Ring Theory 1
Examples to keep in mind, basic definitions, ideals, the isomorphism theorems
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!

User's Guide

By my estimation, ring theory and module theory are both the most frequent qual questions (I estimate about they make up about 2/5 of every qual), as well as some of the toughest questions. For this reason, I have tried to make the notes on them thorough, at some cost to brevity, with the goal that the thoroughness will help you if you have less background in ring theory already, and will be a useful reference even if you already know more ring theory.

If you've already taken a course in ring theory, I would expect you to be familiar with most of the things discussed in these notes. For such a person, I think the most important things in these notes are:

- to know the basic properties of the three big examples
- the little bit of content discussed in the section on noncommutative ring theory, and
- the various examples and counterexamples that pop up throughout. (e.g. a UFD that is not a PID, a prime ideal that isn't maximal, ideals whose intersection is not equal to their product, etc.)

The next set of notes will discuss, among other things, **the lattice isomorphism theorem** and **localization**, which are both very important and appear on the qual quite frequently.

Conventions

In these notes, all rings will have unity, but may or may not be commutative, depending on the section. As a reminder, a homomorphism $R \to R'$ of unital rings is required to send 1_R (the multiplicative unit of R) to $1_{R'}$ (that of R'), and a subring $R'' \subset R$ is required to have the same unit as R does, so that the inclusion $R'' \hookrightarrow R$ is a unital ring homomorphism. These conventions differ from the conventions in Dummit and Foote, where they allow rings without unity, and they allow "subrings" of rings with unity to not have unity. In particular, they are happy to call ideals a special kind of "subring". I think these conventions were a little out of date at the time, and nowadays I think it'd be hard to find authors who allow rings without unity.

Exercise 1. Find a subset of $M_2(\mathbb{R})$ which has the structure of a ring with unity under the operations of matrix addition and multiplication, but which is not a subring of $M_2(\mathbb{R})$.

Examples

The three big ones

I think there are three main examples you should keep in mind for ring theory:

- the ring of integers $\mathbb{Z}$,
- the ring of complex polynomials in one variable $\mathbb{C}[x]$,
- the ring of complex 2×2 matrices $M_2(\mathbb{C})$.

Especially when we start talking about modules, it will be enlightening to be able to think about what modules look like for these three examples. (In the past I haven't emphasized non-commutative rings enough, but when preparing these notes I realized they show up on the qual somewhat frequently.)

Other good examples

Here are a few more rings you should have in your head for various examples/counterexamples in ring theory.

- The rings $\mathbb{R}[x]$, $\mathbb{Q}[x]$, and $\mathbb{Z}[x]$. The rings $\mathbb{R}[x]$ and $\mathbb{Q}[x]$ will have a lot in common with $\mathbb{C}[x]$, but if k is not algebraically closed you will get different irreducible elements. The ring $\mathbb{Z}[x]$ is closely connected to $\mathbb{Q}[x]$ (via Gauss' lemma, see the next set of notes), but also has additional interesting structure of its own.
- Rings of polynomials in more than one variable. For example, $\mathbb{C}[x, y]$ and $\mathbb{C}[x, y, z]$.
- Quotient rings of rings you already know. Some examples that come to mind are:
  - If $f \in \mathbb{Q}[x]$ is an irreducible polynomial, the ring $\mathbb{Q}[x]/(f)$ is a field extension of $\mathbb{Q}$. This kind of example is very important in field theory.
  - For k a field, the ring $k[x]/(x^2)$ is sometimes called "the ring of dual numbers". In this ring, the element x behaves like an infinitesimal in old-timey calculus, because x is not zero, but $x^2 = 0$.
  - There are lots of interesting quotients of polynomial rings in many variables. For example, $\mathbb{C}[x]/(x^2+y^2-1)$ is a ring that is associated to the equation $x^2+y^2-1 = 0$, or $x^2+y^2 = 1$ as a sane person might write it. So, this ring captures some information about the unit circle. The ring $\mathbb{C}[x, y]/(xy)$ has come up a couple times on old quals. In a sense, the field of **algebraic geometry** is concerned with studying the rings that arise as quotients of multivariable polynomial rings.
- Other matrix rings such as $M_2(\mathbb{R})$ and $M_2(\mathbb{Z})$. Sometimes you might need to think about matrices larger than 2×2, but there's a meta-principle that "any behavior that can occur for matrices, can occur for 2×2 matrices". This, of course, is not literally true, but it's true often enough to be a useful guide.

- Given a group G, one can form the **group ring** $\mathbb{C}[G]$ (sometimes written $\mathbb{C}G$). The elements of the group ring are formal linear combinations $\sum c_i g_i$, where we treat the group elements as linearly independent vectors over $\mathbb{C}$. Addition is straightforward, and multiplication is defined by using the multiplication in the group. (The complex numbers are not important here, one can just as easily form $\mathbb{R}[G]$, $\mathbb{Z}[G]$, or $R[G]$ for any ring R.) Group rings come up in the area of **representation theory**, which is listed as a qual topic but usually only appears disguised as something else, such as ring theory questions about a group ring.

Basics about commutative rings

Ideals in commutative rings

For now, all our rings will be commutative. An **ideal** in a commutative ring R is a subset $I \subset R$ with the following two properties:

(i) I is closed under addition, and

(ii) I is *absorbing* under multiplication; that is, for any $r \in R$ and $i \in I$, $ri \in I$.

Later in this section I'll give some historical examples that motivated creating ideals. For now, I'll note that given some elements $g_1, \ldots, g_n \in R$, we can form an ideal *generated by* those elements, denoted either $\langle g_1, \ldots, g_n \rangle$ or just $(g_1, \ldots, g_n)$ when the parentheses will cause no confusion, which is simply the subset of R consisting of elements of the form $r_1 g_1 + \cdots + r_n g_n$. (This definition can be extended to ideals generated by infinite sets, with the condition that you are only ever allowed to take a finite sum of $r_i g_i$. Our rings don't have a notion of "convergent series" in them ... yet.) If an ideal can be written as $I = (g)$, then I is called **principal**.

A ring R is always an ideal of itself, often denoted (1) to distinguish when we're thinkging about R as a ring versus as an ideal of itself. This ideal is often called the *unit ideal*. There's one more ideal that every ring has: the ideal that consists just of the element 0, intuitively named the *zero ideal*.

Euclidean domains, PIDs, and UFDs

Turning to our examples, notice that both $\mathbb{Z}$ and $\mathbb{C}[x]$ have a notion of "division with remainder", which you hopefully learned about sometime during your K-12 education. They are examples of **Euclidean domains**: a ring R together with a function $f\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ so that for any pair a, b, we can find q, r so that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$. In the case of $\mathbb{Z}$, the function in question is the usual absolute value, and in the case of $\mathbb{C}[x]$ the function takes a polynomial to its degree. It might seem strange to single out the element 0 to not be given a value by this function. The reason it is left out is that there are contexts in which you want the degree of 0 to be $-\infty$ to make some formula work, and there are instances in which you want the degree of 0 to be ∞ to make some formula work. So, all in all, it's best to not say anything about the degree of 0, and single it out for special treatment.

Let's start working on understanding $\mathbb{Z}$ and $\mathbb{C}[x]$. One extremely basic observation about these rings is that if the product of two elements is 0, one of the two elements is 0. A ring R is an **integral domain**, or simply a **domain**, if whenever $ab = 0$, either $a = 0$ or $b = 0$. An element z such that there exists a non-zero element b satisfying $zb = 0$ is called a **zero-divisor**. So, another equivalent thing to say is that in an integral domain, the only zero-divisor is 0. (Sometimes people define a zero-divisor to be non-zero.)

Another rephrasing is that integral domains are the rings in which *cancellation* is valid: if $ab = ac$, then either $a = 0$ or $b = c$. Notice that every Euclidean domain is also an integral domain.

Let's start working on understanding the ideals of $\mathbb{Z}$ and $\mathbb{C}[x]$. Define an element $d \in R$ to be a **greatest common divisor** (gcd) of two elements a and b if $d \mid a$, $d \mid b$, and for any other element n that divides a and b, we also have that $n \mid d$. Notice that I said a gcd, not *the* gcd, because such an element need not be unique: for example, if d is a gcd of a and b, then so is $-d$. More generally, if $u \in R$ is a **unit** (i.e. there exists $v \in R$ so that $uv = 1$) then ud is also a gcd of a and b. Two elements r, r' in a ring R that differ only by multiplication by a unit $r = ur'$ are called **associates**.

Exercise 2. (gcds) Let R be a Euclidean domain.

(a) Suppose $a = bq + r$, and suppose d is a gcd of a and b. Show that d is a gcd of b and r as well.

(b) Given two elements $a, b \in R$, we may perform division with remainder to write $a = bq_1 + r_1$ with either $r_1 = 0$ or $f(r_1) < f(b)$. Then, we may do it again to b and r_1: $b = q_2 r_1 + r_2$. Then to r_1 and r_2. And so on, and so on. Prove that eventually this process reaches 0.

(c) Let r_n be the last nonzero remainder found by the above process. Show that r_n is a gcd of a and b.

(d) The penultimate step of the process gives us an expression of the form $r_{n-2} = q_n r_{n-1} + r_n$, so rearranging we get $r_n = r_{n-2} - q_n r_{n-1}$. Do this all the way up the chain to show that there exist $x, y \in R$ so that $r_n = ax + by$.

(e) Perform the algorithm outlined above starting with the integers $a = 13623$ and $b = 9215$. Calculate their gcd d, then back-substitute to find integers x and y so that $d = 13623x + 9215y$. Yes, I'm serious.

Greatest common divisors are related to thinking about factorizations. An element $p \in R$ is called **irreducible** if whenever $a \mid p$, we have that a is either a unit or an associate of p. Whenever we can take gcds between elements, we can use gcds to factor a given element into irreducibles, like we can factor integers in $\mathbb{Z}$. An integral domain in which every element can be written as a product of irreducible elements, and that product is unique up to multiplying the whole thing by a unit, and up to replacing the irreducible elements in the product by associates, is called a **Unique Factorization Domain** (UFD). (For example, in $\mathbb{Z}$, we don't consider $6 = 2 \cdot 3 = (-2) \cdot (-3) = -(2 \cdot (-3))$ to really be different factorizations of 6.)

Exercise 3. (EDs are PIDs) Prove that if R is a Euclidean domain, then every ideal in R is principal. An integral domain in which every ideal is principal is called a **principal ideal domain** (PID).

Exercise 4. (PIDs are UFDs, Part 1) Let R be a PID. This exercise, along with Exercise 6, will prove that R is also a UFD.

(a) Prove that the ideal $(p) \subset R$ is maximal if and only if p is irreducible.

(b) Prove that every element $r \in R$ has an irreducible divisor. (Hint: every ideal is contained in a maximal ideal.)

The idea is basically to use the proof of unique factorization that is familiar in $\mathbb{Z}$, and adapt it to a general PID. For $\mathbb{Z}$, the outline of the proof is:

1. First, show that any positive integer has a positive prime factor.

2. Then, successively factor $n = p_1 n_1 = p_1 p_2 n_2 = \dots$. The sequence of integers $n, n_1, n_2, \dots$ is a decreasing sequence of positive integers, and since $\mathbb{Z}$ is well-ordered this sequence must end after finitely many steps. By design, it can only end when $n_\ell = 1$, at which point we will have achieved some prime factorization of n.

3. Finally, show that any two putatively distinct factorizations of n actually have the same primes to the same powers.

In the exercise above, we have already accomplished step 1 in a general PID. Step 3 is no harder for a general PID than it is for $\mathbb{Z}$. However, there is something difficult in step 2, because we cannot assume that our PID is well-ordered like the positive integers are. We need some other way to guarantee that this process cannot go on indefinitely, which is provided by the next exercise.

Exercise 5. Let R be a PID, and suppose we have an infinite chain of ideals

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

(a) Prove that $\bigcup_{j=1}^{\infty} I_j$ is an ideal of R.

(b) Prove that this sequence terminates, in the sense that there is some N so that $I_j = I_N$ for all $j \geq N$.

The property (b) above implies that a PID is **Noetherian**, which we will discuss further in the next set of notes. This tool fills the gap we had.

Exercise 6. (PIDs are UFDs, Part 2) This exercise continues Exercise 4. Let R be a PID.

(a) Prove that any $r \in R$ has a (finite) factorization into irreducible elements.

(b) Suppose $r = up_1^{e_1} \dots p_m^{e_m} = vq_1^{f_1} \dots q_n^{f_n}$, where u, v are units and p_i, q_j are irreducibles with the p_i distinct and the q_j distinct. Prove that every p_i is associate to some q_j, and that $e_i = f_j$. Conclude that also $n = m$. Thus, the factorization is unique in the manner desired, so R is a UFD.

(Actually, it may not be worth your time to think too much about part (b). It's a bit of a tedious argument, and the conclusion is what's important.)

This whole story about factorization is related to why ideals were originally created. People were looking at rings of the form $\mathbb{Z}[\alpha]$ where $\alpha \in \mathbb{C}$ was the root of a monic polynomial with integer coefficients. They hoped that arithmetic in these rings would work a lot like arithmetic in $\mathbb{Z}$. Tragically, it does not. For example, in the ring $\mathbb{Z}[\sqrt{-5}]$, I can factorize $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. All of the elements $2, 3, 1 \pm \sqrt{-5}$ are irreducible in this ring, but none of them are associate to one another (the only units in this ring are ± 1). Kummer observed that the problem here is that there is no number that can serve as $\gcd(2, 1 + \sqrt{-5})$ or $\gcd(3, 1 \pm \sqrt{-5})$. So, he introduced what he called "ideal numbers", which vaguely served to stand in for these missing gcds, and with them he achieved the factorization $6 = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$. Later, Dedekind solidified Kummer's idea by defining ideals as we do today, as subsets of a ring R.

So, one important takeaway is that an ideal $I = (g_1, \dots, g_n)$ can be thought of as a "generalized gcd" of the elements $g_1, \dots, g_n$.

Fun things to do with ideals

You can do several things to ideals to get new ideals:

- If I, J are ideals, then their **intersection** $I \cap J$ is an ideal. When R is a PID, $(a) \cap (b) = (\text{lcm}(a, b))$, and in general you should think of $I \cap J$ as being like the least common multiple of I and J. **Exercise 7.** Prove that $I \cap J$ is an ideal.

- If I, J are ideals, then their **sum** $I + J = \{i + j : i \in I,\ j \in J\}$ is an ideal. When R is a PID, $(a) + (b) = (\gcd(a, b))$. The sum of two ideals I and J is the smallest ideal that contains both I and J. **Exercise 8.** Prove that $I + J$ is an ideal. Prove that for any ideal I' such that $I' \supset I$ and $I' \supset J$, $I' \supset I + J$.

- If I, J are ideals, then their **product** $IJ = \langle ij : i \in I,\ j \in J \rangle$ is an ideal. This ideal always sits inside $I \cap J$, and it can be strictly smaller. If R is a PID, $(a)(b) = (ab)$, and the fact that IJ can be strictly smaller than $I \cap J$ is similar to how the product of two numbers can be larger than their lcm if they have common factors. **Exercise 9.** Notice that in the definition of IJ I put angle brackets rather than curly brackets, because in general $\{ij : i \in I,\ j \in J\}$

is not an ideal. Let $R = \mathbb{C}[x, y]$, $I = J = (x, y)$. Show that there are elements in IJ that are not expressible as just a product of the form $ij,\ i \in I,\ j \in J$.

Exercise 10. Let $R = \mathbb{C}[x, y, z]$, and define the ideals $I = (x^3, x^2z)$ and $J = (x^4, x^2y^2)$.

(a) Find a generating set for $I + J$.

(b) Find a generating set for IJ.

(c) Find a generating set for $I \cap J$.

(d) Verify that $I \cap J \supsetneq IJ$ by demonstrating a polynomial in $I \cap J$ that is not in IJ.

Since ideals are like numbers, we have an analog of prime numbers. An ideal P is **prime** if it is proper (not all of R), and whenever $ab \in P$, either $a \in P$ or $b \in P$. This gives us one more way to rephrase what it means to be an integral domain: a ring is an integral domain if the ideal (0) is prime. One more kind of ideal that is very important, but which doesn't have a direct analog for numbers are maximal ideals. A proper ideal is **maximal** if it is not contained in any other proper ideal.

The following fact is good to know, but unenlightening to prove. (It is just an exercise in using Zorn's lemma.)

Fact. Given a ring R and an ideal $I \subset R$, there exists a maximal ideal $\mathfrak{m} \supset I$.

Given an ideal I, we can form the **quotient ring** R/I. The elements of the quotient ring are *additive cosets* $r+I = \{r+i : i \in I\}$, and the ring operations are more or less clear: $(r_1+I)+(r_2+I) = (r_1 + r_2) + I$, $(r_1 + I)(r_2 + I) = r_1r_2 + I$. As usual, you can shortcut this in your mind as just setting all the elements of the ideal equal to zero, and working "modulo I". Notice that unlike with groups, we don't quotient rings by subrings, but rather by ideals, which have a somewhat different flavor.

Exercise 11.

(a) Prove that $\mathbb{C}[x]/(x - 3) \cong \mathbb{C}$.

(b) Prove that $\mathbb{C}[x, y, z]/(x - 3, y + 1, z - 2) \cong \mathbb{C}$.

(c) Prove that $\mathbb{C}[x]/(x^2 + x + 1)$ is a 2-dimensional $\mathbb{C}$-vector space.

Exercise 12. Let $\phi\colon R \to R'$ be a ring homomorphism. Show that $\ker \phi$ is an ideal of R.

Exercise 13.

(a) Prove that a maximal ideal is prime.

(b) Let I be an ideal of R. Prove that I is prime if and only if R/I is an integral domain.

(c) Let I be an ideal of R. Prove that I is maximal if and only if R/I is a field.

(d) Let $\phi\colon R \to R'$ be a ring homomorphism, and let $I \subset R'$ be an ideal. Prove that $\phi^{-1}(I)$ is an ideal of R. (How does this relate to Exercise 12 above?)

(e) Let $\phi\colon R \to R'$ be a ring homomorphism, and let $P \subset R'$ be a *prime* ideal. Prove that $\phi^{-1}(P)$ is a prime ideal of R.

Exercise 14. Suppose R is a ring with exactly two ideals. Prove that R is a field.

Exercise 15.

(a) Prove that the maximal ideals of $\mathbb{Z}$ are the ideals (p) where p is a prime number. What are the prime ideals of $\mathbb{Z}$? (The answer is different!)

(b) What are the prime and maximal ideals in $\mathbb{C}[x]$?

(c) Consider the ring $\mathbb{R}[x]$. Like $\mathbb{C}[x]$, this ring is also a Euclidean domain, hence a PID and a UFD as well. However, its prime ideals are different from $\mathbb{C}[x]$. Describe the prime ideals of $\mathbb{R}[x]$.

(d) The rings $\mathbb{Z}[x]$ and $\mathbb{C}[x, y]$ are both UFDs, but not PIDs. Choose one, and prove that it is not a PID by finding an ideal which is not principal, and proving that it is such an example.

The next exercise introduces two kinds of ideals which I won't discuss much further in these notes, but which are good to know in general: primary ideals and the radical of an ideal. Primary ideals don't tend to feature on the qual, and when they do they are defined. There has been a qual question asking you to know the definition of the radical before.

Exercise 16. (August 2019 Problem 2) This problem involves ideals in a commutative ring (with unit). A proper ideal I is *primary* if whenever $ab \in I$ and $a \notin I$, then $b^n \in I$ for some $n > 0$. The radical of an ideal I, denoted $\sqrt{I}$, is the set $\sqrt{I} = \{f : f^n \in I \text{ for some } n > 0\}$.

(a) Prove that if I is primary, then $\sqrt{I}$ is prime.

(b) Is the ideal $J = (x^2, xy) \subset \mathbb{Q}[x, y]$ primary? Be sure to carefully justify your answer.

Exercise 17. Let $I = (r)$ be an ideal in a PID R.

(a) Prove that $\sqrt{I}$ is generated by the largest squarefree factor of r.

(b) **(August 2022 Problem 1 (b))** What is the radical of the ideal $(x^3 - x^2)$ in $\mathbb{R}[x]$?

The Isomorphism Theorems

In this section I'll recap the three basic isomorphism theorems in the context of commutative rings. There will be a similar section in the notes on modules and groups, for the correct statements in those contexts. (The statements below hold for non-commutative rings with every instance of "ideal" replaced by "two-sided ideal".)

I won't dwell long here, but I want to draw some attention to the following **Motto: the Isomorphism Theorems for a given algebraic object are analogs of the Rank-Nullity Theorem for vector spaces.** Vector spaces are very simple objects, there is really only one invariant a vector space has, its dimension, and any two vector spaces of the same dimension are isomorphic. The reason nobody ever talks about the isomorphism theorems for vector spaces is that often distinctions that hold when speaking of e.g. groups, rings, or modules will collapse down to statements about dimensions of vector spaces adding to the correct number. The isomorphism theorems below capture facts that are true for vector spaces, and indeed follow from the Rank-Nullity Theorem, but require greater nuance in other contexts

This highlights a strategy, which is perhaps not always helpful on the qual, but is often helpful when doing math. A very general way of thinking about algebra when you are stuck is to see if you can imagine what an algebraic statement would say if everything was a vector space. This doesn't always work, but it can be enlightening, and sometimes the isomorphism theorems will let you directly apply your reasoning from one domain to the other. In the notes about modules, we will see that Nakayama's lemma is another theorem that allows one to transfer information about vector spaces back to rings/modules.

Theorem (first isomorphism theorem)**.** Let $\phi\colon R \to S$ be a ring homomorphism. Then $\ker\phi$ is an ideal of R (see Exercise 12), $\operatorname{im}\phi$ is a subring of S, and the induced homomorphism $R/\ker\phi \to \operatorname{im}\phi$ is an isomorphism. In particular, if ϕ is surjective, then $S \cong R/\ker\phi$.

Theorem (second isomorphism theorem)**.** Let R be a ring, $S \subset R$ a subring, and $I \subset R$ an ideal. Then $S + I = \{s + i : s \in S,\ i \in I\}$ is a subring of R, I is an ideal of $S + I$, $(S + I)/I$ is a subring of R/I, $S \cap I$ is an ideal of S, and the composition $S \hookrightarrow R \twoheadrightarrow R/I$ induces an isomorphism $S/(S \cap I) \xrightarrow{\sim} (S + I)/I$.

Theorem (third isomorphism theorem)**.** Let R be a ring and I an ideal. Then if A is a subring of R such that $I \subset A \subset R$, then A/I is a subring of R/I (we have already used this in the previous isomorphism theorem). Furthermore, if J is an ideal of R such that $I \subset J \subset R$, then J/I is an ideal of R/I, and the composition $R \twoheadrightarrow R/I \twoheadrightarrow (R/I)/(J/I)$ induces an isomorphism $R/J \xrightarrow{\sim} (R/I)/(J/I)$.

Some ideal theory in noncommutative rings

For noncommutative rings like $M_2(\mathbb{C})$, we can also define ideals, but now there's a little rub: an ideal can have the absorbing property under left multiplication, under right multiplication, or under

both. These are called, respectively, left ideals, right ideals, and two-sided ideals. You can prove the analog of Exercise 12 by proving that the kernel of a homomorphism $R \to R'$ is a two-sided ideal of R.

The following exercise is here to give you some practice working with ideals in the most basic noncommutative rings.

Exercise 18. (ideals in matrix rings)

(a) **(August 2020 Problem 1 (c), August 2019 1 (a)** Let $R = M_2(\mathbb{C})$. Give an example of a left ideal that is not a right ideal. (In 2019, it was $R = M_2(\mathbb{Z})$, but same dif.)

(b) **(August 2022 Problem 1 (e))** How many two-sided ideals are there in $M_2(\mathbb{C})$? (The answer is going to be a small number.)

(c) **(January 2021 Problem 1 (b), August 2019 Problem 1 (b))** Let $R = M_2(\mathbb{Z})$. Give an example of a proper, non-zero, two-sided ideal.

Something that comes up for noncommutative rings that doesn't come up for commutative rings are simple rings. A **simple ring** is a ring with no proper, non-zero ideals. So, (spoilers) above you should have shown that $M_2(\mathbb{C})$ is simple. A commutative ring is simple if and only if it is a field, but for noncommutative rings there can be many examples of interesting simple rings.

Exercise 19. (January 2020 Problem 1 (a) and (b)) On this problem, no justification is required; only the answer will be graded. Let S_3 be the symmetric group on 3 letters, and let R be the group ring $\mathbb{Z}[S_3]$.

(a) Write down a nonzero element of R which is a zero-divisor.

(b) Write down an element in the center of R which is not in $\mathbb{Z}$.

A few caveats about ideals in noncommutative rings

In noncommutative rings, the definition of a prime ideal is somewhat modified: a proper two-sided ideal P is prime if whenever the product $AB \subset P$ for *ideals* A, B, we in fact have either $A \subset P$ or $B \subset P$. Equivalently, P is prime if whenever the product of principle (two-sided) ideals $(a)(b) \subset P$, then either $a \in P$ or $b \in P$.

Exercise 20.

(a) Prove that in a commutative ring, the two conditions in the preceding paragraph are equivalent to the usual definition of a prime ideal.

(b) Prove that in $M_2(\mathbb{C})$, the zero ideal is prime using the above definition, but is not prime using the definition for commutative rings. (Ideals in a noncommutative ring which satisfy the commutative definition of "prime" are sometimes called **completely prime ideals**.)

Quotient rings can only be constructed when I is a two-sided ideal. If I is one-sided, you can still construct R/I as an abelian group, but you won't be able to make the multiplication work. However, you should keep these kinds of quotients in mind, because later they will be important ways to construct modules over noncommutative rings.