Ring Theory 2

Several important bits and bobs, a long section on localization

by Ivan Aidun

These are notes interspersed with exercises. The purpose of these notes is to be more fleshed out than Evan Dummit's old notes, but shorter and more focused than a textbook treatment. Halfway between Dummit and Dummit and Foote, so to speak. I hope these are helpful to you!

Conventions

In these notes, all rings will be commutative with unity. Altho some of the statements generalize (with more or less effort) to the noncommutative setting, we won't be concerned with stating/proving the most general version.

The universal property of quotient rings

Quotient rings (or groups, or modules) have a special property which not everybody sees/appreciates in their first algebra class. I'm going to spend a little space discussing htis property because of how fundamental it is.

Theorem. Let R, R' be rings, I an ideal of R, and $q\colon R \to R/I$ the quotient homomorphism. If $\phi\colon R \to R'$ is a homomorphism, and $\ker\phi \supset I$, then there is a unique map $\widetilde{\phi}\colon R/I \to R'$ such that $\phi = \widetilde{\phi} \circ q$.

Concretely, the map $\widetilde{\phi}$ sends the coset $r + I$ to $\phi(r)$. The content of the statement is mostly verifying that this is a well-defined function.

Of course, given any map $\psi\colon R/I \to R'$, we can readily obtain a map $R \to R'$ whose kernel contains I by taking the composition $\psi \circ q$. So, what this theorem is saying is that in fact, there is a bijection between the set of homomorphisms $R \to R'$ whose kernel contains I, and the set of all homomorphisms $R/I \to R'$. Here's another way of thinking about things: suppose somebody gave you a (admittedly very bizarre) puzzle or a brain teaser by giving you a specific $\phi\colon R \to R'$ satisfying $\ker\phi \supset I$, and saying "I'm thinking of a homomorphism $\psi\colon R \to R'$, and this homomorphism satisfies that $\psi \circ q = \phi$, can you figure out what ψ is?". What this theorem says is that this is a very well-designed puzzle, in the sense that there is exactly one answer, and the puzzle-maker has given you exactly the right amount of information to figure out what the answer is, no more no less.

On a practical level, I think about the importance of this theorem in the following way. As a set, the quotient ring R/I is pretty unwieldy. Manipulating cosets is not easy or intuitive, and there's an annoying indeterminacy about cosets where two seemingly different representatives might give the same coset. For example, $1 + 2\mathbb{Z} = 3 + 2\mathbb{Z}$. What the above theorem tells you is that if you want to define a homomorphism from a quotient ring R/I to some other ring R', then you can instead specify what that homomorphism should look like on elements of R, and all you have to do to make sure it descends to the quotient is verify that $\ker\widetilde{\phi} \supset I$, which is often an easy condition to check.

This theorem is perhaps best illustrated by drawing a picture containing all the homomorphisms involved. In diagram form, this theorem looks like this:

$$\begin{tikzcd} R \arrow[d, "q"'] \arrow[dr, "\phi"] & \\ R/I \arrow[r, dashed, "\widetilde{\phi}"'] & R' \end{tikzcd}$$

A restatement of the theorem is "for all homomorphisms ϕ such that $\ker \phi \supset I$, there exists a unique homomorphism $\widetilde{\phi}$ making the above diagram commute". (To say a diagram **commutes** just means that composing the homomorphisms along each directed path gives the same thing in the end, so in this diagram it says that $\phi = \widetilde{\phi} \circ q$.)

The lattice theorem: ideals in a quotient

The lattice isomorphism is often glossed over in a first course in ring theory. The third isomorphism theorem stated that we can find ideals in a quotient ring R/I by taking ideals $J \supset I$ and passing to the quotient J/I. The lattice isomorphism theorem asserts that this process in fact produces a bijection

$$\{\text{ideals of } R \text{ containing } I\} \xrightarrow{\sim} \{\text{ideals of } R/I.\}$$

It also states that this correspondence has a few further properties:

1. This correspondence preserves the subset relation: if J and J' are ideals of R containing I, then $J \subset J'$ iff then $J/I \subset J'/I$.

2. As a consequence, this correspondence preserves ideal sums and intersections: if J and J' are as above, then $(J + J')/I = (J/I) + (J'/I)$ and $(J \cap J')/I = (J/I) \cap (J'/I)$ as ideals of R/I.

3. This correspondence also preserves ideal products: if J and J' are as above, then $(J/I)(J'/I) = (JJ')/I$ as ideals of R/I.

4. As a further consequence of 1. and 3., this correspondence preserves prime and maximal ideals: if P is a prime/maximal ideal of R containing I, then P/I is a prime/maximal ideal of R/I, and all prime/maximal ideals of R/I arise in this way.

This is called the "lattice" isomorphism theorem because we can imagine the ideals of R in a lattice indicating their subset relationships. For example, (part of) the lattice of ideals in $\mathbb{Z}$ is shown in Figure 1.

The lattice isomorphism theorem says that the lattice of ideals for R/I is exactly the part of this lattice that lies above the ideal I. So, for example, the lattice for $\mathbb{Z}/6\mathbb{Z}$ is shown in Figure 2, deliberately illustrated to highlight the similarity in structure to the ideals of $\mathbb{Z}$ above the ideal (6). Furthermore, the lattice theorem says this correspondence also descends prime and maximal ideals, so for example the prime ideals of $\mathbb{Z}/6\mathbb{Z}$ are the ideals (2) and (3), because these descend from prime ideals of $\mathbb{Z}$.

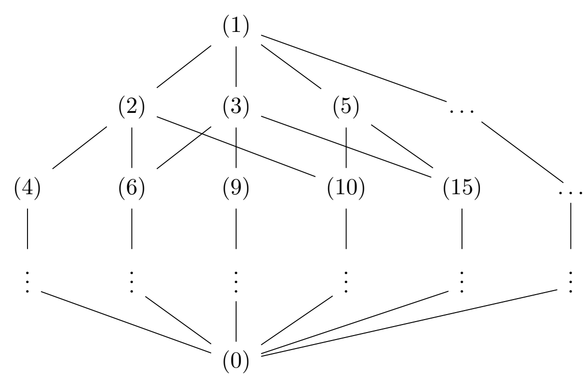

Figure 1: The lattice of ideals in $\mathbb{Z}$

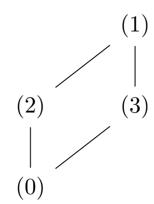

Figure 2: The lattice of ideals in $\mathbb{Z}/6\mathbb{Z}$

Exercise 1. (January 2020 Problem 3(b), August 2023 Problem 1 (d)) Give an example of a ring with finitely many elements that has exactly three prime ideals. (In 2023, the problem didn't specify "with finitely many elements". Can you find an example with infinitely many elements?)

The Chinese Remainder Theorem

Background on solving congruences

The Chinese Remainder Theorem (CRT) is one of my favorite theorems. The name comes because of computations appearing in an ancient Chinese mathematical treatise, the *Sunzi Suanjing*. Eric Bach, here at UW, often calls it "Sunzi's theorem" as a way of crediting the original author, rather than just having a name attributed to his nationality.

The original scope of the CRT is solving systems of congruence relations. For example, consider the system

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 7. \end{aligned}$$

Are there any integers x which satisfy these relations? The answer in this case is yes, for example, $x = 11$ works, as does $x = 53$ and $x = 95$. However, consider the system

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{8}. \end{aligned}$$

Now the answer is no, because if $x \equiv 1 \pmod{2}$, then x must be odd, but if $x \equiv 4 \pmod{8}$ then x must be even. What differs between the two examples is that the integers $\{2, 3, 7\}$ are "multiplicatively independent" of one another, by virtue of being pairwise coprime, whereas the integers $\{2, 3, 8\}$ are not.

Theorem (CRT, congruence form)**.** A system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \quad \vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

where the m_i are pairwise coprime always has an integer solution. Moreover, the set of solutions forms a residue class modulo $M = \prod_i m_i$.

More generally, if the m_i are not pairwise coprime, then a solution exists iff for all pairs i, j we have that $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$. In this case, the set of solutions forms a residue class modulo $M = \operatorname{lcm}\{m_i\}_i$

A more modern presentation

The statement of the CRT given above is actually a bit difficult to prove by purely elementary means, and also it would be a weird thing to include in these notes if there wasn't a way it applied to ring theory more generally. The modern way to interpret it is to consider the ring homomorphism $\mathbb{Z} \to \prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}$ which sends an element $a \in \mathbb{Z}$ to the tuple of its reductions modulo each m_i: $(a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_n)$. The first statement of the CRT above asserts that this map is surjective, and that its kernel is exactly the ideal $M\mathbb{Z}$, so by the first isomorphism theorem we get an isomorphism of rings $\mathbb{Z}/M\mathbb{Z} \cong \prod_i \mathbb{Z}/m_i\mathbb{Z}$.

In the more general setting where the m_i need not be coprime, for every pair i, j we get a *group* homomorphism $\mathbb{Z}/m_i\mathbb{Z} \times \mathbb{Z}/m_j\mathbb{Z} \to \mathbb{Z}/\gcd(m_i, m_j)\mathbb{Z}$ which takes the pair $(a \bmod m_i, b \bmod m_j)$ to $a - b \bmod \gcd(m_i, m_j)$. (This is not a ring homomorphism because the multiplicative identity in $\mathbb{Z}/m_i\mathbb{Z} \times \mathbb{Z}/m_j\mathbb{Z}$ is $(1, 1)$, which gets sent to 0.) The second statement above is equivalent to saying that a tuple $(a_1 \bmod m_1, \ldots, a_n \bmod m_n)$ is in the image of the map $\mathbb{Z}/M\mathbb{Z} \to \prod_i \mathbb{Z}/m_i\mathbb{Z}$ exactly when it is in the kernel of *all* of these $\binom{n}{2}$ difference-mod-gcd maps.

Rephrasing the statement in these terms both makes it easier to prove, and also makes it easier to generalize. In the first set of notes, we saw analogs for all of the above statements in terms of ideals in an arbitrary ring: gcd corresponds to ideal sum, lcm corresponds to ideal intersection. We are therefore able to state a version of the CRT valid for an arbitrary ring.

Theorem (CRT, general ring version)**.** Let R be a ring and $I_1, \ldots, I_n$ be ideals. The ring homomorphism

$$\begin{aligned} R &\xrightarrow{\pi} \prod_{i=1}^{n} R/I_i \\ r &\mapsto (r \bmod I_1, \ldots, r \bmod I_n) \end{aligned}$$

has kernel $\bigcap_{i=1}^n I_i$, so by first isomorphism theorem we get an injective ring homomorphism

$$\frac{R}{\bigcap_i I_i} \xrightarrow{\widetilde{\pi}} \prod_i R/I_i.$$

Furthermore, we have a group homomorphism (but not ring homomorphism, as discussed above)

$$\begin{aligned} \prod_i R/I_i &\xrightarrow{d} \prod_{i \neq j} R/(I_i + I_j) \\ (a_1, \ldots, a_n) &\mapsto (a_i - a_j \bmod I_i + I_j)_{i \neq j}, \end{aligned}$$

and we have that $\ker d = \operatorname{im} \pi$.

In particular, if $I_i + I_j = (1)$ for every pair i, j, then $\widetilde{\pi}$ is an isomorphism.

Exercise 2. Prove that the group homomorphism $d\colon R/I \times R/J \to R/(I + J)$ defined in the statement above is a well-defined function.

The payout of the CRT is that we can sometimes decompose a ring into a direct product of simpler rings. In particular, the comment at the end of the statement of the general ring CRT indicates we can do this if we have the condition $I_i + I_j = (1)$. By analogy with $\mathbb{Z}$, if two ideals $I, J \subset R$ satisfy $I + J = (1)$, those ideals are called **coprime**, or **comaximal** (I slightly prefer the latter, but the former is more common).

Exercise 3. Prove that if I and J are coprime ideals, then $IJ = I \cap J$.

As a short example of a kind of commutative algebra calculation that gets simplified by CRT, consider the ring $\mathbb{C}[x]/(x^2 - 1)$. We can factor $x^2 - 1 = (x - 1)(x + 1)$, which also gives us a factorization on the level of ideals: $(x^2 - 1) = (x - 1)(x + 1)$. Also, the ideals $(x - 1)$ and $(x + 1)$ are coprime, since $x - 1$ and $x + 1$ are distinct irreducibles and $\mathbb{C}[x]$ is a PID. Thus, CRT tells us that

$$\frac{\mathbb{C}[x]}{(x^2 - 1)} = \frac{\mathbb{C}[x]}{(x - 1)(x + 1)} = \frac{\mathbb{C}[x]}{(x - 1) \cap (x + 1)} \cong_{\text{CRT}} \frac{\mathbb{C}[x]}{(x - 1)} \times \frac{\mathbb{C}[x]}{(x + 1)}.$$

This is a simpler ring to understand, because $\mathbb{C}[x]/(x \pm 1) \cong \mathbb{C}$.

Exercise 4. Above, we verified that $(x-1)$ and $(x+1)$ are coprime ideals by appealing to the fact that they are generated by distinct irreducibles in a PID.

(a) Prove that if R is a PID, and f, g are distinct irreducible elements of R, then $(f, g) = (1)$.

(b) On the other hand, give an example of $f, g \in \mathbb{C}[x, y]$ such that $\gcd(f, g) = 1$ but $(f, g) \neq (1)$.

Comment. If you know a typed programming language, you will be dismayed that in my general statement of the CRT, I seem to be mixing functions of the type `ring homomorphism` with functions of the type `group homomorphism`. I'm gonna get a compilation error! To make sure my theorems compile correctly, I technically should say that everything is a homomorphism of R-modules, and some of those also happen to be homomorphisms of R-algebras. But this is a little bit of a piddling point.

Exact sequence formulation

When I was taking 742, Daniel Erman told me the following way to think about the CRT in the case of two ideals. I'm going to write it in terms of exact sequences, but I will not define exact sequences until the module theory notes. The CRT asserts that the following sequence of morphisms is exact

$$0 \to R/(I \cap J) \xrightarrow{\tilde{\pi}} R/I \times R/J \xrightarrow{d} R/(I + J) \to 0.$$

We have an analogy that R/I and R/J are like two subsets of some set $\mathcal{S}$, $R/(I \cap J)$ is like the intersection of the two sets, and $R/(I + J)$ is like their union. In this analogy, $R/I \times R/J$ is like the disjoint union of the two sets, which is what you would get if you took two disjoint copies of $\mathcal{S}$, and cut out R/I from one of them and R/J from the other one. What the CRT is saying is that if we take these two disjoint copies, and glue them together along the intersection $R/(I \cap J)$, we would exactly reconstruct the union $R/(I + J)$. (Algebraic geometers will object that I should have told you that $R/(I \cap J)$ is like a union and $R/(I + J)$ is like an intersection.)

You see ideas similar to this in Topology, where the Mayer-Vietoris sequence looks very similar to the above sequence, and encodes information about intersections, disjoint unions, and unions. The van Kampen theorem does something similar, altho it doesn't have a nice formulation in terms of a sequence.

Noetherian Rings

All of the rings discussed so far have had a nice property called the **ascending chain condition** (ACC), which was first "isolated" by Emmy Noether in her work on invariant theory. In her honor, rings with this property are called **Noetherian rings** (sometimes not capitalized, the same way we sometimes don't capitalize abelian even tho it is named after Abel). The condition goes like this: a ring satisfies the ascending chain condition if any (possibly infinite) chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

eventually stabilizes. That is, there exists an integer N such that for all $n > N$, $I_n = I_N$.

You should think of this in the context of $\mathbb{Z}$ or $\mathbb{C}[x]$. Since those are PIDs, we can instead look at the generators of the ideals, and $(r_n) \subset (r_{n+1})$ means that $r_{n+1} \mid r_n$. So, in these contexts, the ACC says that we can't have an infinitely long chain of divisibilities $\dots r_n \mid r_{n-1} \mid \cdots \mid r_1$. This makes sense in $\mathbb{Z}$ because in that case the divisors have to get progressively smaller, and in $\mathbb{C}[x]$ they have to have lower and lower degree. So, a ring being Noetherian is a kind of "finiteness" condition, and it plays a similar role for general rings that well-orderedness/induction plays for $\mathbb{Z}$.

In general, what kind of thing does the ACC rule out? The standard example of a non-Noetherian ring is the polynomial ring in infinitely many variables $\mathbb{C}[x_1, x_2, \dots]$. This ring has an infinitely ascending chain of ideals $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \dots$. The ascending chain condition doesn't allow this kind of perverse behavior.

Exercise 5.

(a) Prove that in any Noetherian ring, every ideal can be generated by finitely many elements.

(b) In the first set of notes, we proved that any PID is Noetherian. Suppose more generally that a ring R has the property that every ideal can be finitely generated. Prove that R is Noetherian.

(c) **(January 2023 Problem 1 (e), modified)** True or False: any ideal $I \subset \mathbb{C}[x, y]$ can be generated by (at most) 2 elements.

Exercise 6.

(a) Suppose R is a commutative Noetherian ring, and $I \subset R$ is an ideal. Prove that R/I is Noetherian.

(b) If R is Noetherian, and R' is a subring of R, it is *not* necessarily true that R' is also Noetherian! Prove this by finding a subring of $\mathbb{C}[x, y]$ that is not Noetherian. (Hint: use the non-Noetherian example above as inspiration. Try to find infinitely many elements so that no element can be obtained from the rest via sums and products. Think about the degrees with respect to x and to y.)

Exercise 7. (Hilbert's basis theorem) The goal of this exercise is to prove that if R is Noetherian, so too is $R[x]$. We will do this by proving that any ideal of $R[x]$ is finitely generated, which is sufficient by Exercise 5 (c).

(a) Let $I \subset R[x]$ be any ideal. Prove that the set of leading coefficients of polynomials in I is an ideal $J \subset R$.

(b) Suppose that I is not finitely generated, and let $f_1, f_2, \dots$ be elements such that $f_n \in I$, $f_n \notin \backslash(f_1, \dots, f_{n-1})$, and f_n has minimal degree among polynomials with those two properties. Define the ideals $I_n = (f_1, \dots, f_n) \subset R[x]$, and define J_n to be the ideal of R generated by the leading coefficients of $f_1, \dots, f_n$. Prove that $J_N = J$ for some N.

(c) Let N be an integer such that $J_N = J$. Prove that $f_{N+1} \in I_N$. Since this is a contradiction with the construction of the fs, conclude that I is finitely generated.

There is a complementary condition to the ACC called the **descending chain condition** (DCC), and rings satisfying the DCC are called **Artinian rings** (same thing about the capitalization). Despite the formal similarity, a ring being Artinian is a *much* more restrictive class of rings. In particular, every Artinian ring is in fact Noetherian, altho proving this is not straightforward.

As an example, $\mathbb{Z}$ is Noetherian but not Artinian, while for any $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is both Noetherian and Artinian.

Comment. Artinian rings were first discussed in the context of central simple algebras, the classification of which is the subject of the Wedderburn-Artin theorem. It is possible that in the notes about modules I will include some further comments on this.

Exercise 8. Suppose R is a commutative Artinian ring. Prove that any prime ideal $P \subset R$ is maximal. (Hint: prove that R/P is a field.)

Fields of fractions and Gauss' Lemma

Given an integral domain R, there's an important field attached to R called its **field of fractions**, denoted $\operatorname{Frac} R$, which consists of all fractions r/s where $r, s \in R$ and $s \neq 0$. Addition and multiplication work just the way you think they should for fractions. For example, the field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. An example you might not already be familiar with is the field of fractions of $\mathbb{C}[x]$ is $\mathbb{C}(x)$, the field of rational functions. Next section we will discuss localization, of which the field of fractions is just one example.

The field of fractions is useful because often things are easier to prove for fields, and sometimes we can transfer properties from the field of fractions back to the original ring R. For example, we have already proven that $k[x]$ is a Euclidean domain whenever k is a field. The next exercise is to prove **Gauss' lemma**, a super important lemma which, among other things, shows that if R is a UFD, then so is $R[x]$. Hence, so is $R[x_1, \ldots, x_n]$ for all n. In particular, this proves the assertions above that $\mathbb{Z}[x]$ and $\mathbb{C}[x, y]$ are UFDs.

(I feel sometimes that whenever there's a hard proof in ring theory, the proof always reduces to either Gauss' lemma or the Cayley-Hamilton theorem, or both!)

Exercise 9. (Gauss' lemma)

(a) Let R be a UFD. Given a polynomial $f \in R[x]$, the *content* of f, $\operatorname{cont}(f)$, is the gcd of all the coefficients in f. Prove that $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

(b) A polynomial such that $\operatorname{cont}(f) = 1$ is called *primitive*. Show that fg is primitive if and only if f and g are primitive.

(c) Let $K = \operatorname{Frac} R$. Prove that a primitive polynomial $f \in R[x]$ is irreducible if and only if it is irreducible when considered as an element of $K[x]$.

(d) Prove that $R[x]$ is a UFD.

Comment. There are actually many related results that get called "Gauss' lemma", some of which can look significantly different from the formulation above.

Localization

This final section is the longest, and most important in these notes. Localization refers to the process of adding fractions to a ring. Altho this is a very simple premise, this turns out to enjoy many useful formal properties that makes it very helpful, which we will begin exploring here, and will continue to discuss in the notes on modules. If you're curious about why this process is called "localization", there are two optional exercises in the last section attempting to illustrate the connection between fractions and "local" information, in a geometric or topological sense.

We already know some examples of localization, because, as previously mentioned, taking an integral domain to its field of fractions is a localization. The procedure we will describe will generalize this in two directions:

1. We will be able to talk about fractions in an arbitrary ring, no longer restricted to just integral domains.

2. We will have the option to add only some denominators and not others, and this flexibility will be valuable.

The next exercise is an opportunity for you to reflect on what the algebraic implications are of adding in denominators.

Exercise 10.

(a) Consider the ring $\mathbb{Z}[\frac{1}{2}]$, which consists of the integers, the fraction $\frac{1}{2}$, and the minimum of other numbers which must be in the set in order for it to be a ring. Describe the set of all possible denominators a fraction in this ring can have.

(b) Consider the ring $R = \mathbb{Z}/12\mathbb{Z}$. As in the previous example, I want to be able to make sense of fractions with 2 in the denominator, but now it's more complicated because 2 is a zero-divisor. Denote the ring where I can take denominators of 2 by $R[\frac{1}{2}]$.

  (i) Use your knowledge of how to manipulate fractions to convince yourself that $\frac{3}{2} = 0$ in $R[\frac{1}{2}]$. (Hint: you can multiply the top and bottom of a fraction by the same number to get an equivalent fraction.)

  (ii) On the other hand, convince yourself that if $n \in R$ is not in the ideal (3), then $\frac{n}{2} \neq 0$ in $R[\frac{1}{2}]$.

  (iii) The ring $R[\frac{1}{2}]$ is finite. Use what you deduced above to figure out how many inequivalent elements it has.

(c) Still thinking about $R = \mathbb{Z}/12\mathbb{Z}$, what ring would we get if we decided to take 5 in the denominator? What would we get if we decided to take 6 in the denominator?

In general, what do we need from a set of possible denominators $S \subset R$ in order for it to make sense to add in all those denominators to our ring? We always want to be able to have a denominator of 1, so we will demand that $1 \in S$ always. In order for the familiar property $\left(\frac{r_1}{s_1}\right)\left(\frac{r_2}{s_2}\right) = \frac{r_1 r_2}{s_1 s_2}$ to hold, we need $s_1 s_2 \in S$ for any $s_1, s_2 \in S$. Any set S that satisfying these two properties is called **multiplicatively closed**. Given a multiplicatively closed subset $S \subset R$, we define a new ring $S^{-1}R$ in imitation of the definition of the rational numbers, with one twist:

- The elements of $S^{-1}R$ are symbols of the form $\frac{r}{s}$ where $r \in R$ and $s \in S$.
- You might expect two symbols $\frac{r_1}{s_1}, \frac{r_2}{s_2}$ to be equal if their cross difference vanishes, $r_1 s_2 - r_2 s_1 = 0$. However, this is the twist: we actually say they are equal if *there is some $s \in S$ such that* $s(r_1 s_2 - r_2 s_1) = 0$.
- Multiplication is defined as you would expect. Addition is defined by taking common denominators:
$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}.$$

I think about the modification in the second bullet point like this. We all agree how addition and subtraction of fractions should work, and we all agree that $\frac{a}{b} = \frac{sa}{sb}$ for any $s \in S$. The change in the second bullet point over what you would naively expect is there to account for situations where you can chain these two rules to get unexpected results. In the example computed in Exercise 10 (b), we could have
$$4 - 1 = 3 = \frac{4 \cdot 3}{4} = \frac{0}{4} = 0,$$
so in fact we find that $4 = 1$ once we allow in $\frac{1}{2}$.

Comment. The notation S is standard for a multiplicatively closed subset, and also as the name of a second ring after R is taken. I've avoided using the latter so that I can have S always be a multiplicatively closed subset. Some authors, such as Atiyah-Macdonald and also me in other writings, adopt the French convention in which rings are A (for "anneau"), and further rings are B, C, which has the added benefit of leaving S available to always be a multiplicatively closed subset.

Example 1. Here are two very commonly used kinds of localization.

- Given a ring R and an element $f \in R$, the set $S = \{1, f, f^2, \ldots\}$ consisting of all the powers of f is multiplicatively closed. In this case, the localization $S^{-1}R$ is commonly denoted by either R_f or $R[\frac{1}{f}]$. The former is both more traditional and faster to write, while the latter is much more unambiguous. When written R_f, it is commonly said aloud as "R localized at (the element) x", and when written $R[\frac{1}{f}]$ it is said as "R adjoin $\frac{1}{f}$".

- Given a ring R and a prime ideal P, the set $S = R \setminus P$, all the elements of R that are *not* in P, is multiplicatively closed. In this case, the localization $S^{-1}R$ is denoted by R_P, and it is said aloud as "R localized at (the ideal) P". Sometimes I have heard people say "R localized *away from* P", to emphasize that S is the complement of P. **Exercise 11.** Prove that $S = R \setminus P$ is multiplicatively closed. Prove that in R_P, the ideal generated by the elements of P, $\langle \frac{p}{1} : p \in P \rangle$, is a maximal ideal.

As one example, if R is an integral domain, we have already seen that (0) is a prime ideal of R. Then the localization $R_{(0)}$ is just the same thing as throwing in $1/r$ for every nonzero $r \in R$, which is the same thing as taking the fraction field. So, $\mathrm{Frac}(R) = R_{(0)}$.

Comment. Considering the element $x \in \mathbb{C}[x]$, note that the ideal (x) is prime. So, I can either form the localization $\mathbb{C}[x]_x$ or $\mathbb{C}[x]_{(x)}$, and these are two *different* rings! This is why in many cases I would prefer to write $\mathbb{C}[x]_x$ as $\mathbb{C}[x, x^{-1}]$. What is worse, when $R = \mathbb{Z}$, group theorists and topologists will write $\mathbb{Z}_n$ to mean the cyclic group $\mathbb{Z}/n\mathbb{Z}$, and number theorists will write $\mathbb{Z}_p$ to mean the p-adic integers (which are closely related to localization, but distinct). So, in the context of $\mathbb{Z}$, you should always write $\mathbb{Z}[\frac{1}{n}]$, and if you want to localize at (away from) the prime ideal (p), make sure you include the parentheses: $\mathbb{Z}_{(p)}$.

The localization homomorphism

Whenever you learn a way to get a new object from old objects, you should ask "how does this interact with homomorphisms?". In many respects, localization behaves a lot like a quotient ring. There is a homomorphism $R \to S^{-1}R$ that takes $r \to \frac{r}{1}$. The quotient homomorphism $R \to R/I$ is characterized by taking every element of I to 0 in the quotient. The localization homomorphism is characterized by taking every element $s \in S$ to a unit in the localization, which makes sense because, after all, we're explicitly adding in elements of the form $\frac{1}{s}$. The localization homomorphism also has a property similar to the one discussed above in the section **The universal property of quotient rings**:

Theorem. Let R, R' be rings, let S be a multiplicatively closed subset of R, and let $\ell \colon R \to S^{-1}R$ be the localization homomorphism. If $\phi \colon R \to R'$ is a homomorphism such that for every $s \in S$, $\phi(s)$ is a unit in R', then there is a unique map $\widetilde{\phi} \colon S^{-1}R \to R'$ such that $\phi = \widetilde{\phi} \circ \ell$.

Concretely, the map $\widetilde{\phi}$ sends the fraction $\frac{r}{s} \mapsto \phi(r)\phi(s)^{-1}$. As before, the content of the statement is mostly verifying that this is a well-defined function.

The discussion of how to think about/interpret the similar property for quotient rings applies equally well to this theorem. Similar to quotient rings, if we tried to write down functions out of a localization on the level of the elements of the localization, it would be difficult because (1) the localization can have many new elements that weren't in the original ring, and (2) the elements of the localization might have difficult-to-anticipate relationships between them, as we saw above when we showed that $4 = 1$ in $(\mathbb{Z}/12\mathbb{Z})[\frac{1}{2}]$. This theorem gives us an alternative way of defining these maps, which can be much easier to check in general.

Here is a diagram for the universal property of the localization homomorphism:

$$\begin{tikzcd} R \arrow[d, "q"'] \arrow[dr, "\phi"] & \\ S^{-1}R \arrow[r, dashed, "\widetilde{\phi}"'] & R' \end{tikzcd}$$

A restatement of the theorem is "for all homomorphisms ϕ such that $\phi(s)$ is a unit for all $s \in S$, there exists a unique homomorphism $\widetilde{\phi}$ making the above diagram commute".

Exercise 12.

(a) Let $f, g \in R$. Prove that $R[\frac{1}{fg}] \cong R[\frac{1}{f}, \frac{1}{g}]$. (Try doing this once using the definition of localization, and once using the theorem above to construct homomorphisms in both directions, then showing they are inverses. Reflect on how these two arguments feel different to think about.)

(b) Prove that the localization homomorphism $\ell\colon R \to S^{-1}R$ is injective if and only if S contains no zero-divisors.

(c) Prove that the localization $S^{-1}R$ is the zero ring if and only if $0 \in S$.

Exercise 13. Give an example of a ring homomorphism $\phi\colon R \to S$, and a maximal ideal $\mathfrak{m} \subset S$ such that $\phi^{-1}(\mathfrak{m})$ is *not* a maximal ideal of R. (Hint: this problem is in the section on localization.)

Ideals in a localization

There is an analog to the lattice isomorphism theorem for ideals in a localization.

Theorem. Let R be a ring, S a multiplicatively closed subset, and I an ideal of R that *does not meet* S. That is, $I \cap S = \emptyset$. Then the ideal $S^{-1}I = \langle \frac{i}{1} : i \in I \rangle$ is a *proper* ideal of $S^{-1}R$, and moreover every proper ideal of $S^{-1}R$ can be obtained this way. This correspondence has the further properties:

- It preserves the subset relation: if $I \subset J$, then $S^{-1}I \subset S^{-1}J$.
- It preserves prime ideals: if P is a prime ideal of R that does not meet S, then $S^{-1}P$ is a prime ideal of $S^{-1}R$.

When the localization is of the form R_P, where P is a prime ideal, then often instead of writing $S^{-1}I$ people will write I_P. Similarly, when the localization is of the form R_f, where $f \in R$ is an element, often people will write I_f. This is the main situation in which the notation R_f seems better than the notation $R[\frac{1}{f}]$, because nobody writes (or wants to write) $I[\frac{1}{f}]$, and writing something more apt like $IR[\frac{1}{f}]$ is a bit cumbersome. (But people do write it, e.g. number theorists will write things like $3\mathbb{Z}[\frac{1}{2}]$ quite happily.)

The moral here is that if we add in a fraction $\frac{1}{f}$, then we effectively eliminate all the ideals that contain f, because now any ideal that contains f also contains $f \cdot \frac{1}{f} = 1$, and so is the unit ideal.

So, for example, referencing our lattice of the ideals in $\mathbb{Z}$ from earlier, the lattice of ideals in $\mathbb{Z}[\frac{1}{6}]$ is illustrated in Figure 3, where I have slashed out the ideals that have become the unit ideal after localizing. Notice that any ideal divisible by only (2) and/or (3) has now become the unit ideal, and several other ideals have merged, like $(5) = (10) = (15) = (30)$.

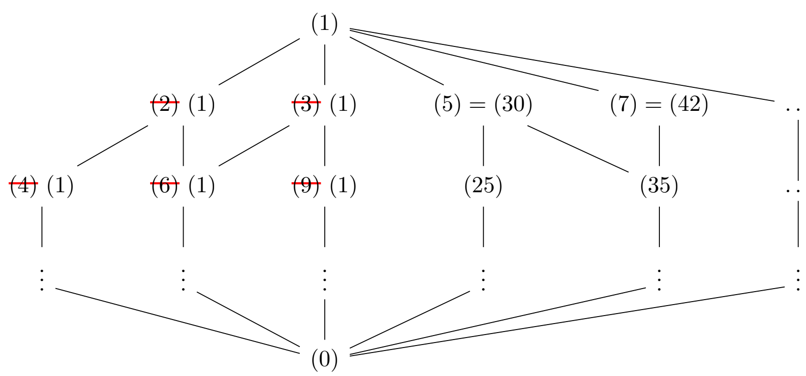

Figure 3: The lattice of ideals in $\mathbb{Z}[\frac{1}{6}]$

Exercise 14. (January 2020 Problem 3 (a), (c)) Let R be a commutative ring, I an ideal in R, and S a multiplicative subset of R. There are two standard correspondences involving prime ideals:

(i) Prime ideals in R/I are in bijection with prime ideals in R which contain I.

(ii) Prime ideals in $S^{-1}R$ are in bijection with prime ideals in R which do not meet S.

(a) Prove (i) and (ii). (The original problem only asked for one or the other, but you should be able to prove both.)

(c) Give an example of a subring of $\mathbb{Q}$ that has exactly three prime ideals.

Exercise 15. (August 2021 Problem 1 (a), (b)) On this problem, only the answer will be graded.

(a) Put $R = \mathbb{Z}/12\mathbb{Z}$. For which elements $f \in R$ is the localization $R_f = 0$?

(b) Put $R = \mathbb{Z}/12\mathbb{Z}$. For which elements $f \in R$ is the localization R_f a field? (Recall that the zero ring is not a field.)

Local rings

A ring is called a **local ring** if it has exactly one maximal ideal. All fields are local rings (because (0) is maximal in a field).

Exercise 16.

(a) Suppose R is a local ring with unique maximal ideal $\mathfrak{m}$. Prove that any $x \in R \setminus \mathfrak{m}$ is a unit.

(b) Conversely, suppose that R is a ring, and I is an ideal of R with the property that every $x \in R \setminus I$ is a unit. Prove that R is local and I is its unique maximal ideal.

(c) Find an example of a quotient of $\mathbb{Z}$ or $\mathbb{C}[x]$ that is a local ring that is not a field.

(d) Let R be a ring, P a prime ideal. Prove that R_P is a local ring with maximal ideal P_P (using the notation from above).

If fields are easiest rings to work with, local rings are for most things the second easiest rings to work with, and if you do anything with commutative algebra, algebraic geometry, or the algebraic side of number theory, you will encounter local rings of the form R_P very frequently. A proof strategy that is used very commonly goes like this:

1. First, prove a statement is true for fields. This is usually very easy.

2. Next, prove that the statement for fields implies the statement for local rings. If R is a local ring with maximal ideal $\mathfrak{m}$, then $R/\mathfrak{m}$ is called the **residue field** of R, and many properties of the residue field can be lifted to R, for example by using Nakayama's lemma (which will be discussed more in the notes on modules).

3. Finally, prove that if R is an arbitrary ring, then the statement holds for R if and only if it holds for all the rings R_P, where P ranges over all prime ideals of R. This is usually the hardest part of the process, and is frequently not true without pretty strong hypotheses on the ring R.

Exercise 17. (January 2018 Problem 1) For this problem, your answer will be graded on correctness alone, and no justification is necessary.

(a) Give an example of a commutative ring R and a nonzero element $f \in R$ where the localization $R_f = 0$.

(b) Give an example of a commutative ring R and a nonzero element $f \in R$ where the localization map $R \to R_f$ is neither injective nor surjective.

(c) Give an example of a *local* ring R and an element $f \in R$ where $R_f \neq 0$ but R_f is no longer a local ring.

What makes local rings "local"?

The following two exercises are optional. Their purpose is to give a hopefully enlightening example showing in what sense "local rings" and "localization" can capture "local" information, in a topological or geometric sense.

Exercise 18. (localization in geometry) Take the plane $\mathbb{R}^2$ with the usual topology via open disks.

(a) For any open set $U \subset \mathbb{R}^2$, show that $\mathcal{C}(U)$, the set of continuous functions $U \to \mathbb{R}$, is a commutative ring under the operations of pointwise addition and multiplication.

(b) For any $f\colon U \to \mathbb{R}$, show that $f^{-1}(0)$ is a closed subset of U.

(c) Show conversely that for any closed subset $K \subset U$, there exists a function $f\colon U \to \mathbb{R}$ such that $f^{-1}(0) = K$. (Don't spend too long on this, it's not worth it to do it in great detail.)

(d) If U, V are open sets with $V \subset U$, then given any $f \in \mathcal{C}(U)$, we can restrict f to V to get a function $f|_V \in \mathcal{C}(V)$. Show that this defines an injective ring homomorphism $\mathcal{C}(U) \to \mathcal{C}(V)$. (Notice that the map goes the opposite direction from the set inclusion!)

(e) If V is open, $V \subset U$, then $U \setminus V$ is a closed subset of U. Call this closed subset K. Show that if $f \in \mathcal{C}(U)$ satisfies $f^{-1}(0) \subset K$, then $f|_V$ is a unit in $\mathcal{C}(V)$. Thus, by restricting to a smaller open set, we have added $1/f$ to the ring for all such f.

Exercise 19. (continuation of Ex. 18) Take again the plane $\mathbb{R}^2$.

(a) Let $U \subset \mathbb{R}^2$ be any open set containing the origin. Show that the set $\mathfrak{m}_{0,U} := \{f \in \mathcal{C}(U) : f(0,0) = 0\}$, the set of functions which vanish at the origin, is a maximal ideal of $\mathcal{C}(U)$. (Hint: show that $\mathcal{C}(U) \to \mathbb{R}$ given by $f(x,y) \mapsto f(0,0)$ is a ring hom.)

(b) Let U and V be any two open sets containing the origin, and declare a function $f \in \mathcal{C}(U)$ to be equivalent to a function $g \in \mathcal{C}(V)$ if there is some open set $W \subset U \cap V$, $0 \in W$, so that $f|_W = g|_W$. That is, two functions are equivalent if they look the same once we zoom in close enough to $(0,0)$.

    Check that this is an equivalence relation on the set of pairs (U, f), where U is an open set containing the origin, and $f \in \mathcal{C}(U)$.

(c) Define a ring $\mathcal{C}_0$ as follows: the elements of $\mathcal{C}_0$ are pairs (U, f), where U is an open set containing the origin, and $f \in \mathcal{C}(U)$, subject to the equivalence relation above. The equivalence classes under this relation are called **germs** of functions. To add or multiply two germs (U, f) and (V, g), we pass to some smaller open set $W \subset U \cap V$, and then add or multiply $f|_W$ with $g|_W$.

    Prove that $\mathcal{C}_0$ is a local ring, whose unique maximal ideal consists of germs of the form (U, f), where $f \in \mathfrak{m}_{0,U}$. (Hint: prove that if a germ is not in $\mathfrak{m}_{0,U}$, then it is a unit.)

(d) In fact, prove that if U is an open set containing the origin, then $\mathcal{C}_0 \cong \mathcal{C}(U)_{\mathfrak{m}_{0,U}}$.

You should think of the germ of a function f as essentially remembering its Taylor expansion at the origin (disregarding the fact that I stated the above for continuous rather than differentiable or analytic functions). It remembers the value $f(0,0)$, and all the infinitesimal information about f's behavior near 0, but it doesn't remember the value of $f(x)$ for any $x \neq 0$. One could say that the germ of f remembers all, and only, the local information about f near the point $x = 0$.

Notice that in the two proceeding exercises, it was never particularly important that the space we were considering was $\mathbb{R}^2$, and that the functions were landing in $\mathbb{R}$. In some sense, all we used in the constructions was:

- the space $\mathbb{R}^2$ is a topological space,
- the ring $\mathbb{R}$ is a ring,
- for any two points $x, y \in \mathbb{R}^2$, there is a function $f\colon \mathbb{R}^2 \to \mathbb{R}$ so that $f(x) = 0$ and $f(y) \neq 0$.

Because of how lax these requirements are, similar constructions can be (and are) used to study many different kinds of geometric objects from an algebraic perspective: manifolds, complex analytic spaces, varieties, and more.