MAT 3343, APPLIED ALGEBRA, FALL 2003

Handout 2: Ideals of Integers

(Supplement to Chapter 1.2)

Peter Selinger

1 Ideals of Integers

Recall that $\mathbb{Z} = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$ is the set of integers. If $n \in \mathbb{Z}$ is any integer, we write $n\mathbb{Z}$ for the set

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}.$$

So for example, $2\mathbb{Z}$ is the set of even numbers, $3\mathbb{Z}$ is the set of multiples of 3, and $0\mathbb{Z}$ is the one-element set $\{0\}$. Notice that $a \in n\mathbb{Z}$ if and only if n divides a. In particular, we have $n \in n\mathbb{Z}$ and $0 \in n\mathbb{Z}$, for all n.

Remark 1.1. If $n\mathbb{Z} = m\mathbb{Z}$, then $n = m$ or $n = -m$. To prove this, first notice that in this situation, $n \in m\mathbb{Z}$ and $m \in n\mathbb{Z}$. Thus $m|n$ and $n|m$. This implies that $n = m$ or $n = -m$.

Notice that, as shown in examples in class, the intersection of two sets $n\mathbb{Z}$ and $m\mathbb{Z}$ is again of the form $k\mathbb{Z}$, for some k. For example:

$$\begin{array}{rcl} 4\mathbb{Z} \cap 6\mathbb{Z} & = & 12\mathbb{Z} \\ 4\mathbb{Z} \cap 5\mathbb{Z} & = & 20\mathbb{Z} \\ 0\mathbb{Z} \cap 5\mathbb{Z} & = & 0\mathbb{Z}. \end{array}$$

Also, if A and B are sets of integers, let us write $A + B$ for the set

$$A + B = \{a + b \mid a \in A \text{ and } b \in B\}.$$

So, for example, $4\mathbb{Z} + 6\mathbb{Z}$ is the set of all integers of the form $4x + 6y$, where $x, y \in \mathbb{Z}$. This happens to cover precisely the even integers, so we find that $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$. Again, trying different examples, we find that the sum of two sets $n\mathbb{Z}$ and $m\mathbb{Z}$ always seems to be of the form $d\mathbb{Z}$, for some integer d. For example:

$$\begin{array}{rcl} 4\mathbb{Z} + 6\mathbb{Z} & = & 2\mathbb{Z} \\ 4\mathbb{Z} + 5\mathbb{Z} & = & 1\mathbb{Z} \\ 0\mathbb{Z} + 5\mathbb{Z} & = & 5\mathbb{Z}. \end{array}$$

Our goal is to show that this always works. It will be useful to characterize the sets of the form $n\mathbb{Z}$ a little more abstractly.

Definition. A subset $I \subseteq \mathbb{Z}$ is called an *ideal* if it satisfies the following three conditions:

(1) If $a, b \in I$, then $a + b \in I$.

(2) If $a \in I$ and $k \in \mathbb{Z}$, then $ak \in I$.

(3) $0 \in I$.

The point is that, as we will show now, the ideals in $\mathbb{Z}$ are exactly the subsets of the form $n\mathbb{Z}$. In other words, the sets of the form $n\mathbb{Z}$ are *characterized* by the three properties (1)–(3) in the definition. This is proved by the combination of Lemmas 1.2 and 1.3 below.

Lemma 1.2. *Any set of the form $n\mathbb{Z}$ is an ideal.*

Proof. Let $I = n\mathbb{Z}$. We have to show I satisfies the three properties in the definition of an ideal.

(1) Take arbitrary elements $a, b \in I$. We have to show that $a + b \in I$. Because $a \in n\mathbb{Z}$, we know that $a = nx$ for some $x \in \mathbb{Z}$. Because $b \in n\mathbb{Z}$, we know that $b = ny$ for some $y \in \mathbb{Z}$. Then $a + b = nx + ny = n(x + y) \in n\mathbb{Z} = I$.

(2) Take arbitrary elements $a \in I$ and $k \in \mathbb{Z}$. We have to show that $ak \in I$. But $a \in n\mathbb{Z}$, hence we know that $a = nx$ for some $x \in \mathbb{Z}$. It follows that $ak = (nx)k = n(xk) \in n\mathbb{Z} = I$.

(3) We have to show that $0 \in I$. But clearly, $0 = 0n$, so it follows that $0 \in n\mathbb{Z} = I$. $\square$

Lemma 1.3. *Any ideal I of integers is of the form $n\mathbb{Z}$, for some $n \in \mathbb{Z}$.*

The idea of the proof is simple: let n be the smallest positive element in I, and then prove (using the three properties of I) that $I = n\mathbb{Z}$.

The reason the real proof is a bit longer is that we have to worry about a number of details: for instance, we have to worry about what happens if there are no positive elements in I (in this case we can't let n be such an element!).

The proof makes use of the following principle, which says that if there is a positive integer with a certain property, then there is a *smallest* such integer.

Principle 1.4 (Well-foundedness principle). *If A is a non-empty set of positive integers, then A has a smallest element.*

Proof of Lemma 1.3: We know, from property (3), that $0 \in I$. In case $I = \{0\}$, we are done, because $I = 0\mathbb{Z}$ is of the desired form. Otherwise, there must be some non-zero element $k \in I$. Let $A = \{x \in I \mid x > 0\}$. Note that A is non-empty, because from property (2), $-k \in I$, and hence either k or $-k$ is in A. By the well-foundedness principle, A has a smallest element. Let n be the smallest element in A.

Next, we want to show that $I = n\mathbb{Z}$. We do this by first showing than $n\mathbb{Z} \subseteq I$, then that $I \subseteq n\mathbb{Z}$.

To show that $n\mathbb{Z} \subseteq I$, take an arbitrary element $a \in n\mathbb{Z}$. By definition of $n\mathbb{Z}$, we know that $a = nx$, for some $x \in \mathbb{Z}$. Then from $n \in I$ and $x \in \mathbb{Z}$, it follows by property (2) that $nx \in I$, thus $a \in I$. Since a was arbitrary, this shows that $n\mathbb{Z} \subseteq I$.

To show that $I \subseteq n\mathbb{Z}$, we use the method of contradiction. Thus, assume that $I \not\subseteq n\mathbb{Z}$. Then there exists some $k \in I$ such that $k \notin n\mathbb{Z}$. Note that $k \notin n\mathbb{Z}$ implies $k \neq 0$. Let $B = \{x \in I \mid x > 0 \text{ and } x \notin n\mathbb{Z}\}$. From property (2), we know that $-k \in I$ and $-k \notin n\mathbb{Z}$, so either $k \in B$ or $-k \in B$. Thus, B is non-empty, and by the well-foundedness principle, it has a least element, say a.

We distinguish three cases:

Case 1: Suppose $a > n$. Then $a - n$ is positive. Also, from $a \in I$ and $n \in I$, it follows by property (2) that $-n \in I$ and by property (1) that $a - n \in I$. Also, since $a \notin n\mathbb{Z}$, it follows that $a - n \notin n\mathbb{Z}$. So $a - n \in B$, contradicting the fact that a is the *smallest* element of B.

Case 2: Suppose $a = n$. This contradicts the fact that $a \notin n\mathbb{Z}$.

Case 3: Suppose $a < n$. But $a \in I$, therefore $a \in A$, contradicting the fact that n was the smallest element in A.

All three cases lead to a contradiction, which implies that our assumption that $I \not\subseteq n\mathbb{Z}$ was false. Therefore $I \subseteq n\mathbb{Z}$. Together with $n\mathbb{Z} \subseteq I$, this implies that $I = n\mathbb{Z}$, which finishes the proof of the lemma. □

Now that we know that an ideal is exactly the same thing as a set of the form $n\mathbb{Z}$, we want to show that the intersection of two ideals is again an ideal, and similarly for sums.

Lemma 1.5. *(a) If I and J are ideals, then so is $I \cap J$.*

(b) If I and J are ideals, then so is $I + J$.

In the following proof, only one of the six cases is given. The remaining cases are left as homework.

Proof. (a) Suppose I and J are ideals. To show that $I \cap J$ is an ideal, we must show that it satisfies the three properties in the definition of an ideal. We prove each property in turn.

(1) Suppose $a, b \in I \cap J$. We want to show that $a + b \in I \cap J$. By assumption, we know that $a \in I$ and $a \in J$ and $b \in I$ and $b \in J$. By property (1) of I, we have $a + b \in I$. By property (1) of J, we have $a + b \in J$. It follows that $a + b \in I + J$.

(2) …

(3) …

(b) Suppose I and J are ideals. We need to show that $I + J$ is an ideal.

(1) …

(2) …

(3) …

We have now proved what we stated in the beginning: any intersection or sum of two sets of the form $n\mathbb{Z}$ and $m\mathbb{Z}$ is again of the form $k\mathbb{Z}$. We summarize this result in the following theorem:

Theorem 1.6. *If $n, m \in \mathbb{Z}$, then there exist integers k and d such that*

$$\begin{aligned} n\mathbb{Z} \cap m\mathbb{Z} &= k\mathbb{Z}, \\ n\mathbb{Z} + m\mathbb{Z} &= d\mathbb{Z}. \end{aligned}$$

Proof. By Lemma 1.2, we know that $n\mathbb{Z}$ and $m\mathbb{Z}$ are ideals. By Lemma 1.5, we know that $n\mathbb{Z} \cap m\mathbb{Z}$ and $n\mathbb{Z} + m\mathbb{Z}$ are also ideals. By Lemma 1.3, we know that they are of the form $k\mathbb{Z}$ and $d\mathbb{Z}$, respectively. □

Also note that, by Remark 1.1, the numbers k and d in Theorem 1.6 are essentially unique: they are determined up to a sign.

2 Least common multiple, greatest common divisor

Let us compute some instances of Theorem 1.6. We compute k and d for various different values of n and m.

$$\begin{array}{rcl} 4\mathbb{Z}\cap 6\mathbb{Z} &=& 12\mathbb{Z} \\ 6\mathbb{Z}\cap 6\mathbb{Z} &=& 6\mathbb{Z} \\ 8\mathbb{Z}\cap 5\mathbb{Z} &=& 40\mathbb{Z} \\ 9\mathbb{Z}\cap 6\mathbb{Z} &=& 18\mathbb{Z} \\ 3\mathbb{Z}\cap 5\mathbb{Z} &=& 15\mathbb{Z} \end{array} \qquad \begin{array}{rcl} 4\mathbb{Z}+6\mathbb{Z} &=& 2\mathbb{Z} \\ 6\mathbb{Z}+6\mathbb{Z} &=& 6\mathbb{Z} \\ 8\mathbb{Z}+5\mathbb{Z} &=& 1\mathbb{Z} \\ 9\mathbb{Z}+6\mathbb{Z} &=& 3\mathbb{Z} \\ 3\mathbb{Z}+5\mathbb{Z} &=& 1\mathbb{Z} \end{array}$$

We observe that the numbers in the first column appear to be greatest common divisors, and the number in the right column appear to be least common multiples.

Definition. A *common divisor* of two integers n and m is an integer d such that $d|n$ and $d|m$. Further, d is called a *greatest common divisor* if, whenever e is another common divisor of n and m, then $e|d$.

Definition. A *common multiple* of two integers n and m is an integer k such that $n|k$ and $m|k$. Further, k is called a *least common multiple* if, whenever e is another common multiple of n and m, then $k|e$.

The following lemma shows that the numbers d and k in Theorem 1.6 are indeed a greatest common divisor and a least common multiple.

Lemma 2.1. *(a) $a\mathbb{Z}\subseteq b\mathbb{Z}$ if and only if $b|a$.*

(b) If $n\mathbb{Z}+m\mathbb{Z}=d\mathbb{Z}$, then d is a greatest common divisor of n and m.

(c) If $n\mathbb{Z}\cap m\mathbb{Z}=k\mathbb{Z}$, then k is a least common multiple of n and m.

Proof. (a) Exercise.

(b) Suppose that $n\mathbb{Z}+m\mathbb{Z}=d\mathbb{Z}$. First, we need to show that d is a common divisor of n and m. But we have $n\mathbb{Z}\subseteq d\mathbb{Z}$ and $m\mathbb{Z}\subseteq d\mathbb{Z}$. It follows from part (a) that $d|n$ and $d|m$, hence d is a common divisor. Next, we need to show that it is a least common divisor. So suppose that e is another common divisor, i.e., that $e|n$ and $e|m$. By part (a), we have $n\mathbb{Z}\subseteq e\mathbb{Z}$ and $m\mathbb{Z}\subseteq e\mathbb{Z}$. Since $e\mathbb{Z}$ is closed under addition, it follows that $n\mathbb{Z}+m\mathbb{Z}\subseteq e\mathbb{Z}$, and therefore $d\mathbb{Z}\subseteq e\mathbb{Z}$. Finally, by part (a) again, it follows that $e|d$. Thus, d is a greatest common divisor.

(c) Suppose that $n\mathbb{Z}\cap m\mathbb{Z}=k\mathbb{Z}$. First, we show that k is a common multiple of n and m. But we have $k\mathbb{Z}\subseteq n\mathbb{Z}$ and $k\mathbb{Z}\subseteq m\mathbb{Z}$. It follows from part (a) that $n|k$ and $m|k$, so k is a common multiple. Now, suppose that e is another common multiple of n and m. then $n|e$ and $m|e$. By part (a), we have $e\mathbb{Z}\subseteq n\mathbb{Z}$ and $e\mathbb{Z}\subseteq m\mathbb{Z}$. It follows from set theory that $e\mathbb{Z}\subseteq n\mathbb{Z}\cap m\mathbb{Z}=k\mathbb{Z}$, hence, again by part (a), we have $k|e$. Thus, k is a least common multiple. □

Corollary 2.2. *Any pair of integers n,m have a greatest common divisor and a least common multiple.*

Proof. Theorem 1.6 and Lemma 2.1. □

Greatest common divisors and least common multiples are unique up to a sign. For instance, if d and d' are both greatest common divisors of n and m, then we must have $d|d'$ and $d'|d$, which implies $d=d'$ or $d=-d'$. When we speak of *the* greatest common divisor, we always mean the one that is not negative. It is also denoted as $\gcd(n,m)$. The situation is similar for least common multiples, and the unique non-negative least common multiple of n and m is often written as $\operatorname{lcm}(n,m)$.

Remark. In our definition of the greatest common divisor d of n and m, we have not actually required that d is *greater* than any other common divisor, but only that it is a *multiple* of any other common divisor. In this way, we do not have to make special arrangements in the case where n and/or m are 0. For instance, any integer is a common divisor of 0 and 0, but $\gcd(0,0)=0$. The name "greatest" common divisor is actually bad terminology, but it is nevertheless standard. A similar remark applies to least common multiples.

Theorem 2.3. *If $d=\gcd(n,m)$, then there exists integers a and b such that $d=an+bm$.*

Proof. This follows directly from the fact that $n\mathbb{Z}+m\mathbb{Z}=d\mathbb{Z}$. Namely, we have $d\in n\mathbb{Z}+m\mathbb{Z}$, and thus, $d=an+bm$, for some $a,b\in\mathbb{Z}$. □

In general, finding a and b such that $d=an+bm$ is not as easy as it looks. For instance, we have $\gcd(89,144)=1$. Therefore, there exist integers a and b such that $89a+144b$. Try to find them yourself! This can be quite a lot of work. We will later learn a method for finding a and b efficiently.

3 Exercises

Problem 1 Finish the proof of Lemma 1.5. Try to imitate the style used in the first part.

Problem 2 Prove that $n|m$ and $m|p$ implies $n|p$.

Problem 3 Prove Lemma 2.1(a). There are two directions to prove: $a\mathbb{Z} \subseteq b\mathbb{Z} \Rightarrow b|a$, and $b|a \Rightarrow a\mathbb{Z} \subseteq b\mathbb{Z}$.

Problem 4 Consider Principle 1.4, the well-foundedness principle. It states that any non-empty subset of positive integers has a least element. Answer the following questions. In each case, if the answer is "no", give a counterexample (i.e., a set which does not have a least element).

(a) Is the principle still true if we drop the word "non-empty"?

(b) Is the principle still true if we drop the word "positive"?

(c) Is the principle still true if we replace the word "integer" by "rational number"?

(d) Is the principle still true if we replace the word "positive" by "non-negative"? Recall that a number x is positive if $x > 0$, and non-negative if $x \geqslant 0$.