MATH 351 SECTION 2: IDEALS OF $\mathbb{Z}_{20}$

TAMAR BLANKS

During workshop, we briefly talked about the ideals of $\mathbb{Z}_{20}$, but didn't prove anything. In this document, I'll share two different approaches for proving what these ideals are.

Ideals of $\mathbb{Z}_{20}$

Like every ring, the ring $\mathbb{Z}_{20}$ has the principal ideal $\langle 0 \rangle$, which just contains the element 0, and the principal ideal $\langle 1 \rangle$, which is the whole ring. It turns out that its other ideals are just the principal ideals generated by the elements which are not units. More precisely:

Proposition. *The ring $\mathbb{Z}_{20}$ has exactly six ideals: the principal ideals $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 4 \rangle$, $\langle 5 \rangle$, and $\langle 10 \rangle$.*

The proof of this uses a lemma.

Lemma. *Let $I = \langle a \rangle$ be a principal ideal in the ring $\mathbb{Z}_n$. If $b = \gcd(a, n)$, then $I = \langle b \rangle$.*

The proof of this is a good exercise. Hint: For the proof that $\langle b \rangle \subseteq \langle a \rangle$, use a property of the gcd to show that $b \in I$.

Proof. Of the Proposition.

One can check that the given ideals are all distinct by writing down their elements and noting that they are all different sets. (For example, the ideal $\langle 4 \rangle$ is the set of five congruences classes $\{0, 4, 8, 12, 16\}$.) To prove that this list includes all the ideals of $\mathbb{Z}_{20}$, we will first show that it includes every *principal* ideal of $\mathbb{Z}_{20}$, and then show that all ideals of $\mathbb{Z}_{20}$ are principal.

Let $I = \langle a \rangle$. By the Lemma, I is generated by $b = \gcd(a, 20)$. So $I = \langle b \rangle$ for some divisor b of 20. The divisors of 20 are 1, 2, 4, 5, 10, and 20, so I must be one of the ideals in our list.

Now let's check that every ideal I of $\mathbb{Z}_{20}$ is principal. Since $\mathbb{Z}_{20}$ is a finite set, so is I, so we may write $I = \langle a_1, \ldots, a_n \rangle$ for some $a_i \in \mathbb{Z}_{20}$.[1]

Let $b_1 = \gcd(a_1, a_2)$. Then $b_1 = c_1 a_1 + c_2 a_2$ for some integers c_1 and c_2. Since I is closed under addition and under multiplication by elements of $\mathbb{Z}_{20}$, we have $b_1 \in I$. So $I = \langle b_1, a_3, \ldots, a_n \rangle$. Repeat this process to show that $I = \langle b_2, a_4, \ldots, a_n \rangle$ for $b_2 = \gcd(b_1, a_3)$, and so on. At the final step, we have $I = \langle b \rangle$ for $b = \gcd(b_{n-2}, a_n)$. So I is principal. □

As a challenge, think about how you would generalize this proof to $\mathbb{Z}_n$.

Date: March 7, 2022.

[1]If I is the set $\{a_1, \ldots, a_n\}$, then every element of I is equal to a sum of the form $\sum c_i a_i$ for some $c_i \in \mathbb{Z}_{20}$ (set all but one c_i to 0). Since I is closed under addition and absorption, all sums of the form $\sum c_i a_i$ are in I. So $I = \langle a_1, \ldots, a_n \rangle$.

A More High-Tech Proof

There is another way to describe the ideals of $\mathbb{Z}_n$ using a general theorem in ring theory called the correspondence theorem. In Hungerford's book this is Exercise 32 in Section 6.2.

Theorem. (Correspondence theorem for rings.) *Let R be a ring with identity and let I be an ideal of R. Then the ideals of R/I are exactly the ideals of the form J/I, where J is an ideal of R containing I.*

Now using the facts that

- $\mathbb{Z}_n \cong \mathbb{Z}/\langle n\rangle$,
- the ideals of $\mathbb{Z}$ are the principal ideals $\langle d\rangle$ for $d \in \mathbb{Z}$, and
- the ideals of $\mathbb{Z}$ containing $\langle n\rangle$ are the ideals $\langle d\rangle$ for $d|n$,

the correspondence theorem shows that the ideals of $\mathbb{Z}_n$ are exactly the principal ideals generated by the divisors of n.