. Then, if $a + c = b + c$ then $a = b$.*

Exercise 2. Use the inverse of c to prove the above theorem.

Theorem 7. *Suppose $a \in \mathbb{Z}$, or more generally suppose $a \in G$ where G is a group under addition $+$. Then $-(-a) = a$.*

One advantage of using integers over $\mathbb{N}$ is that you can always solve equations of the form $x + a = b$.

Theorem 8. *Suppose $a, b \in \mathbb{Z}$, or more generally suppose $a, b \in G$ where G is a group under addition $+$. Then, the equation $x + a = b$ has a unique solution in $\mathbb{Z}$. The solution is $x = b - a$.*

Exercise 3. Prove the above theorem.

Exercise 4. Suppose $a, b \in \mathbb{Z}$, or more generally suppose $a, b \in G$ where G is an abelian group under addition $+$. Show that $-(a+b) = (-a) + (-b)$. We often write this with the parentheses removed as

$$-(a+b) = -a - b.$$

(The proof is easier, and better with the parentheses.)

Exercise 5. Show that if e is the identity element of a group, then e is its own inverse.

Theorem 9. *Suppose $a, b \in \mathbb{Z}$, or more generally suppose $a, b \in G$ where G is an abelian group under addition $+$. Then $a - b = 0$ if and only if $a = b$.*

3. Order

Definition 4. Suppose $a, b \in \mathbb{Z}$. Then $a < b$ is defined to mean that there is an element $n \in \mathbb{N}^+$ such that $b = a + n$.

Remark 2. Since this is essentially the same definition we gave in Chapter 1, we infer that the order $<$ on $\mathbb{Z}$ extends the order $<$ on $\mathbb{N}$.

Theorem 10. *Suppose $a, b \in \mathbb{Z}$. Then $a < b$ if and only if $b - a \in \mathbb{N}^+$.*

Definition 5. Suppose $a, b \in \mathbb{Z}$. Then $a \leq b$ means either $a < b$ or $a = b$.

Theorem 11. *Suppose $a, b \in \mathbb{Z}$. Then $a \leq b$ if and only if $b - a \in \mathbb{N}$.*

Theorem 12. *Suppose $a, b, c \in \mathbb{Z}$. If $a < b$ then $a + c < b + c$. If $a \leq b$ then $a + c \leq b + c$.*

Theorem 13. *Let $a \in \mathbb{Z}$. Then $a \in \mathbb{N}$ if and only if $a \geq 0$. Also, a is positive if and only if $a > 0$, and a is negative if and only if $a < 0$.*

Theorem 14. *Transitivity for $<$ holds.*

Theorem 15. *Transitivity for $\leq$ hold. Mixed transitivity for $<$ and $\leq$ hold.*

Theorem 16. *Trichotomy for $<$ holds.*

Remark 3. Since trichotomy and transitivity hold for $<$, it is a linear order.

Theorem 17. *Let $a, b \in \mathbb{Z}$. If $a < b$ then $-b < -a$. If $a \leq b$ then $-b \leq -a$.*

Corollary 18. *Let $c \in \mathbb{Z}$. If $c > 0$ then $-c < 0$. If $c < 0$ then $-c > 0$. If $c \geq 0$ then $-c \leq 0$. If $c \leq 0$ then $-c \geq 0$.*

Theorem 19. *Let $a \in \mathbb{Z}$. There is no integer x with $a < x < a + 1$.*

4. Multiplication in $\mathbb{Z}$

Multiplication is extended from $\mathbb{N}$ to $\mathbb{Z}$. The extension can be described by the following rules:

(i) If $a \geq 0$ and $b \geq 0$, we use the multiplication of $\mathbb{N}$.

(ii) If $a \geq 0$ and $b < 0$, then $b = -n$ where n is a natural number, and ab is given by $-(an)$.

(iii) If $a < 0$ and $b \geq 0$, then $a = -m$ where m is a natural number, and ab is $-(mb)$.

(iv) If $a < 0$ and $b < 0$, then $(-a)$ and $(-b)$ are natural numbers and the product ab is given by natural number multiplication $(-a)(-b)$.

Theorem 20. *If $a \in \mathbb{Z}$ then*

$$0 \cdot a = a \cdot 0 = 0.$$

Lemma 21. *If $a \in \mathbb{Z}$ then*

$$a \cdot 1 = a.$$

Theorem 22. *If $a \in \mathbb{Z}$ then*

$$a \cdot (-1) = -a.$$

Theorem 23 (Distributive law)**.** *If $a, b, c \in \mathbb{Z}$ then*

$$a(b + c) = ab + ac.$$

Theorem 24. *If $a, b \in \mathbb{Z}$ then*

$$(-a)b = a(-b) = -(ab).$$

Theorem 25 (Commutative law)**.** *If $a, b \in \mathbb{Z}$ then*

$$a \cdot b = b \cdot a.$$

Theorem 26 (Associative law)**.** *If $a, b, c \in \mathbb{Z}$ then*

$$a(bc) = (ab)c.$$

5. The ring of integers

Definition 6. A *ring* is a set R equipped with *two* binary operations $R \times R \to R$ satisfying the properties listed below. The binary operations are called *addition* and *multiplication*, and are typically written $+ : R \times R \to R$ and $\cdot : R \times R \to R$. Multiplication is also indicated by juxtaposition, and the usual conventions for parentheses are employed. A ring R must satisfy the following:

(i) The set R is an abelian group under addition. In other words,
- (i.1) addition is associative,
- (i.2) addition has an identity, typically written 0,
- (i.3) every element $x \in R$ has an additive inverse, typically written $-x$, and
- (i.4) addition is commutative.

(ii) Multiplication is associative: for all $x, y, z \in R$,

$$(xy)z = x(yz).$$

(iii) There is a multiplicative identity[2], typically written 1: for all $x \in R$,

$$x \cdot 1 = 1 \cdot x = x.$$

(iv) The distributive law holds: for all $x, y, z \in R$

$$x(y + z) = xy + xz,$$

$$(y + z)x = yx + zx.$$

Definition 7. Suppose that R is a ring such that

$$xy = yx$$

for all $x, y \in R$. Then we say that the *commutative law* holds for R, and we call R a *commutative ring.*

Remark 4. The set of 2 by 2 matrices with entries in $\mathbb{R}$ forms a non-commutative ring. Thus not all rings are commutative.

Exercise 6. Explain why $\mathbb{N}$ is not a ring.

Theorem 27. *The integers $\mathbb{Z}$ form a commutative ring.*

Proof. This follows from earlier results. □

Exercise 7. List the results needed to prove the above theorem. Hint: start with Theorem 5.

Many results that hold for $\mathbb{Z}$ actually extends to other rings as well. We give four examples.

Theorem 28. *If R is a ring, then*

$$x \cdot 0 = 0 \cdot x = 0$$

for all $x \in R$.

Proof. Recall the law $y + 0 = y$ for any additive group. So $0 + 0 = 0$. Thus

$$x \cdot 0 = x(0 + 0) = x \cdot 0 + x \cdot 0$$

by the distributive law. By adding the inverse $-(x \cdot 0)$ to both sides, we get

$$0 = x \cdot 0.$$

A similar argument shows $0 \cdot x = 0$. □

Theorem 29. *If $x, y \in R$ where R is a ring, then*

$$(-x)y = -(xy) = x(-y).$$

[2]Some algebra textbooks do not require the multiplicative identity, but many do. Most rings that one considers, however, have a multiplicative identity.

Proof. Observe that

$$xy + (-x)y = \big(x + (-x)\big)y = 0 \cdot y = 0$$

by the previous theorem. Thus xy and $(-x)y$ are additive inverses. So

$$(-x)y = -(xy).$$

A similar argument shows $x(-y) = -(xy)$. □

Theorem 30. *If $y \in R$ where R is a ring, then*

$$(-1)y = y(-1) = -y.$$

Proof. This follows from the previous theorem. For example, if $x = 1$ then $(-1)y = -(1y)$ by the previous theorem. □

Theorem 31. *If $x, y \in R$ where R is a ring, then*

$$(-x)(-y) = xy.$$

Proof. By Theorem 29, used twice,

$$(-x)(-y) = -\big(x(-y)\big) = -\big(-(xy)\big).$$

However, $-(-z) = z$ for all z in an additive group (and R is an additive group under addition by the definition of ring). Thus

$$(-x)(-y) = -\big(-(xy)\big) = xy.$$

□

We end the section with the so-called "FOIL-rule".[3]

Theorem 32. *Let $a, b, c, d \in R$ where R is a ring then*

$$(a + b)(c + d) = ac + ad + bc + bd.$$

Remark 5. Parentheses are not needed because + is associative.

Exercise 8. Prove Theorem 32 using the distributive law.

6. Other Properties of Multiplication

We end with some important properties of $\mathbb{Z}$.[4]

Theorem 33. *The product of two positive integers is positive, the product of two negative integers is positive, the product of a positive and a negative integer is negative.*

Corollary 34. *Suppose $x, y \in \mathbb{Z}$. If $x \neq 0$ and $y \neq 0$, then $xy \neq 0$.*

Corollary 35. *If $x, y \in \mathbb{Z}$ and if $xy = 0$, then $x = 0$ or $y = 0$.*

Exercise 9. Show how the above corollaries follow from Theorem 33.

[3] A favorite mnemonic in HS algebra: "first, outside, inside, last"

[4] These are properties that will extend to $\mathbb{Q}$ and $\mathbb{R}$, but not to rings in general.

Definition 8. An *integral domain* is a commutative ring R with the additional properties that (i) $0 \neq 1$, and (ii) for $x, y \in R$,

$$xy = 0 \ \Rightarrow \ x = 0 \ \vee \ y = 0.$$

The name *integral* domain suggests it was inspired by the integers. Needless to say, there are other interesting integral domains that mathematicians study.

Corollary 36. *The ring $\mathbb{Z}$ is an integral domain.*

The cancellation law for $\mathbb{N}$ can be found in Chapter 1. This law also holds in $\mathbb{Z}$. In fact, it doesn't just hold in $\mathbb{Z}$, but it holds in any integral domain. (Warning: it does not hold in every ring though).

Theorem 37 (Cancellation Law for Multiplication)**.** *Let R be $\mathbb{Z}$ or any integral domain. If $a, b, c \in R$ and if $c \neq 0$ then*

$$ac = bc \implies a = b.$$

Proof. Add $-ac$ to both sides of the equation $ac = bc$:

$$0 = ac + (-ac) = bc + (-ac) = bc + (-a)c = (b - a)c$$

(using Theorem 29, and the Distributive Law). Since R is an integral domain, $b - a = 0$ or $c = 0$. However, $c \neq 0$ by assumption. Thus $b + (-a) = 0$. By adding a to both sides, and using the identity, associative, and inverse laws (valid since R is a ring), we get $b = a$. □

We end with standard laws concerning multiplication and inequalities.

Theorem 38. *Suppose that $x, y, z \in \mathbb{Z}$. Then*

$$x < y \ \wedge \ z > 0 \ \Rightarrow \ xz < yz,$$
$$x < y \ \wedge \ z < 0 \ \Rightarrow \ xz > yz,$$
$$x \leq y \ \wedge \ z \geq 0 \ \Rightarrow \ xz \leq yz,$$

and

$$x \leq y \ \wedge \ z \leq 0 \ \Rightarrow \ xz \geq yz.$$