Ideals

A subset I of $\mathbf{Z}$ is said to be an *ideal* if:

(i) I contains 0

(ii) the sum of any two elements of I is in I: if $x, y \in I$ then $x + y \in I$

(iii) any integer multiple of any element of I is in I, i.e. if $m \in \mathbf{Z}$ and $x \in I$ then $mx \in I$.

Observe that if k is any integer then the set of all multiples of $\mathbf{Z}$,

$$k\mathbf{Z} \stackrel{\text{def}}{=} \{kx : x \in \mathbf{Z}\},$$

is an ideal. The integer k is called a *generator* of this ideal.

In fact all ideals are of this form:

Theorem If I is an ideal then there is an integer k such that $I = k\mathbf{Z}$. If $I = \{0\}$ then $k = 0$; if $I \neq \{0\}$ then k can be taken to be the smallest positive integer in I.

Proof. The simplest case is if $I = \{0\}$; in this case $k = 0$ does the job, i.e. I is $0\mathbf{Z}$.

Suppose now that $I \neq \{0\}$. We will show that I equals $k\mathbf{Z}$, where k is the smallest positive integer in I. To begin with we need to check that I does indeed contain positive integers. Since I contains 0 but is not equal to $\{0\}$, it follows that I contains some integer m other than 0. If m is positive then we already see that I contains a positive integer. If m is negative we note that $-m = (-1)m$, being a multiple of m, is in I and $-m$ is positive. Thus, in either case, I contains a positive integer.

Let k be the smallest positive integer in I (such a k exists by the well-ordering principle). Since $k \in I$ all multiples of k are in I and so $k\mathbf{Z} \subset I$. We will now show that every element of I is a multiple of k. Let $x \in I$. Dividing x by k we obtain a quotient q and a remainder r, both integers, with $0 \leq r < k$ and

$$x = qk + r$$

Thus $r = x - qk = x + (-q)k$ is in I since both x and $(-q)k$ (a multiple of k) are in I. But then we have this new element r in I which is ≥ 0 and less than k. Since k is the *smallest* positive integer in I it follows that $r = 0$. This means

$$x = qk$$

Thus x is a multiple of k, i.e. $x \in k\mathbf{Z}$. This every element of I is in $k\mathbf{Z}$. We have already noted that every element of $k\mathbf{Z}$ is in I. So

$$I = k\mathbf{Z}.$$

Note that any integer multiple of k is also an integer multiple of $-k$, and conversely. So $(-k)\mathbf{Z} = k\mathbf{Z}$, and so we could also take for k the negative of the smallest positive integer in I. **QED**

If A and B are any sets of integers then their *sum* $A + B$ is the set of all sums of elements drawn from A and from B:

$$A + B \stackrel{\text{def}}{=} \{x + y : x \in A, y \in B\}$$

Define $A_1 + \cdots + A_n$ for any $A_1, ..., A_n \subset \mathbf{Z}$ similarly, to be the set of all numbers which can be expressed as sums $a_1 + \cdots + a_n$, with $a_1 \in A_1, ..., a_n \in A_n$. There is an official definition of this type which uses an inductive procedure: first define the sum of any two subsets; then, assuming that the sum of n subsets have been defined, define the sum $A_1 + \cdots + A_{n+1}$ to be the sum of $A_1 + \cdots + A_n$ and A_{n+1}.

Proposition The sum of any two ideals is an ideal.

Proof. Consider ideals I and J. We shall show that $I + J$ is an ideal. First, since 0 is in both I and J we have $0 = 0 + 0 \in I + J$. Next suppose $x, y \in I + J$. We have to show that $x + y$ is in $I + J$. Since $x \in I + J$ we have $x = a + b$ for some $a \in I$ and $b \in J$. Since $y \in I + J$ we have $y = c + d$ for some $c \in I$ and $d \in J$. Then

$$x + y = (a + b) + (c + d) = (a + c) + (b + d)$$

In this $a + c$ is in I since $a, c \in I$, while $b + d \in J$ because $b, d \in J$. So $x + y$ is the sum of an element $a + c$ of I and an element $b + d$ of J. This $x + y \in I + J$. Next, for any integer m we have

$$mx = m(a + b) = ma + mb$$

Here ma, being a multiple of $a \in I$ is in I, and similarly mb is in J. So mx is the sum of an element of I and an element of J. Then $mx \in I + J$. **QED**

There is a standard procedure for extending such a result, valid for two objects, to a result for a finite number of objects. Here is an example:

Proposition The sum of any finite non-empty collection of ideals is an ideal, i.e. if $I_1, ..., I_n$ are ideals in $\mathbf{Z}$ then $I_1 + \cdots + I_n$ is an ideal.

Proof. The result is trivially true if $n = 1$. For $n = 2$ we have already proved the result. Now suppose the result holds for $n = k$. We will prove it for $k + 1$ ideals. Let $I_1, ..., I_{k+1}$ be ideals. From

$$I_1 + \cdots + I_{k+1} = (I_1 + \cdots + I_k) + I_{k+1}$$

we see that the first term on the right $J = I_1 + \cdots + I_k$ is an ideal and of course so is I_{k+1}, and so the sum $J + I$ is an ideal. Thus the result holds for $n = k + 1$. So the result holds for all $n \in \{1, 2, 3, ...\}$. **QED**

You should work out the proof of:

Proposition The intersection of any non-empty collection of ideals is an ideal.

There is an important relation between divisibility and inclusion of ideals:

Proposition. For any integers $a, b \in \mathbf{Z}$, the ideal $a\mathbf{Z}$ is a subset of $b\mathbf{Z}$ if and only if b is a divisor of a:

$$a\mathbf{Z} \subset b\mathbf{Z} \leftrightarrow b|a$$

Proof. Suppose $a\mathbf{Z} \subset b\mathbf{Z}$. Since $a = a.1 \in a\mathbf{Z}$ we have $a \in b\mathbf{Z}$, i.e. a is a multiple of b, which means that $b|a$.

Next suppose conversely that $b|a$. Then $a = bx$ for some integer x. Then any multiple ka of a is of the form $ka = kbx = (kx)b$, i.e. is a multiple of b. Thus $a\mathbf{Z} \subset b\mathbf{Z}$. **QED**

As an application we have

Proposition. For any integers $a, b \in \mathbf{Z}$, the ideal $a\mathbf{Z} + b\mathbf{Z}$ is generated by the greatest common divisor of a, b:

$$a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}$$

where $c = \gcd(a, b)$. (The gcd of 0 and 0 is defined to be 0.)

Proof. Lets deal with the trivial case first. Suppose $a = b = 0$. Then $a\mathbf{Z} = \{0\}$ and $b\mathbf{Z} = \{0\}$ and so $a\mathbf{Z} + b\mathbf{Z}$ is also $\{0\} = 0\mathbf{Z}$, and so $c = 0$, which is, by definition, the gcd of a and b here.

Now suppose a or b is not zero. Then $a\mathbf{Z} + b\mathbf{Z} \neq \{0\}$. Since $a\mathbf{Z} + b\mathbf{Z}$ is an ideal, we have

$$a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}$$

where c is the smallest positive integer in $a\mathbf{Z} + b\mathbf{Z}$. Now $a = a.1 + 0.b$ is in $a\mathbf{Z} + b\mathbf{Z}$, and so a is a multiple of c. Similarly, c is a multiple of b. So c is a divisor of both a and b, i.e. a common divisor of a and b. Next suppose k is any common divisor of a and b, i.e. $a\mathbf{Z} \subset k\mathbf{Z}$ and $b\mathbf{Z} \subset k\mathbf{Z}$. So, since $k\mathbf{Z}$ is an ideal,

$$a\mathbf{Z} + b\mathbf{Z} \subset k\mathbf{Z}$$

Thus $c\mathbf{Z} \subset k\mathbf{Z}$, and so $k|c$. Thus k is a divisor of the positive integer c and so $k \geq c$. So c is the greatest common divisor of a and b. **QED**