Rings, divisors and ideals

Rings

A ring is a set R with binary operations of addition ($+$) and multiplication ($\cdot$) satisfying the following properties:

- addition and multiplication are associative.

$$a + (b + c) = (a + b) + c \text{ and } a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- addition is commutative: $a + b = b + a$.
- multiplication distributes over addition.

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and } (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

- we have an additive identity 0 and a multiplicative identity 1.

$$a + 0 = a = 0 + a \text{ and } 1 \cdot a = a = a \cdot 1$$

- each element a has an additive inverse $-a$.

$$a + (-a) = 0 = (-a) + a$$

In other words, it is just like our usual number system (except that we do not require multiplication to be commutative). Hence, we can and will use the usual bracketing and grouping rules to write expressions involving elements of a ring.

Examples: Keep the following basic examples in mind at all times! We will learn more complicated examples as the course progresses.

1. The ring $\mathbb{Z}$ of all integers with the usual operations.
2. The ring $\{0\}$ which consists of just one element 0 with $0 + 0 = 0$ and $0 \cdot 0 = 0$.
3. For each integer n, the ring $\mathbb{Z}/n$ which consists of the set of numbers $\{0, 1, \ldots, n - 1\}$. The addition operation is defined by usual integer addition followed by taking the remainder after division by n. Similarly, multiplication is defined by usual integer multiplication followed by taking the remainder after division by n. The usual 0 and 1 are the additive and multiplicative identities. The additive inverse of an element a is given by $n - a$.

4. The usual sets $\mathbb{Q}$ of rational numbers, $\mathbb{R}$ of real numbers, $\mathbb{C}$ of complex numbers are also rings with the usual operations of addition and multiplication.

Exercise: Check that the axioms of a ring are satisfied by $\mathbb{Z}/n$. (Hint: One can always take remainder "at the end.")

Note that the example $\mathbb{Z}/n$ can be visualised like a clock with n hours. This is why the name "ring" has been chosen for this concept in mathematics.

Exercise: In a ring, check that $a.0 = 0 = 0.a$ for any element a of the ring.

Ideals

A fundamental property of integers that we have learned in school is "division." Given an integer a and a positive integer b, we can find unique integers $q = a//b$ and $r = a\%b$ so that (here the symbol after the equality is the computer operation that can be used to calculate the value in Sage):

$$a = b \cdot q + r \text{ and } 0 \leq r < b$$

In fact, this r is the remainder that we used in the definition of $\mathbb{Z}/n$with b replaced by n.

We can also allow b to be negative (but *not* 0). In this case we replace the above requirement for r with $0 \leq r < |b|$.

We say that a is "divisible" by b when $r = 0$ and we also write this as $b|a$ or say b divides a. We also say that b is a divisor of a when b is positive.

Since we can write $a = 1 \cdot a + 0$, every number has 1 as a divisor. Given two numbers a and b, we can look for the *greatest* common divisor (since 1 is clearly a common divisor). One of the algorithms we learned in school is the "Division algorithm" which allows us to calculate this. It goes as follows (given as a Python program):

```
def gcd(a,b):
    a, b = abs(a), abs(b)
    if b > a:
        a, b = b, a
    while b != 0:
        a, b = b, a%b
    return a
```

Exercise: Check that this program actually calculates the greatest common divisor of a and b. (Hint: We only need to check that the greatest common divisor is *invariant* under the above substitutions.)

Given three numbers a, b and c, we can calculate $gcd(gcd(a, b), c)$.

Exercise: Check that this calculation does give the greatest common divisor of a, b and c.

More generally, given a finite collection of integers $a_1, a_2, \ldots, a_k$, We can inductively calculate the greatest common divisor by applying the above `gcd` function pairwise repeatedly.

Even *if* we have an infinite collection of integers, we can see that the greatest common divisor can be calculated this way since the value *keeps decreasing* and is non-negative. Hence, it must stop after a finite stage.

In summary, given a set $S \subset \mathbb{Z}$ of integers, we can find the greatest non-negative integer d for which every element of S is a multiple of S. (The only case when $d = 0$ is when $S = \{0\}$!) This means that $S \subset d\mathbb{Z}$ and moreover, this is the largest integer for which this is true.

Exercise: If the greatest common divisor of S is d then d (and any multiple of d can be written as a *finite* additive combination of multiples of elements of S.

The non-negative integers form the collection of divisors for integers. We can think of a divisor d as something for which we can say `an integer $a$ is a multiple of $d$" or`a is divisible by d.”

Divisors have the following properties. Given two divisors, we can multiply them to get a new divisor; if a is a multiple of d_1 and b is a multiple of d_2 then $a \cdot b$ is a multiple of $d_1 \cdot d_2$. Given two divisors, we can form the greatest common divisor; it divides any element which is divisible by both of them.

Can we make sense of divisors in a general ring? The division algorithm is something special for integers. Even more so, it may not always be possible to identify a *single* element of a ring that is the greatest common divisor of two elements of the ring.

Example: Consider the set R of real numbers of the form $a + b\sqrt{5}$ where a and b are *integers* with the usual operations of addition and multiplication of real numbers.

Exercise: Check that R as defined above is a ring.

Now we have $(-1 + \sqrt{5}) \cdot (1 + \sqrt{5}) = 4 = 2 \cdot 2$. It follows quite easily that there is no element other than ± 1 that divides *both* $1 + \sqrt{5}$ and 2. On the other hand, we see that $(1 + \sqrt{5}) \cdot a + 2 \cdot b = 1$ has no solution with a and b in R.

This says that we should *not* think of 1 as the greatest common divisor of $1 + \sqrt{5}$ and 2 as it is not an additive combination of multiples of these two numbers. The only solution is to think of an `idealised" divisor which divides all such additive combinations. This led Dedekind and Kronecker to introduce the concept of an`ideal divisor’‘which we have now shorted to the name “ideal”.

An *ideal* of R is a subset I of R which is closed under addition and (left or right) multiplication by elements of R. (If it is only closed under left multiplication by elements of R, it is called a left ideal; similarly, we have right ideals.)

For any non-negative integer d, the multiples of d form the ideal $d\mathbb{Z}$ of $\mathbb{Z}$.

Given ideals I and J, we can create the set $I \cdot J$ that consists of additive combinations of elements of the form $a \cdot b$ for a in I and b in J. Similarly, we can create the set $I + J$ consisting of elements of the form $a + b$ for a in I and b in J.

Exercise: Show that $(m\mathbb{Z}) \cdot (n\mathbb{Z}) = (mn) \cdot \mathbb{Z}$ and $(m\mathbb{Z}) + (n\mathbb{Z}) = \gcd(m, n)\mathbb{Z}$.

Exercise: More generally, for any ring R and ideals I and J in R, show that $I \cdot J$ and $I + J$ are ideals in R.

Thus ideals have properties similar to those of divisors. Note that $I + J$ is to be thought of as similar to the greatest common divisor of the divisors associated with I and J.

Homomorphisms

The word `homomorphism" is meant to be a combination of`homo’‘, meaning similar, “morphism” meaning transformation; a transformation between similar things.

Given a ring R, we can define a set map $r : \mathbb{Z} \to R$ by defining the image of 0 as 0 (in R), the image of a positive integer n is the sum of n copies of 1 (in R), the image of a negative integer $-n$ is the sum of n copies of -1 (in R).

Exercise: The above map r has the property that $r(m + n) = r(m) + r(n)$ and $r(m \cdot n) = r(m) \cdot r(n)$.

A set $f : R \to S$, where R and S are rings is called a *homomorphism* of rings if $f(a + b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$.

For example, we can examine the homomorphism $r : \mathbb{Z} \to \mathbb{Z}/n$. The collection of all elements that go to 0 under r are precisely the elements of $n\mathbb{Z}$, an ideal.

Exercise: More generally, if $f : R \to S$ is a homomorphism of rings then define the set I to consist of elements a such that $f(a) = 0$. Check that I is an ideal.

The set of such elements is called the *kernel* of the homomorphism f and denoted as $\ker(f)$.

Conversely, suppose I in an ideal in R. Given a in R, we define $a + I$ as the subset of R that consists of elements of the form $a + b$ where b is in I.

The power set $P(R)$ consists of subsets of R. We define the set R/I as the subset of $P(R)$ that consists of the subsets of the form $a + I$ of R where a is an element of R.

Exercise: What are the elements a and a' of R such that $a + I = a' + I$?

Given subsets A and B of R, we can define $A \oplus B$ to be the subset of R that consists of elements of the form $a + b$ with a in A and b in B. We also define $A \odot B$ to be the subset of R that consists of elements of the form $a \cdot b$ with a in A and b in B.

Exercise: Check that R/I with the operations $\oplus$ and $\odot$ as addition and multiplication forms a ring with $0 + I$ and $1 + I$ as additive and multiplicative identity respectively.

Note that from one point of view an element of R/I is a subset of R. However, beyond the initial calculations below it is convenient *not* to think of it in these terms; just as we do not think of 42 as 1 added to 0 42 times, or as the size of the set of elements $\{0, \ldots, 41\}$. Like in Sage we can use mathematical objects without thinking of how they are stored, it is useful to learn how to use mathematical concepts without worrying about a particular way of constructing them.

There is a natural map $i : R \to R/I$ which sends a to the element $a + I$. The kernel of i consists precisely of I. Thus, given an ideal, we have a homomorphism which has *that* ideal as its kernel.

This gives us another way to approach ideals: as kernels of homomorphisms to other rings.

Conclusion

In this section we have seen only a few examples of rings, ideals and homomorphisms. However, we have given general definitions and properties. When we study other examples later during the course, we will see how these definitions and properties have wider applicability.
