Quotient Rings and Ideals

The difficult thing about coming up with a ring (really, the only thing) is defining the arithmetic operations, $+$ and $\cdot$, so that they satisfy all of the ring axioms. Rather than coming up with these operations out of whole cloth, if we already have some rings lying around we might try to build a new ring out of their "parts". We've already seen a few examples of exactly this idea.

- Subrings, built using subsets of existing rings
- Direct sums, built using tuples with entries from existing rings
- Localization, built out of fractions
- Polynomial rings, matrix rings, rings of functions, and more.

Another way to build new rings out of the parts of old ones is by constructing *quotients*. This idea is very frequently a stumbling block for beginning students of mathematics, so we will spend some time on it. But our effort will be rewarded; quotient rings turn out to be an extremely powerful and natural idea, and more generally the concept of "quotient" used here is pervasive in other fields of math.

Here is the basic idea behind quotient rings: given a ring R, partition R into equivalence classes as R/Φ. Now attempt to define an arithmetic on *equivalence classes* as follows:

- Given two *classes*, say X and Y in R/Φ, **choose** some representatives $x \in X$ and $y \in Y$. Now compute the sum $x + y$ in R. This element is in some other class Z in R/Φ. We define Z to be the sum of X and Y.
- Likewise, to multiply classes, we **choose** representatives, multiply in R, and determine the class of the product.

This is a fine idea, but unfortunately it has a problem: the sum of two classes may depend on our **choice** of representatives. See Figure 1 for a graphic example. As a more concrete example, consider that the set of integers can be partitioned into two sets; the primes P and the nonprimes N. We might try to compute the sum $P + P$ using representatives 2 and 3; in this case

$$P + P = [2] + [3] = [2 + 3] = [5] = P.$$

But if we use representatives 3 and 7, we have

$$P + P = [3] + [7] = [3 + 7] = [10] = N.$$

This is a problem- it means that this $+$ operation is not well-defined.

To fix this problem, we just need to make sure our partition is chosen so that this bad thing never happens.

Definition 1 (Ring Congruence)**.** *Let R be a ring. An equivalence relation Φ on R is called a* congruence *if the following hold.*

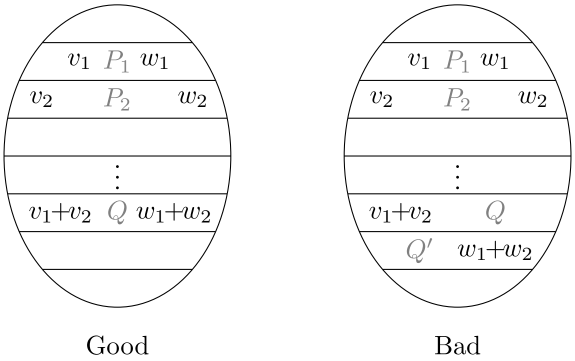

Figure 1: What can go wrong when making partitions into rings

1. *If $x_1 \Phi y_1$ and $x_2 \Phi y_2$, then $(x_1 + x_2)\Phi(y_1 + y_2)$.*
2. *If $x_1 \Phi y_1$ and $x_2 \Phi y_2$, then $(x_1 \cdot x_2)\Phi(y_1 \cdot y_2)$.*

Proposition 1. *If Φ is a congruence on a ring R and $x\Phi y$ then $(-x)\Phi(-y)$.*

Proof. We have $x\Phi y$, $(-x)\Phi(-x)$, and $(-y)\Phi(-y)$. So $(x - x - y)\Phi(y - x - y)$, and thus $(-y)\Phi(-x)$, so that $(-x)\Phi(-y)$. □

Proposition 2. *Let R be a ring and Φ an equivalence on R.*

1. *The operations $+$ and $\cdot$ on R/Φ given by*

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [a \cdot b]$$

   are well-defined if and only if Φ is a congruence.

2. *In this case, $(R/\Phi, +, \cdot)$ is a ring, called the* quotient *of R by Φ. If R is commutative, then R/Φ is commutative, and if R is unital, the R/Φ is unital.*

Proof. (type this) □

The congruence condition may at first glance seem to be very strong – so strong that we might doubt whether any such equivalences exist. We will see that they are abundant. In fact, we already know of one very important example: $\mathbb{Z}/(n)$ is the quotient of $\mathbb{Z}$ by the congruence $r\Phi s \Leftrightarrow n|(s - r)$. More generally,

Proposition 3. *Let R be a commutative ring and $a \in R$. The relation Φ on R given by $r\Phi s$ iff $a|(s - r)$ is a congruence. We denote the ring R/Φ by $R/(a)$.*

Proof. (exercise.) □

As an example, what can we say about the ring $\mathbb{Q}[x]/(x^2 + 1)$? Using the division algorithm, every polynomial in $\mathbb{Q}[x]$ can be written as $(x^2+1)q(x)+r(x)$, where r is either 0, a nonzero constant, or a linear polynomial. Etc. etc.

What are congruences?

We've seen that special equivalence relations called *congruences* can be used to build new rings out of old ones via the quotient construction. We'd like to understand the congruences in more depth.

Proposition 4. *Let R be a ring and Φ a congruence on R. Let I be the Φ-class of 0.*

1. *I is a subring of R.*
2. *I absorbs R under multiplication from either side. That is, if $a \in I$ and $r \in R$, then $ar \in I$ and $ra \in I$.*
3. *Every Φ-class is of the form $r + I = \{r + a \mid a \in I\}$ for some $r \in R$. Sets of this form are called* cosets*.*

Definition 2 (Ideal)**.** *Let R be a ring. A subring $I \subseteq R$ which absorbs R under multiplication from both sides is called an* ideal*.*

Proposition 5. *Let R be a ring and Φ an equivalence on R. Then the following are equivalent.*

1. *Φ is a congruence.*
2. *There is an ideal $I \subseteq R$ such that the Φ-classes are precisely the cosets of I.*
3. *There is a surjective ring homomorphism $\varphi : R \to S$ such that $x\Phi y$ if and only if $y - x \in \mathsf{ker}(\varphi)$.*

Proof. (type this) □

That is, the congruences on a ring are in bijective correspondence with special subsets called *ideals*. It is much easier to directly describe ideals in a ring than congruences (although the two are equivalent). For this reason, if Φ is a congruence with associated ideal I, we will frequently abuse the notation and refer to the quotient ring R/I rather than R/Φ, with the understanding that R/I is the quotient with respect to the congruence $y - x \in I$.

The First Isomorphism Theorem

Defining a mapping on a quotient set is generally difficult, for the same reason that defining operations on a quotient set is difficult; the most natural thing to try is to define our mapping in terms of representatives, but this is generally not well-defined.

The first important result about quotient rings gives us a standard way to construct homomorphisms on a quotient ring that bypasses this difficulty. This result, known as the First Isomorphism Theorem, is due to Emmy Noether, and is an important tool in ring theory.

Proposition 6 (First Isomorphism Theorem for Rings)**.** *Let R be a ring and I an ideal of R.*

1. *The natural projection $\pi : R \to R/I$ given by $\pi(x) = x + I$ is a ring homomorphism, which is unital if R is unital.*

2. *If $\varphi : R \to S$ is a ring homomorphism such that $I \subseteq \mathsf{ker}(\varphi)$, then there is a ring homomorphism $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi}(x + I) = \varphi(x)$. That is, $\varphi = \overline{\varphi} \circ \pi$.*

Another way to state FIT is as follows: If φ is a ring homomorphism and I an ideal contained in the kernel of φ, then φ factors through the projection induced by I. This terminology is inspired by the commutative diagram associated to FIT, in which we literally have $\varphi = \overline{\varphi} \circ \pi$.

Exercises

1. (One-sided ideals)