The Multiplicative Arithmetic of Ideals

R. C. Daileda

1 Introduction

Definition 1. Let R be a ring and $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals.[1] The *sum* and *product* of $\mathfrak{a}$ and $\mathfrak{b}$ are the ideals[2]

$$\mathfrak{a}+\mathfrak{b} = (\mathfrak{a} \cup \mathfrak{b}),$$
$$\mathfrak{a}\mathfrak{b} = (\mathfrak{a} \cdot \mathfrak{b}).$$

We can easily describe the elements in both $\mathfrak{a}+\mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$ in terms of the elements of $\mathfrak{a}$ and $\mathfrak{b}$.

Lemma 1. *Let R be a ring with ideals $\mathfrak{a}$ and $\mathfrak{b}$. Then*

$$\mathfrak{a}+\mathfrak{b} = \{a+b \,|\, a \in \mathfrak{a}, b \in \mathfrak{b}\},$$
$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N} \right\}.$$

Proof. Let $I = \{a+b \,|\, a \in \mathfrak{a}, b \in \mathfrak{b}\}$. Since $\mathfrak{a} \subset (\mathfrak{a} \cup \mathfrak{b})$, $\mathfrak{b} \subset (\mathfrak{a} \cup \mathfrak{b})$ and $(\mathfrak{a} \cup \mathfrak{b})$ is closed under addition, $a+b \in (\mathfrak{a} \cup \mathfrak{b})$ for all $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Thus $I \subset (\mathfrak{a} \cup \mathfrak{b})$. On the other hand, I is an ideal (exercise) containing both $\mathfrak{a}$ and $\mathfrak{b}$ (since 0 belongs to both ideals). Therefore $(\mathfrak{a} \cup \mathfrak{b}) \subset I$ as well.

Let $J = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$.[3] Then $0 \in J$ and if $x = \sum_i a_i b_i$ and $y = \sum_j a'_j b'_j$, then

$$x - y = \sum_i a_i b_i - \sum_j a'_j b'_j = \sum_i a_i b_i + \sum_j (-a'_j) b'_j \in J,$$

since $-a'_j \in \mathfrak{a}$ for all j. If $r \in R$, then

$$rx = \sum_i (r a_i) b_i \in J$$

since $r a_i \in \mathfrak{a}$ for all i. It follows that J is an ideal containing $\mathfrak{a} \cdot \mathfrak{b}$. Thus $(\mathfrak{a} \cdot \mathfrak{b}) \subset J$. In the other direction, any ideal containing $\mathfrak{a} \cdot \mathfrak{b}$ must necessarily contain all finite sums of elements in $\mathfrak{a} \cdot \mathfrak{b}$, as ideals are closed under addition. That is, any ideal containing $\mathfrak{a} \cdot \mathfrak{b}$ must contain J. This immediately implies that $J \subset (\mathfrak{a} \cdot \mathfrak{b})$, completing the proof.

□

Because $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, the elements of $\mathfrak{a} \cdot \mathfrak{b}$ all belong to both $\mathfrak{a}$ and $\mathfrak{b}$. Thus, $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$, which implies

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}.$$

[1] The lower case *Fraktur* alphabet ($\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$) is traditionally used to typeset the names of ideals. As ideals can be thought of as generalized, or "ideal," ring elements, it's natural to give them lower case names, as we typically do with the elements themselves. However, to avoid confusion between elements and ideals, different alphabets are required for each. The use of the gothic Fraktur alphabet for ideals is long-established. In class I've opted to simply use the capital letters in the Roman alphabet instead, only because they are easier to write on the board.

[2] Here and elsewhere we will denote the element-wise product of subsets of R with $\cdot$ in order to avoid confusion with the ideal product.

[3] From now on, the notation $\sum_i$ will indicate a sum indexed by an arbitrary finite set.

In general this containment is proper. We will give sufficient conditions for equality later. If R is commutative and $S \subset R$, then the elements of (S) are the finite R-linear combinations of elements of S. Suppose $T \subset R$ as well. Then for any $x \in (S)$ and $y \in (T)$ we have

$$x = \sum_i r_i s_i \ \ (r_i \in R, s_i \in S),$$
$$y = \sum_j r'_j t_j \ \ (r'_j \in R, t_j \in T),$$

so that

$$xy = \sum_{i,j} r_i r'_j s_i t_j \in (S \cdot T).$$

Since the elements xy generate $(S)(T)$, we find that $(S)(T) \subset (S \cdot T)$. But $S \cdot T \subset (S)(T)$, so we also have $(S \cdot T) \subset (S)(T)$. We conclude that

$$(S)(T) = (ST).$$

This implies that if R is commutative and $\mathfrak{a}$, $\mathfrak{b}$ are finitely generated, then so is $\mathfrak{ab}$. In particular, for principal ideals we have

$$(a)(b) = (ab) \quad \text{when } R \text{ is commutative.}$$

Ideal arithmetic enjoys almost all of the features of ordinary arithmetic. For example, let's prove that if $\mathfrak{a}, \mathfrak{b}$ and C are ideals in R, then

$$\mathfrak{a}(\mathfrak{b} + C) = \mathfrak{ab} + \mathfrak{a}C.$$

If $x \in \mathfrak{a}(\mathfrak{b} + C)$, then there are $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $c_i \in C$ so that

$$x = \sum_i a_i(b_i + c_i) = \sum_i a_i b_i + \sum_i a_i c_i \in \mathfrak{ab} + \mathfrak{a}C.$$

Hence $\mathfrak{a}(\mathfrak{b} + C) \subset \mathfrak{ab} + \mathfrak{a}C$. To establish the opposite inclusion, it is enough to show that $\mathfrak{ab} \subset \mathfrak{a}(\mathfrak{b} + C)$, since then $\mathfrak{a}C \subset \mathfrak{a}(C + \mathfrak{b}) = \mathfrak{a}(\mathfrak{b} + C)$ and

$$\mathfrak{ab} + \mathfrak{a}C = (\mathfrak{ab} \cup \mathfrak{a}C) \subset \mathfrak{a}(\mathfrak{b} + C).$$

Let $x = \sum_i a_i b_i \in \mathfrak{ab}$, with $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Then $x = \sum_i a_i(b_i + 0) \in \mathfrak{a}(\mathfrak{b} + C)$, proving that $\mathfrak{ab} \subset \mathfrak{a}(\mathfrak{b} + C)$, as needed. The remaining arithmetic properties of ideals are stated in the next result. We leave their proofs as exercises.

Theorem 1. *Let R be a ring. Ideal addition in R is commutative and associative, with identity (0). Ideal multiplication in R is associative, and has identity R. Multiplication of ideals distributes over addition, on both the left and the right. Multiplication of ideals is commutative provided R is commutative.*

Remark 1. The converse of the final statement in the theorem is false. It is possible for a noncommutative ring to have commutative ideal multiplication. For example, take $R = \mathrm{M}_n(F)$ for any field F and any $n \geq 2$. In this case the only ideals are R and (0), which certainly commute.

Remark 2. No nontrivial ideal $\mathfrak{a}$ has an additive inverse, since $(0) \subsetneq \mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}$ implies $\mathfrak{a} + \mathfrak{b} \neq (0)$ for any ideal $\mathfrak{b}$.

Remark 3. No proper ideal $\mathfrak{a}$ has a multiplicative inverse, since $\mathfrak{ab} \subset \mathfrak{a} \subsetneq R$ implies $\mathfrak{ab} \neq R$ for any ideal $\mathfrak{b}$.

2 Divisibility of Ideals

Let's take a look at ideal arithmetic in $\mathbb{Z}$. Given $m, n \in \mathbb{Z}$, one has

$$m\mathbb{Z} \subset n\mathbb{Z} \ \Leftrightarrow \ m \in n\mathbb{Z} \ \Leftrightarrow \ m = nk \ \Leftrightarrow \ n \text{ divides } m.$$

Moreover, according to Bézout's lemma (or otherwise),

$$m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}.$$

This says that the ideal in $\mathbb{Z}$ generated by m and n is the same as the ideal generated by their greatest common divisor, or

$$(m, n) = (\gcd(m, n)).$$

As such, it is not uncommon to simply write (m, n) for $\gcd(m, n)$. Whether (m, n) denotes a single integer or an ideal is usually clear from context, but the distinction is often irrelevant. Finally, since $m\mathbb{Z} \cap n\mathbb{Z}$ consists of the common multiples of m and n, we find that

$$m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{lcm}(m, n)\mathbb{Z}.$$

The following definitions generalize these observations to an arbitrary ring.

Definition 2. Let R be a ring, $\mathfrak{a}, \mathfrak{b} \subset R$ ideals. We say that $\mathfrak{a}$ *divides* $\mathfrak{b}$ if $\mathfrak{b} \subset \mathfrak{a}$.

Remark 4. In the context of ideals, "divides" is simply a synonym for "contains,"[4] and we will continue to use the latter term on occasion.

Definition 3. Let R be a ring, $\mathfrak{a}, \mathfrak{b} \subset R$ ideals. The *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal $\mathfrak{a} + \mathfrak{b}$. The *least common multiple* of $\mathfrak{a}$ and $\mathfrak{b}$ is $\mathfrak{a} \cap \mathfrak{b}$.

Remark 5. Definition 2 is consistent not only with arithmetic in $\mathbb{Z}$, but also with the behavior of principal ideals in any commutative ring R. If $a, b \in R$ then $aR \subset bR$ if and only if $a \in bR$, which is equivalent to $a = bc$ for some $c \in R$. That is, c divides a in R.

Remark 6. Let $\mathfrak{a} \subset \mathfrak{b}$ be ideals in R. Does $\mathfrak{b}$ divide $\mathfrak{a}$ in the traditional sense? That is, is there an ideal $\mathfrak{c}$ dividing $\mathfrak{a}$ so that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$? Any $c \in \mathfrak{c}$ would have to have the property that $bc \in \mathfrak{a}$ for every $b \in \mathfrak{b}$. Thus, the only candidate is

$$\mathfrak{c} = \{r \in R \,|\, \mathfrak{b}r \subset \mathfrak{a}\}.$$

One can readily show that $\mathfrak{c}$ is an ideal dividing $\mathfrak{a}$ and

$$\mathfrak{b}\mathfrak{c} \subset \mathfrak{a} \subset \mathfrak{b} \cap \mathfrak{c}.$$

This shows that $\mathfrak{a}$ is somewhere between the product and the LCM of $\mathfrak{b}$ and $\mathfrak{c}$, and this is the most we can expect, in general. Actually obtaining $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ or $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ is another matter entirely.

Given $m, n \in \mathbb{Z}$, one has the lovely relationship

$$mn = \gcd(m, n) \operatorname{lcm}(m, n).$$

The following result gives the ideal analogue.

Lemma 2. *Let R be a ring. For any ideals $\mathfrak{a}$ and $\mathfrak{b}$, one has*

$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b} + \mathfrak{b}\mathfrak{a}.$$

Proof.

$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b})\mathfrak{a} + (\mathfrak{a} \cap \mathfrak{b})\mathfrak{b} \subset \mathfrak{b}\mathfrak{a} + \mathfrak{a}\mathfrak{b}.$$

□

Definition 4. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a ring R are called *relatively prime* or *coprime* if $\mathfrak{a} + \mathfrak{b} = R$.

Remark 7. This agrees with our previous conventions. Two ideals should be relatively prime if their GCD is trivial, namely equal to R.

[4] As my Ph. D. adviser Bill Duke used to say, "To contain is to divide."

The following are immediate consequences of Lemma 2.

Corollary 1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals in a ring R, then*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b} + \mathfrak{b}\mathfrak{a}.$$

Corollary 2. *If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals in a commutative ring R, then*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

Remark 8. Note that this final corollary states that for relatively prime ideals, the product and the LCM coincide, as in $\mathbb{Z}$.

3 The Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) provides an explicit connection between a product of quotients of a ring R and a quotient of R by a product of coprime ideals. The classical number-theoretic CRT is obtained by taking $R = \mathbb{Z}$.

Theorem 2 (Chinese Remainder Theorem)**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals in a ring R. Then there is a well-defined isomorphism*

$$R/(\mathfrak{a} \cap \mathfrak{b}) \to R/\mathfrak{a} \times R/\mathfrak{b}$$

given by $r + (\mathfrak{a} \cap \mathfrak{b}) \mapsto (r + \mathfrak{a}, r + \mathfrak{b})$.

Proof. The canonical surjections $\pi_\mathfrak{a} : R \to R/\mathfrak{a}$ and $\pi_\mathfrak{b} : R \to R/\mathfrak{b}$ together yield a map $\pi_\mathfrak{a} \times \pi_\mathfrak{b} : R \to R/\mathfrak{a} \times R/\mathfrak{b}$ defined by

$$(\pi_\mathfrak{a} \times \pi_\mathfrak{b})(r) = (\pi_\mathfrak{a}(r), \pi_\mathfrak{b}(r)) = (r + \mathfrak{a}, r + \mathfrak{b}).$$

We clearly have

$$\ker(\pi_\mathfrak{a} \times \pi_\mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}.$$

According to the next lemma, $\pi_\mathfrak{a} \times \pi_\mathfrak{b}$ is surjective, so a straightforward application of the first isomorphism theorem completes our proof. □

Lemma 3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in a ring R. Then $\varphi = \pi_\mathfrak{a} \times \pi_\mathfrak{b}$ is surjective if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.*

Proof. We leave it to the reader to verify that φ is surjective if and only if $(\mathfrak{a}, 1+\mathfrak{b}), (1+\mathfrak{a}, \mathfrak{b}) \in \operatorname{im}\varphi$. We will prove that the latter condition is equivalent to $\mathfrak{a}+\mathfrak{b} = R$. First suppose that $x, y \in R$ satisfy $\varphi(x) = (\mathfrak{a}, 1+\mathfrak{b})$ and $\varphi(y) = (1 + \mathfrak{a}, \mathfrak{b})$. By the definition of φ, this means $x \in \mathfrak{a}$, $1 - x \in \mathfrak{b}$. But then $1 = x + (1 - x) \in \mathfrak{a} + \mathfrak{b}$, which implies $\mathfrak{a} + \mathfrak{b} = R$.

Conversely, assume $\mathfrak{a} + \mathfrak{b} = R$. Write $1 = a + b$ with $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Then

$$\varphi(b) = (b + \mathfrak{a}, b + \mathfrak{b}) = (1 - a + \mathfrak{a}, \mathfrak{b}) = (1 + \mathfrak{a}, \mathfrak{b}).$$

Likewise, $\varphi(a) = (\mathfrak{a}, 1 + \mathfrak{b})$. Hence $(\mathfrak{a}, 1 + \mathfrak{b}), (1 + \mathfrak{a}, \mathfrak{b}) \in \operatorname{im}\varphi$.

□

If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime and R is commutative, we have seen that $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$. This yields the following version of the CRT for commutative rings.

Corollary 3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals in a commutative ring R. Then the map $R/\mathfrak{a}\mathfrak{b} \to R/\mathfrak{a} \times R/\mathfrak{b}$ given by $r + \mathfrak{a}\mathfrak{b} \mapsto (r + \mathfrak{a}, r + \mathfrak{b})$ is a well-defined isomorphism of rings.*

4 Appendix: Measuring Ideals

The terminology "$\mathfrak{b}$ divides $\mathfrak{a}$" for the arrangement $\mathfrak{a} \subset \mathfrak{b}$ seems somewhat arbitrary, perhaps even counterintuitive. After all, both "divides" (in the traditional sense) and "contains" are just partial orderings, so why change terminology? And we're used to thinking of divisors as being smaller than what they divide, and doesn't $\mathfrak{a} \subset \mathfrak{b}$ indicate that $\mathfrak{b}$ is somehow bigger than $\mathfrak{a}$? It contains $\mathfrak{a}$, at least. So what's going on?

For one, we'd like our usage to be consistent across all rings, and we've just seen how divisibility works at the level of ideals in $\mathbb{Z}$. For another, although saying "$\mathfrak{b}$ divides $\mathfrak{a}$" does nothing more than psychologically reverse the sense of the relationship $\mathfrak{a} \subset \mathfrak{b}$, it can be argued that the reversed sense is, indeed, more appropriate. In multiplicative ideal theory, the unit ideal is R, the entire ring. As such, we'd like to treat R (not zero!) as trivial. On the other hand, (0) acts multiplicatively like infinity, and therefore ought to be regarded as the "largest" ideal. The easiest way to arrange this state of affairs is to turn the lattice of ideals in R on its head, and declare that $\mathfrak{b} < \mathfrak{a}$ if and only if $\mathfrak{a} \subset \mathfrak{b}$ for all ideals $\mathfrak{a}$ and $\mathfrak{b}$. Then $<$ will order the ideals R and (0) correctly relative to all the others. But as we have already seen in $\mathbb{Z}$, a more appropriate choice for symbolism would be $\mathfrak{b}|\mathfrak{a}$ when $\mathfrak{a} \subset \mathfrak{b}$, a relationship we choose to call "divides."

This seems reasonable for R and (0), but what about other ideals? Ideals "closer" to R in the containment sense are to be regarded as small, and those that at "almost zero" should be thought of as very large. Given an ideal $\mathfrak{a} \subset R$, the most natural way to measure how much or how little of R the ideal "takes up" is through the quotient ring $R/\mathfrak{a}$. Because the cosets of $\mathfrak{a}$ cover R and can each be bijected with $\mathfrak{a}$, the size of $R/\mathfrak{a}$ tells us how many copies of $\mathfrak{a}$ it takes to cover R. Smaller $R/\mathfrak{a}$ means fewer cosets, which intuitively means that there is "more" of $\mathfrak{a}$, i.e. $\mathfrak{a}$ and R are "close" ideals $\mathfrak{a}$ is "small." Conversely, when $R/\mathfrak{a}$ is large, it takes a lot of $\mathfrak{a}$s to get all of R, so $\mathfrak{a}$ is intuitively near zero, and therefore "big."

Given an ideal $\mathfrak{a}$ in R, we will call the ring $i(\mathfrak{a}) = R/\mathfrak{a}$ the *index* of $\mathfrak{a}$ in R. The *norm* of $\mathfrak{a}$ will be the size (or cardinality) of $R/\mathfrak{a}$:

$$N(\mathfrak{a}) = |R/\mathfrak{a}|.$$

While the norm certainly does the job of the preceding paragraph, by measuring $R/\mathfrak{a}$ in a consistent way, the index contains a good deal of additional information about $\mathfrak{a}$, so it's worth hanging on to. For example, given a prime p, the nonisomorphic indices $R/\mathfrak{a} \cong \mathbb{Z}/p^4\mathbb{Z}$ and $R/\mathfrak{a} \cong \mathrm{M}_2(\mathbb{F}_p)$ both satisfy $N(\mathfrak{a}) = p^4$. As another example, if $N(\mathfrak{a})$ is ever infinite, the index is almost certainly more useful to look at. If $\mathfrak{b}$ is an ideal dividing $\mathfrak{a}$, the (generalized) first isomorphism theorem provides a surjective map

$$R/\mathfrak{a} \to R/\mathfrak{b},$$

whose kernel is $\mathfrak{b}/\mathfrak{a}$. We call $\mathfrak{b}/\mathfrak{a}$ the index of $\mathfrak{a}$ *relative to* $\mathfrak{b}$ and $N_{\mathfrak{b}}(\mathfrak{a}) = |\mathfrak{b}/\mathfrak{a}|$ the norm of $\mathfrak{a}$ *relative to* $\mathfrak{b}$. By the first isomorphism theorem the norms satisfy[5]

$$N(\mathfrak{a}) = N(\mathfrak{b})N_{\mathfrak{b}}(\mathfrak{a}). \tag{1}$$

Remark 9. Given ideals $\mathfrak{a}$ and $\mathfrak{b}$ in R, a *common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ is an ideal I so that $\mathfrak{a} \subset I$ and $\mathfrak{b} \subset I$. That is, I is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ if and only if $\mathfrak{a} + \mathfrak{b} \subset I$. Since in this arrangement we know that $N(\mathfrak{a} + \mathfrak{b}) \geq N(I)$, the common divisor with greatest possible norm is $I = \mathfrak{a} + \mathfrak{b}$. Hence the name *greatest common divisor.* Likewise, I is a *common multiple* of $\mathfrak{a}$ and $\mathfrak{b}$ provided $I \subset \mathfrak{a}$ and $I \subset \mathfrak{b}$, or $I \subset \mathfrak{a} \cap \mathfrak{b}$. Now we have $N(I) \geq N(\mathfrak{a} \cap \mathfrak{b})$, so that the common multiple with the least possible norm is $I = \mathfrak{a} \cap \mathfrak{b}$, justifying the name *least common multiple.*

Remark 10. In number theory, a function $f : \mathbb{N} \to \mathbb{C}$ (which is equivalent to a function on the ideals of $\mathbb{Z}$), is called *multiplicative* provided $f(ab) = f(a)f(b)$ for all coprime $a, b \in \mathbb{N}$. According to the CRT, if R is commutative and $\mathfrak{a}, \mathfrak{b}$ are coprime ideals in R, then

$$i(\mathfrak{a}\mathfrak{b}) \cong i(\mathfrak{a}) \times i(\mathfrak{b}),$$

[5] The norms we've defined are simply the usual indices $[R : \mathfrak{a}]$ and $[\mathfrak{b} : \mathfrak{a}]$ of additive subgroups. The equation (1) is just a restatement of the multiplicativity of the usual index in towers, namely $[R : \mathfrak{a}] = [R : \mathfrak{b}][\mathfrak{b} : \mathfrak{a}]$.

which in turn implies that

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

That is, both the index and the norm can be regarded as multiplicative functions of the ideals in a commutative ring.

Remark 11. Another justification for the "size reversal" of ideals comes from algebraic geometry. Let R be a commutative ring and let the *spectrum* of R be

$$\operatorname{Spec} R = \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ is a prime ideal}\}.$$

Every ideal $\mathfrak{a}$ in a commutative ring R gives rise to a certain *zero set* of $\operatorname{Spec} R$, namely the set of primes dividing $\mathfrak{a}$:

$$Z(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{a} \subset \mathfrak{p}\}.$$

Believe it or not, these collections of prime ideals are very natural generalizations of solution sets of simultaneous polynomial equations!

There is a bijective correspondence between the (radical) ideals of R and the zero sets in $\operatorname{Spec} R$. Since the latter turns out to be the true algebro-geometric object of interest, we will choose to judge ideal size based on the size of the corresponding zero set. The definition of $Z(\mathfrak{a})$ implies that if an ideal $\mathfrak{b}$ divides $\mathfrak{a}$, then $Z(\mathfrak{b}) \subset Z(\mathfrak{a})$. Hence, in this situation we should regard $\mathfrak{a}$ as the larger ideal, since it has more "zeros." So once again, to the set-theoretically "smaller" ideal we associate the "larger" object. This means the largest ideal should be (0), since $Z(0) = \operatorname{Spec} R$, while the smallest is R because $Z(R) = \varnothing$.