Lecture 2

Reference: Judson, Chapter 2

Integers $\mathbb{Z}$

Integer numbers not only form a set, but also have a rich algebraic structure. Our goal now is to formalize this structure in an axiomatic way. This will allow us to prove results about integers which will be automatically satisfied in a much wider setting.

Addition

Given two integers $m, n \in \mathbb{Z}$ we can add the up: $(m+n)$. Formally, we have a map

$$+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

This map satisfies several familiar properties

G1 (associativity) Given arbitrary $m, n, k \in Z$, we have

$$(m+n)+k = m+(n+k);$$

G2 (neutral element). There exists a special element (zero) $0 \in \mathbb{Z}$ such that

$$0+m = m+0 = m$$

for any $m \in Z$.

G3 (additive inverse). Given any $n \in \mathbb{Z}$ there exists element $(-n) \in \mathbb{Z}$ such that

$$n+(-n) = (-n)+n = 0.$$

GC (commutativity). Given any $m, n \in \mathbb{Z}$ we have

$$m+n = n+m.$$

The three properties **G1, G2, G3**, that is, associativity, existence of a neutral element and existence of inverses, are characteristic of an important algebraic structure called a **group**. A group satisfying additionally property **GC** is called a **commutative** (or abelian) group. The above shows that the set of integers $(\mathbb{Z}, +)$ endowed with addition is a commutative group. We are going to see many other examples of groups in this course, and are going to study groups in general.

Multiplication

Given two integers $m, n \in \mathbb{Z}$ we can multiply them mn. That is we have a map

$$\begin{aligned} \times \colon \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (m, n) &\mapsto mn \end{aligned}$$

This map satisfies the following properties

R1 (associativity). For all $m, n, k \in \mathbb{Z}$ we have

$$(mn)k = m(nk).$$

R2 (distributivity). For all $m, n, k \in \mathbb{Z}$ we have

$$(m+n)k = mk + nk \text{ and } k(m+n) = km + kn.$$

R3 (neutral element). There exists a distinguished element $1 \in \mathbb{Z}$ such that for any $m \in \mathbb{Z}$ we have

$$1m = m1 = m.$$

The properties **G1, G2, G3, GC, R1 , R2** and **R3** characterize an algebraic structure called a ring. In short, a ring is a commutative group with an extra operation that is well-behaved with respect to the commutative group operation.

The Division Algorithm

Let us recall the notion of divisibility of integers and its basic properties.

Definition 1: Division

We say that nonzero number $b \in \mathbb{Z}$ **divides** $a \in \mathbb{Z}$, if there exists $q \in \mathbb{Z}$ such that

$$a = bq.$$

In this case we write $b \,|\, a$.

Clearly we have the following properties

- for any $a \in \mathbb{Z}$, $a \neq 0$ we have $a|a$;
- any integer divides 0;
- 0 does not divide any integer;
- if $a|b$ and $b|a$, then $a = \pm b$.

Given two integers we can divide one by the other with a remainder:

Theorem 1: Division Theorem

For any $a \in \mathbb{Z}$ and a nonzero $b \in \mathbb{Z}$ there exist unique $q \in \mathbb{Z}$ and a **remainder** $r \in \{0, 1, \ldots, |b| - 1\}$ such that

$$a = bq + r.$$

Example 1

Dividing 7 by 2 with remainder we find

$$7 = 23 + 1,$$

i.e., $q = 3$ and $r = 1$.

Dividing 15 by -4 with remainder we find

$$15 = (-4)(-3) + 3,$$

i.e. $q = -3$ and $r = 3$.

Greatest Common divisor

For any $a, b \in \mathbb{Z}$ such that a and b do not vanish simultaneously, we can define the *greatest common divisor*

$$\gcd(a, b)$$

to be the largest integer d such that $d|a$ and $d|b$. Clearly $\gcd(a, 0) = |a|$.

Our next goal is to develop an efficient algorithm for computing $\gcd(a, b)$ and derive important consequences from it. In particular, we prove that if d' is any common divisor of a and b, then $d'|\gcd(a, b)$.

Theorem 2: Euclidean algorithm

Given a pair $a, b \in \mathbb{Z}$ such that $b \neq 0$, define a sequence of numbers $q_1, q_2, q_3, \ldots$ and $r_1, r_2, r_3, \ldots$ as follows.

1. divide a by b with remainder:
$$a = bq_1 + r_1.$$

2. if $r_1 = 0$ stop. Otherwise divide b by r_1 with remainder:
$$b = r_1 q_2 + r_2.$$

...

$(k+1)$. if $r_k = 0$ stop. Otherwise divide r_{k-1} by r_k with remainder:
$$r_{k-1} = r_k q_{k+1} + r_{k+1}.$$

The process stops at a step such that $r_N = 0$. Then
$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{N-1}, 0) = r_{N-1}.$$

Proof. Let us analyze the first step of the algorithm. Identity
$$a = bq_1 + r_1$$
implies that the set of common divisors of a and b coincides with the set of common divisors of b and r_1. Indeed, any common divisor of a and b will divide r_1 and vice versa: any common divisor of b and r_1 will divide a. In particular, since the sets of common divisors are the same:
$$\gcd(a, b) = \gcd(b, r_1).$$
Proceeding the same way to the second and further steps of the algorithm we find that
$$\gcd(a, b) = \gcd(r_{N-1}, r_N).$$
But since $r_N = 0$, the latter equals r_{N-1}. □

Remark 1

In the course of proof we have shown that the set of common divisors of a and b coincides with the set of divisors of $r_{N-1} = \gcd(a, b)$

Besides providing an efficient way for computing greatest common divisor, Euclidean algorithm also is the key tool in proving many fundamental statements in algebra and number theory. Most importantly, it implies the following statement.

Proposition 1

Let $a, b \in \mathbb{Z}$ be a pair of integers, such that at least one of a and b is nonzero. Then there exist (not unique!) integers $u, v \in \mathbb{Z}$ such that
$$\gcd(a, b) = au + bv.$$

Proof. We will prove this statement by applying Eucledian algorithm to the pair $\gcd(a, b)$. Traversing steps of the algorithm backwards we prove that at every step

- There exist $u_k, v_k \in \mathbb{Z}$ such that
$$\gcd(a, b) = r_{k-1} u_k + r_k v_k.$$

Indeed, it is obviously true at the last step, where $r_{N-1} = \gcd(a, b)$ and $r_N = 0$, since we can take $u_N = 1$ and $v_N = 0$.

Now, going backwards, we have

$$\gcd(a,b) = r_{k-1}u_k + r_k v_k$$
$$r_{k-2} = r_{k-1}q_k + r_k.$$

Substituting r_k from the second equation to the first equation, we find

$$\gcd(a,b) = r_{k-1}u_k + (r_{k-2} - r_{k-1}q_k)v_k = r_{k-2}\underbrace{v_k}_{:=u_{k-1}} + r_{k-1}\underbrace{(u_k - q_k v_k)}_{:=v_{k-1}}.$$

Continuing the process all the way up to a and b we prove the proposition. □

Proposition 1 has two important corollaries.

Corollary 1

Numbers $a, b \in \mathbb{Z}$ are coprime (i.e., $\gcd(a,b) = 1$) if and only if there exist $u, v \in \mathbb{Z}$ such that

$$au + bv = 1$$

Proof. One direction is exactly the statement of Proposition 1. The other direction is obvious, since given u and v as in the identity, we find that any common divisor of a and b must also divide 1, so that a and b must be coprime. □

Corollary 2

Given numbers $a, b, c \in \mathbb{Z}$ such that $a|(bc)$ and $\gcd(a,b) = 1$ we must have

$$a|c.$$

Proof. Since $\gcd(a,b) = 1$, by the above corollary we can find $u, v \in \mathbb{Z}$ such that

$$au + bv = 1,$$

in particular

$$acu + bcv = c.$$

The first summand on the left hand side is obviously divisible by a (since a is one of the factor). The second summand is also divisible by a, since it has a factor bc which is divisible by a by assumption. Therefore the right hand side c is also divisible by a as stated. □