PUMaC 2022* Power Round: The PID Structure Theorem

Frank Lu

Spring 2023

Rules and Reminders

1. Your solutions should be turned in by **12PM Thursday, March 30th, EDT**. You will submit the solutions through Gradescope. The instructions describing how to log into Gradescope will be sent to the coaches. The deadline for submission is clearly visible on the Gradescope site once you enroll in the course.

   Please make sure you submit your work in time. **No late submissions will be accepted.** Please do not submit your work using email or in any other way. If you have questions about Gradescope, please post them on Piazza.

   You may either typeset the solutions in LaTeX or write them by hand. We strongly encourage you to typeset the solutions. This way, the proofs end up being more clear and the chances are you will not lose points there. Moreover, you might want to use some of the LaTeX resources listed in point 2.

   In case your solutions are handwritten, the cover sheet (the last page of this document) should be the first page of your submission. In case you typeset your solutions, please take a look at the Solutions Template we posted and make sure to make the cover sheet the first page of your submission.

   Each page should have on it the **team number** (not team name) and **problem number**. This number can be found by logging in to the coach portal and selecting the corresponding team. Solutions to problems may span multiple pages. Please put them in order when submitting your solutions.

2. You are encouraged, but not required, to use LaTeX to write your solutions. If you submit your power round electronically, **you may submit several times, but only your final submission will be graded** (moreover, you may not submit any work after the deadline). The last version of the power round solutions that we receive from your team will be graded. Moreover, **you must submit a PDF**. No other file type will be graded. For those new and interested in LaTeX, check out Overleaf as well as its online guides. If you do not know the specific command for a math symbol, check out Detexify or TeX.StackExchange.

3. Do not include identifying information aside from your team number in your solutions.

4. Please collate the solutions in order in your submission. Each problem should start on a new page (there is a point deduction for not following this formatting).

5. On any problem, you may use without proof any result that is stated earlier in the test, as well as any problem from earlier in the test, even if it is a problem that your team has not solved. These are the **only** results you may use. In particular, to solve a problem, you may not cite the subsequent ones. You may not cite parts of your proof of other problems: if you wish to use a lemma in multiple problems, please reproduce it in each one.

6. When a problem asks you to "find", "find with proof," "show," "prove," "demonstrate," or "ascertain" a result, a formal proof is expected, in which you justify each step you take, either by using a method from earlier or by *proving* that *everything* you do is correct. When a problem instead uses the word "explain," an informal explanation suffices. When a problem instead uses the word "sketch" or "draw" a clearly marked diagram is expected.

7. All problems are numbered as "Problem x.y.z" where x.y is the subsection number and z is the the number of the problem within the subsection. Each problem's point distribution can be found in the cover sheet.

8. **You may NOT use any references, such as books or electronic resources, unless otherwise specified. You may NOT use computer programs, calculators, or any other computational aids.**

9. Teams whose members use English as a foreign language may use dictionaries for reference.

10. **Communication with humans outside your team of 8 students about the content of these problems is prohibited.**

11. There are two places where you may ask questions about the test. The first is Piazza. Please ask your coach for instructions to access our Piazza forum. On Piazza, you may ask any question **so long as it does not give away any part of your solution to any problem**. If you ask a question on Piazza, all other teams will be able to see it. If such a question reveals all or part of your solution to a power round question, your team's power round score will be penalized severely. For any questions you have that might reveal part of your solution, or if you are not sure if your question is appropriate for Piazza, please email us at pumac@math.princeton.edu. We will email coaches with important clarifications that are posted on Piazza.

Introduction and Advice

In this power round, we state and prove the **PID Structure Theorem**, before describing a few applications of this theorem. This theorem states that certain examples of a structure called a **module** satisfy nice properties. In order to state and prove the theorem, we first need to introduce a few more structures from abstract algebra. We first study rings, which are sets with addition and multiplication operations. This structure includes some familiar sets, such as the set of integers and the set of rational numbers. As we introduce new structures, we will slowly see, under certain conditions, that these structures satisfy nice properties.

The material in this power round belongs to the field of **abstract algebra,** which studies sets equipped with operations that obey certain properties. A large part of the difficulty of this subject arises from the abstraction and the amount of generality present (in contrast with the computation-heavy and concrete world of high school algebra and geometry). Try to keep in mind the examples introduced throughout the power round, and checking the definitions and propositions against these examples. This will be useful in understanding what each of these otherwise abstract statements are saying.

Here is some further advice with regard to the Power Round:

- **Read the text of every problem!** Many important ideas are included in problems and may be referenced later on. In addition, some of the theorems you are asked to prove are useful or even necessary for later problems.
- **Make sure you understand the definitions**. A lot of the definitions are not easy to grasp; don't worry if it takes you a while to fully understand them. If you don't, then you will not be able to do the problems. Feel free to ask clarifying questions about the definitions on Piazza (or email us).
- **Don't make stuff up**: on problems that ask for proofs, you will receive more points if you demonstrate legitimate and correct intuition than if you fabricate something that *looks* rigorous just for the sake of having "rigor."
- **Check Piazza often!** Clarifications will be posted there, and if you have a question it is possible that it has already been asked and answered in a Piazza thread (and if not, you can ask it, assuming it does not reveal any part of your solution to a question). **If in doubt about whether a question is appropriate for Piazza, please email us at pumac@math.princeton.edu.**
- **Don't cheat**: as stated in Rules and Reminders, you may **NOT** use any references such as books or electronic resources. If you do cheat, you will be disqualified and banned from PUMaC, your school may be disqualified, and relevant external institutions may be notified of any misconduct.

Good luck, and have fun!

– Frank Lu

We would like to acknowledge and thank many individuals and organizations for their support; without their help, this Power Round (and the entire competition) could not exist. Please refer to the solutions of the power round for full acknowledgments and references.

Contents

Notation

- $\forall$: for all. *Ex.:* $\forall x \in \{1,2,3\}$ *means "for all* x *in the set* $\{1,2,3\}$*"*
- $A \subset B$: proper subset. *Ex.:* $\{1,2\} \subset \{1,2,3\}$*, but* $\{1,2\} \not\subset \{1,2\}$
- $A \subseteq B$: subset, possibly improper. *ex.:* $\{1\}, \{1,2\} \subseteq \{1,2\}$
- $f : x \mapsto y$: f maps x to y. *Ex.: if* $f(n) = n - 3$ *then* $f : 20 \mapsto 17$ *and* $f : n \mapsto n - 3$ *are both true.*
- $f(C)$: for a function $f : A \to B$ and subset $C \subseteq A$, the set of elements of the form $f(c)$, for $c \in C$.
- $\{x \in S : C(x)\}$: the set of all x in the set S satisfying the condition $C(x)$. *Ex.:* $\{n \in \mathbb{N} : \sqrt{n} \in \mathbb{N}\}$ *is the set of perfect squares.*
- $\mathbb{N}$: the natural numbers, $\{1,2,3,\dots\}$.
- $[n] = \{1,2,3,...,n\}$.
- $\mathbb{Z}$: the integers.
- $\mathbb{Q}$: the rational numbers.
- $\mathbb{R}$: the real numbers.
- $\mathbb{C}$: the complex numbers.
- $|S|$: the cardinality of set S.

1 Rings and Fields

In this section, our goal is to introduce some structures which generalize some of the key features that we like from some familiar objects. The main example to motivate our discussion is the set of integers $\mathbb{Z}$. In particular, we can add and subtract integers, as well as multiply them together. It is these operations and certain nice properties that they satisfy which we would like to capture.

1.1 Rings and Ideals

We begin with the concept of a ring, which generalizes the concept of the integers $\mathbb{Z}$ with its addition and multiplication operations.

Definition 1.1.1. A **ring** is a set R equipped with two operations, $+$ and $\cdot$, satisfying the following conditions:

1. R is closed under $+$ and $\cdot$: that is, $\forall r_1, r_2 \in R$, $r_1 + r_2, r_1 \cdot r_2 \in R$.
2. The operations $+, \cdot$ are associative: $\forall r_1, r_2, r_3 \in R$, we have that $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3), r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$.
3. The operations $+, \cdot$ are commutative: $\forall r_1, r_2 \in R$, $r_1 + r_2 = r_2 + r_1$ and $r_1 \cdot r_2 = r_2 \cdot r_1$.
4. The operations $+, \cdot$ have identity elements: specifically, we have elements $0, 1 \in R$ such that $0 + r = r = 1 \cdot r = \forall r \in R$. We refer to 0 as the **additive identity** of R and 1 as the **multiplicative identity** of R.
5. For each element $r \in R$, there is an element $r' \in R$ such that $r + (r') = 0$. This element r' is the **additive inverse** of r; we will sometimes write r' as $-r$.
6. We have the following distributive law: $\forall r_1, r_2, r_3 \in R$, we have $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$.

A **subring** of a ring R is a subset S of R that is a ring, using the same operations $+, \cdot$ as R.

Remark. Sometimes we will have more than one ring that we will be concerned with. In that case, for the sake of clarity, we will use $+_R$ and $\cdot_R$ to represent the addition and multiplication operations for the ring R. In cases where which ring we are working with is clear, for the sake of notational simplicity, we will write $r_1 \cdot r_2$ as just $r_1 r_2$.

Similarly, we will write $0, 1$ to denote the additive and multiplicative identities of our ring, with subscripts to indicate which ring we are referring to when it isn't clear from context.

Example. We check that $\mathbb{Z}$ is a ring, using the standard addition and multiplication rules. Note that the sum of two integers and the multiplication of two integers is also an integer. Furthermore, we know that addition and multiplication are associative and commutative. The additive identity is 0 and the multiplicative identity is 1.

We observe as well that the additive inverse of an integer is its negative. Finally, we know that addition and multiplication satisfy the distributive law.

Remark. With the above example, we can see how some of the key features of the addition and multiplication operations in $\mathbb{Z}$ are captured in the above definition of a ring. It will be useful throughout this section to think about $\mathbb{Z}$ when presented with a new example; we will sometimes also explicitly relate the examples to the ring $\mathbb{Z}$ throughout the power round.

In addition to the above example, $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all rings; you may assume that these are rings without proof, with the standard addition and multiplication rules. When we write one of the above symbols and refer to the corresponding ring, unless otherwise stated, the addition and multiplication rules we are using are the standard addition and multiplication rules.

We present an example of a ring that is not one of the above rings.

Example. We will show that $\mathbb{Z}[\sqrt{2}]$, the set of real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Z}$, is a ring, under the normal addition and multiplication rules. We know from the properties of addition and multiplication of real numbers that properties 2, 3, and 6 hold. We just need to verify properties 1, 4, 5.

To show property 1, if we are given two elements $r_1, r_2 \in \mathbb{Z}[\sqrt{2}]$, we know by definition that there exist integers a_1, b_1 and a_2, b_2 such that $r_1 = a_1 + b_1\sqrt{2}$ and $r_2 = a_2 + b_2\sqrt{2}$. Then, we find that $r_1 + r_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Furthermore, $r_1 r_2 = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$, which again lies in $\mathbb{Z}[\sqrt{2}]$. This shows the first property holds.

For property 4, note that the identity elements for addition and multiplication over $\mathbb{R}$, which are 0 and 1, respectively, lie in $\mathbb{Z}[\sqrt{2}]$, and so $\mathbb{Z}[\sqrt{2}]$ also contains identity elements for addition and multiplication.

Finally, for property 5, given any element $r \in \mathbb{Z}[\sqrt{2}]$, we know that it takes the form $a + b\sqrt{2}$ for some integers a, b. But then the value $r' = (-a) + (-b)\sqrt{2}$ also lies in $\mathbb{Z}[\sqrt{2}]$, and the sum $r' + r$ yields 0. We have thus shown that $\mathbb{Z}[\sqrt{2}]$ is a ring.

Problem 1.1.1. Here are some more examples, and a non-example, of rings:

1. Show that $2\mathbb{Z}$, the set of even integers, is not a ring. (Hint: which property does it fail? In general, for questions of this nature, it is helpful to go through the properties and figure out which ones are or are not satisfied).
2. Show that $\mathbb{C}[x]$, the set of polynomials in one variable x with complex coefficients, is a ring (under the standard addition and multiplication operations of polynomials)
3. Show that the subset of polynomials in $\mathbb{C}[x]$ whose x coefficient is 0 forms a ring (with the same addition and multiplication as for $\mathbb{C}[x]$).

We also have the following example of a ring. Keep this example in mind as you go through the rest of this section.

Problem 1.1.2. Let $\mathbb{Z}/n\mathbb{Z}$ be the set of remainders of integers upon division by n, where addition and multiplication are defined modulo n. For instance, when $n = 6$, we have that $4 + 5 = 3$, and $4 \cdot 5 = 2$. Prove that this is a ring.

Using the above definition of a ring, we can already prove some basic properties. For instance, we have the following elementary proposition.

Proposition 1.1.2. *Let R be a ring, with additive identity 0 and multiplicative identity 1.*

1. *There exists exactly one element $e \in R$ so $e + r = r \ \forall r \in R$, namely $e = 0$, and there is exactly one element $i \in R$ so $ir = r \ \forall r \in R$, namely $i = 1$. In other words, the additive and multiplicative identity elements are unique.*

2. *For all $r \in R$, $0r = 0$.*

Proof. To prove the first property, suppose there were two elements e, e' such that $e + r = r = e' + r$ for all $r \in R$. Then, observe that $e + e' = e'$, using the left equation, but $e + e' = e' + e = e$, using the right equation. Therefore, $e = e'$, and there is only one additive identity.

Similarly, suppose there were two elements i, i' so that $ir = r = i'r$ for all $r \in R$. Then, we know that $ii' = i'$, from the left equation, but $ii' = i'i = i$ from the right equation, so again $i = i'$, and there is only one multiplicative identity.

To prove the second property, we observe that for each $r \in R$, $0r + 0r = (0 + 0)r = 0r$. Therefore, adding to both sides of the equation the additive inverse of $0r$ yields us that $0r = 0$, which is what we wanted to show. □

Problem 1.1.3. Given a ring R, show that there exists an element $x \in R$ such that for all $r \in R$, $r + xr = 0$. What element is this?

One of the first things we wish to generalize is the notion of divisibility in $\mathbb{Z}$. In particular, we can consider in $\mathbb{Z}$ subsets that are given as multiples of a given integer. We will begin with something which captures some of the most basic properties about these sets; a more precisely analogous concept will be introduced later.

Definition 1.1.3. An **ideal** of a ring R is a nonempty subset $I \subseteq R$ such that the following properties hold:

1. I is closed under addition. That is, for $i, i' \in I$, we have $i + i' \in I$.

2. For every $i \in I$ and $r \in R$, we have that $ri \in I$.

A **proper ideal** of a ring R is an ideal I that is not equal to R itself.

Example. We show that the set of even integers is an ideal in the ring $\mathbb{Z}$. To see this, recall that the set of even integers are all the integers that can be written as $2n$, for some integer $n \in \mathbb{Z}$. Property 1 follows since for any r, r' even integers, we know that there exist integers n, n' so $r = 2n, r' = 2n'$, and so $r + r' = 2(n + n')$, which is again even.

For the second property, given an even integer i, we can write it as $i = 2n$ for some integer n. But then for any integer r, we have that $ri = r2n = 2(nr)$, which is again an even integer.

Problem 1.1.4. Show that the set of odd integers, as a subset of $\mathbb{Z}$, is not an ideal. (Hint: which property does this set not satisfy?)

Sometimes, we want to specify an ideal of R without having to explicitly list all of the elements. In particular, we only need to specify a subset of the elements of the ideal, knowing that our ideal satisfies the properties in the definition. For instance, note that any ideal that contains 2 also must contain the even integers.

Indeed, note that if 2 lies in an ideal I, then so does every even integer, since each even integer is equal to 2 times some other integer. As the even integers are an ideal, it thus makes sense to describe the ideal of even integers as the smallest ideal that contains 2 : that is, every other ideal containing 2 contains the even integers, and the even integers are precisely the set of integers which are a multiple of 2.

These notions, of each even integer being a multiple of 2, and of the even integers being the smallest such ideal containing 2, motivates the notion of generators of an ideal.

Definition 1.1.4. We say that an ideal I is generated by a subset of elements $S \subset I$ if every element $i \in I$ can be written in the form $i = \sum_{j=1}^{n} r_j s_j$, for some positive integer n, and elements $s_1, s_2, \ldots, s_n \in S$ and $r_1, r_2, \ldots, r_n \in R$.

Similarly, given a ring R and elements $s_1, s_2, \ldots, s_n$, we let $\langle s_1, s_2, \ldots, s_n \rangle$ be the set of elements of the form $i = \sum_{j=1}^{n} r_j s_j$ for elements $r_1, r_2, \ldots, r_n \in R$. We can also substitute a set, letting $\langle S \rangle$ be the set of elements in R of the form $i = \sum_{j=1}^{n} r_j s_j$ for some positive integer n, and elements $s_1, s_2, \ldots, s_n \in S$, $r_1, r_2, \ldots, r_n \in R$.

With the notation above, the set of even integers, $2\mathbb{Z}$, can also be written as $\langle 2 \rangle$. Note that the set of even integers is an ideal. This happens more generally, as follows.

Proposition 1.1.5. *Given a subset $S \subset R$, the set $\langle S \rangle$ is an ideal.*

Proof. For the first condition, suppose that we have two elements in $\langle S \rangle$, say i and i'. Then, there are positive integers n, m and elements $s_1, s_2, \ldots, s_n, s'_1, s'_2, \ldots, s'_m \in S$ and $r_1, r_2, \ldots, r_n, r'_1, r'_2, \ldots, r'_m \in S$ such that $i = \sum_{j=1}^{n} r_j s_j$ and $i' = \sum_{j=1}^{m} r'_j s'_j$. Then, their sum is equal to $i + i' = \sum_{j=1}^{n} r_j s_j + \sum_{j=1}^{m} r'_j s'_j$, which is of the given form. Notice that we can further simplify this expression if we know that some of the s_j and s'_j are equal, using the distributive property.

For the second condition, given an element i in $\langle S \rangle$, we can write it as $\sum_{j=1}^{n} r_j s_j$ for some positive integer n, $s_1, s_2, \ldots, s_n \in S$ and $r_1, r_2, \ldots, r_n \in R$. But then, for each element $r \in R$, observe that $ri = \sum_{j=1}^{n} r r_j s_j$, which is also in $\langle S \rangle$. This finishes the proof of the proposition. □

Definition 1.1.6. We call the set $\langle S \rangle$ the **ideal generated by** S.

We now wish to generalize the notion of a prime from $\mathbb{Z}$. Rather than thinking about elements as being primes, we want to think about ideals. The main behavior we want to capture is the fact that, given a prime number p, if ab lies in $p\mathbb{Z}$, then either a or b lies in it. Contrast this with $6\mathbb{Z}$, for instance: $2 \cdot 3$ lies in $6\mathbb{Z}$, but $2, 3$ do not lie in $6\mathbb{Z}$.

Definition 1.1.7. An ideal I of a ring R is said to be **prime** if it is a proper ideal, and furthermore, for all $a, b \in R$, $ab \in I$ implies that either $a \in I$ or $b \in I$.

For instance, the ideal $\langle 2 \rangle \subset \mathbb{Z}$ is a prime ideal, since $ab \in \langle 2 \rangle$ if and only if ab is an even integer; but notice that one of a, b must be even as well.

Problem 1.1.5. Determine, with proof, all the prime ideals of $\mathbb{C}[x]$. You may use, without proof, the following theorem: any nonconstant polynomial in $\mathbb{C}[x]$ can be written as a product of linear factors, and this product is unique up to the order of the linear factors. This theorem is also known as the Fundamental Theorem of Algebra.

We finish by considering functions between rings. To do this, we have the following definition relating functionss between sets.

Definition 1.1.8. Given a function $f : S \to S'$, where S, S' are sets, we say that f is **injective** if $f(s) = f(t)$ implies that $s = t$ for any $s, t \in S$.

We say that f is **surjective** if for all $s' \in S'$, there exists an $s \in S$ so $f(s) = s'$, and **bijective** if it is both injective and surjective.

For instance, treating all the following as functions from $\mathbb{R}$ to $\mathbb{R}$, the function $f(x) = x^3$ is injective and surjective, the function $g(x) = 2^x$ is injective but not surjective, and the function $f(x) = x^3 - x$ is surjective but not injective. Note that the specification of the set S' is important: the function $g(x) = 2^x$ is surjective when viewed as a function from $\mathbb{R}$ to $\{x \in \mathbb{R} | x > 0\}$.

Problem 1.1.6. For each of the functions below, state whether they are injective, surjective, both, or neither.

1. The function $f(x) = |x|$ from the set of negative real numbers to the set of positive real numbers.
2. The function $f(x) = e^x$ from $\mathbb{R}$ to $\mathbb{R}$.
3. The function $f(x) = \sin x$ from $[0, 2\pi]$ to $[-1, 1]$.

Definition 1.1.9. Given a function $f : S \to S'$, an **inverse** of f is a function $g : S' \to S$ such that $f(g(s')) = s'$ for all $s' \in S'$, and $g(f(s)) = s$ for all $s \in S$.

We have the following proposition, which you may assume to be true without proof.

Proposition 1.1.10. *A function has an inverse if and only if it is injective and surjective. If a function has an inverse, this inverse is unique.*

We can now introduce our notion of maps (which is another word for "function") between rings.

Definition 1.1.11. A **ring homomorphism** between rings R and S is a map $\phi : R \to S$ such that the following holds:

1. For all $r, r' \in R$, we have $\phi(r +_R r') = \phi(r) +_S \phi(r')$ and $\phi(r \cdot_R r') = \phi(r) \cdot_S \phi(r')$.
2. $\phi(1_R) = 1_S$.

If this map is bijective, we say that it is a **ring isomorphism,** and then we say that R, S are isomorphic.

The notion of two rings being isomorphic essentially means that two rings are the "same;" that is, you can go from one to the other simply by relabelling the elements.

As a simple example, the function $\mathbb{Z} \to \mathbb{Q}$ sending $n \in \mathbb{Z}$ to itself, is a ring homomorphism. This is injective but not surjective. We also have a ring isomorphism ϕ from $\mathbb{Z}[\sqrt{2}]$ to itself that sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$. One can check that the properties of a ring homomorphism hold for this function: for instance, we notice that $\phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2}) = (a + c) - (b + d)\sqrt{2} = \phi((a + c) + (b + d)\sqrt{2})$.

1.2 A Family of Rings

We are now interested in a variety of different types of rings.

Definition 1.2.1. A **field** is a ring R such that every nonzero element $r \in R$ has a multiplicative inverse; that is, for each nonzero $r \in R$, there is an element $s \in R$ such that $rs = 1$.

For instance, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields; you may assume this fact without proof.

Problem 1.2.1. Show that the set of real numbers $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$, forms a field, under the normal rules of addition and multiplication in $\mathbb{R}$.

Problem 1.2.2. Show that a ring R is a field if and only if it has exactly two ideals. Which two ideals are these? (Hint: think about the second question first. Consider the field of rational numbers $\mathbb{Q}$. What are its ideals?).

Of course, not all rings are fields, such as $\mathbb{Z}$. However, $\mathbb{Z}$ still has some properties that distinguish it from other rings. In particular, it is the following type of ring.

Definition 1.2.2. A **integral domain** is a ring R such that for any $a, b \in R$, $ab = 0$ if and only if one of a, b is zero.

Another example of such a ring is $\mathbb{C}[x]$. One can check that the product of two polynomials is zero if and only if one of the polynomials is zero.

However, not all rings are integral domains. For instance, consider $\mathbb{Z}/4\mathbb{Z}$, where addition and multiplication are done modulo 4. One can verify that this is a ring. Then, notice that $2 \cdot 2 = 0$, but $2 \neq 0$, so this ring is not an integral domain.

We are also interested in rings with particular finiteness properties, with regards to ideals. This motivates the definitions below.

Definition 1.2.3. A **principal ideal domain**, or a PID, is an integral domain such that every ideal can be generated by one element.

Problem 1.2.3. Show that $\mathbb{Z}$ is a PID. As a hint, given any ideal I of $\mathbb{Z}$, consider the smallest positive element in I, say i. Show that every element in the ideal has to be divisible by i.

Remark. In particular, notice that this shows that the only ideals of $\mathbb{Z}$ are the zero ideal (the ideal consisting only of the element 0) and $n\mathbb{Z}$, the set of elements divisible by a positive integer n.

As another example, it turns out that for any field k, we have that $k[x]$, the set of polynomials with coefficients in k, is a PID. Here, we take our addition operation and multiplication operations to be the typical addition and multiplication of two polynomials:

$$\sum_{i=1}^{n} a_i x^i + \sum_{i=1}^{n} b_i x^i = \sum_{i=1}^{n} (a_i + b_i) x^i,$$

and

$$\sum_{i=1}^{n} a_i x^i \cdot \sum_{i=1}^{n} b_i x^i = \sum_{j=1}^{2n} \sum_{k=1}^{n} (a_k b_{j-k}) x^i,$$

where $a_i = b_i = 0$ for i not equal to $1, 2, \ldots, n$. You may use the following theorem without proof.

Theorem 1.2.4. *Given a field k, the ring $k[x]$ is a PID.*

Besides ideals being prime, in $\mathbb{Z}$ we also have the notion of prime elements. There are two properties of primes which seem familiar, but are slightly different. First, note that a prime number cannot be decomposed into a product of two other numbers, where neither is $1, -1$. The second is that if p divides a product of positive integers, then p divides one of the positive integers.

In $\mathbb{Z}$, an element satisfies one property if and only if it satisfies the other. In general, however, we cannot assume this. As such, we have the following definition.

Definition 1.2.5. Given a ring R, a **unit** is an element $u \in R$ with a multiplicative inverse.

An element $r \in R$ is **irreducible** if it cannot be written as the product of two elements in the ring, neither of which are units, and furthermore is not a unit itself.

An element $r \in R$ is **prime** if it is nonzero and the ideal generated by r is prime.

Example. For instance, the prime numbers in $\mathbb{Z}$ are prime in the sense of the above definition. To prove this, given a prime number p, suppose that we have integers $a, b \in \mathbb{Z}$ such that $ab \in \langle p \rangle$. In other words, p divides ab. But we know by the Fundamental Theorem of Arithmetic that this means that p appears in the prime factorization of ab, and thus of either a or b.

The more traditional definition of a prime in $\mathbb{Z}$, that a prime is divisible by only 1 or itself, shows that all the prime numbers are irreducible as well.

However, we note that 4 is not prime: for instance, $2 \cdot 2$ lies in $\langle 4 \rangle$, but 2 does not.

Finally, we observe the only units in $\mathbb{Z}$ are $1, -1$.

Problem 1.2.4. Show that for any integral domain R, every prime element is irreducible.

Recall that we can uniquely factor integers into primes, up to ordering of the primes. However, not all rings have this property. This suggests the following category of ring which we'd like to consider.

Definition 1.2.6. A **unique factorization domain**, or UFD, is an integral domain where every nonzero element can be uniquely written as a product of irreducible elements and a unit, up to the order of irreducible elements and unit multiples.

For instance, $\mathbb{Z}$ is a UFD; this is the condition that lets us perform prime factorization, and this factorization is unique up to ordering of the primes and choice of signs on the primes. In fact, we can say something more general. We present the following theorem, which you may use throughout this power round without proof.

Theorem 1.2.7. *Every PID is a UFD, and in every UFD, every irreducible element is also prime.*

However, we have the following non-example of a UFD.

Problem 1.2.5. Show that the set of elements $\mathbb{Z}[\sqrt{-13}]$, of the form $a + b\sqrt{-13}$, for $a, b \in \mathbb{Z}$, while an integral domain, is not a UFD, and therefore not a PID.

1.3 Product Rings, Quotient Rings and More Examples

In this subsection, we introduce two important constructions with regards to rings, before proceeding with some explicit examples of rings.

Definition 1.3.1. Given two rings R and S, their **product** $R \times S$ is the set of pairs (r, s), where $r \in R, s \in S$. We can then define the addition and multiplication operations by $(r, s) + (r', s') = (r +_R r', s +_S s')$ and $(r, s) \cdot (r', s') = (r \cdot_R r', s \cdot_S s')$. Recall here that $+_R, \cdot_R$ are the addition and multiplication operations on R, and $+_S, \cdot_S$ are the addition and multiplication operations on S.

Example. For instance, consider the product of the rings $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. The addition and multiplication tables for this ring are given below:

$+$	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(0, 2)	(0, 0)	(0, 1)

$\cdot$	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 2)	(0, 0)	(0, 1)	(0, 2)
(0, 2)	(0, 0)	(0, 2)	(0, 1)	(0, 0)	(0, 2)	(0, 1)
(1, 0)	(0, 0)	(0, 0)	(0, 0)	(1, 0)	(1, 0)	(1, 0)
(1, 1)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(1, 2)	(0, 0)	(0, 2)	(0, 1)	(1, 0)	(1, 2)	(1, 1)

One can show that this is a ring; for the purposes of this power round, you may assume this to be true.

Definition 1.3.2. Given a ring R, let $r \in R$ and I be an ideal of R. Let $r + I$ be the set of elements of the form $r + i$, for $i \in I$, and let R/I be the set $\{r + I | r \in R\}$. Then, on this set, define the sum as $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ and the product as $(r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I$.

Example. For instance, consider the ring $\mathbb{Z}$. Note that $3\mathbb{Z}$ is an ideal. Then,

$$0 + 3\mathbb{Z} = \{0, 3, -3, 6, -6, \ldots\},$$

and similarly $1 + 3\mathbb{Z} = \{1, 4, -2, 7, -5, \ldots\}$ and $2 + 3\mathbb{Z} = \{2, 5, -1, 8, -4, \ldots\}$.

First, we need to verify that these operations are well-defined: that is, if we pick a different choice of r' such that $r' + I = r + I$, then the result of the operation should still be the same. In particular, notice that for any $i \in I$, $r + I = (r + i) + I$.

Problem 1.3.1. Prove that the operations are well-defined. That is, if $r_1' + I = r_1 + I$ and $r_2' + I = r_2 + I$, then

$$(r_1 + I) + (r_2 + I) = (r_1' + I) + (r_2' + I)$$

and

$$(r_1 + I) \cdot (r_2 + I) = (r_1' + I) \cdot (r_2' + I).$$

Remark. Note that it is important that we check that this operation is well-defined. Sometimes we want to define an operation that has certain nice properties. However, it is not always clear that such an operation exists. In particular, we should expect to get the same result if we apply the same input, regardless of how we describe that input.

As a non-example, note that the "numerator" of a rational number is not well-defined. The number 0.5 could have numerator 1 (from the fraction 1/2), or numerator 8 (from 8/16). This is a problem, since then this function is not actually a function of the number itself, but rather how we write it. Similarly, we need to check in the above problem that our operations are actually operations that depend only on the sets $r + I$, not on which r we used to represent it.

Now, we claim that this is a ring.

Problem 1.3.2. Prove that R/I is a ring, equipped with the operations we defined above.

We call this ring a **quotient ring** of R. For instance, the set of residues $\pmod m$, for any positive integer m, is a quotient ring, given by $\mathbb{Z}/\langle m\rangle$. One can show that $\mathbb{Z}/m\mathbb{Z}$ can be thought of as the quotient of $\mathbb{Z}$ by the ideal $m\mathbb{Z} = \langle m\rangle$, explaining the notation. You may use this fact without proof throughout the rest of the power round.

We now aim to prove the following theorem.

Problem 1.3.3. Let R be a ring, and let I_1, I_2 be two ideals of R, such that $I_1 + I_2 = \{i_1 + i_2 | i_1 \in I_1, i_2 \in I_2\} = R$.

1. Show that $I_1 \cap I_2$ is an ideal.
2. Consider the homomorphism from $R/(I_1 \cap I_2)$ to $(R/I_1) \times (R/I_2)$ that sends $r + I_1 \cap I_2$ to $(r + I_1, r + I_2)$. Show that this map is well-defined and indeed a homomorphism.
3. Prove that the above map is injective.
4. Prove that the above map is surjective. As a suggestion on where to start, try considering any pair $(r_1 + I_1, r_2 + I_2)$, and the fact that $1 \in R = I_1 + I_2$.

This is known as the **Chinese Remainder Theorem** for rings. This is related to the case of Chinese Remainder Theorem for the integers.

Problem 1.3.4. Using the previous problem, derive the Chinese Remainder Theorem for integers. Namely, show that, given relatively prime integers m, n, show that given residues $r_1 \pmod m$ and $r_2 \pmod n$, there exists a unique residue $r \pmod{mn}$ so $r \equiv r_1 \pmod m$ and $r \equiv r_2 \pmod n$.

2 Vector Spaces

We now foray into a brief introduction into the subject of linear algebra, and the study of **vector spaces.** As we shall see, these structures are comparatively easy to classify.

2.1 Definitions

We begin by introducing our object of study.

Definition 2.1.1. Given a field k, a **vector space** V over the field k is a set of elements, which we call **vectors,** equipped with two operations, addition $+ : V \times V \to V$ and scalar multiplication $\cdot : k \times V \to V$, satisfying the following properties:

1. V is closed under $+$ and $\cdot$: that is, $\forall v_1, v_2 \in V$, $v_1 + v_2 \in V$, and for all $s \in k, v \in V$, we have $s \cdot v \in V$.

2. The operations $+, \cdot$ are associative: $\forall v_1, v_2, v_3 \in V$, we have that $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$, and for $s_1, s_2 \in k$ and $v \in V$, we have $s_1 \cdot (s_2 \cdot v) = (s_1 \cdot_k s_2) \cdot v$.
3. The operation $+$ is commutative.
4. The operation $+$ has an identity element, which we denote as 0.
5. Each element $v \in V$ has an additive inverse.
6. For all $v \in V$, $1_k \cdot v = v$.
7. We have the following distributive laws: $\forall s \in k$ and $v_1, v_2 \in V$, we have $s \cdot (v_1 + v_2) = s \cdot v_1 + s \cdot v_2$, and for all $s_1, s_2 \in k$ and $v \in V$, we have $(s_1 + s_2) \cdot v = s_1 \cdot v + s_2 \cdot v$.

Again, we sometimes omit the multiplication dot, and add subscripts to the operations as needed; the same convention will apply to other structures as well (when we introduce modules in the next section).

We also say that V in this case is an $k-$vector space. A **subspace** of V is a subset U that is also a vector space under the same operations as that of V.

Example. Consider the set of $(x_1, x_2, \ldots, x_n)$ of real numbers. We equip it with coordinate-wise addition and scalar multiplication, by $(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ and $r \cdot (x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n)$. We show that this forms a vector space over $\mathbb{R}$. We first observe that for tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$, we have that their sum is $(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ is also a tuple of real numbers (as the real numbers are closed under addition). Similarly, given $r \in \mathbb{R}$ and a tuple $(x_1, x_2, \ldots, x_n)$, we have that $r \cdot (x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n)$ is a tuple of real numbers (real numbers are closed under addition).

The commutativity, associativity, and distributivity properties are given from those of addition and multiplication over $\mathbb{R}$. Indeed, from the fact that these operations are defined on each coordinate, properties 2, 3, 7 hold if they hold for each coordinate, which is the case because these properties hold for $\mathbb{R}$.

To show identity element, we note that $(0, 0, \ldots, 0)$ is the identity element (since adding this to any tuple doesn't change any of the coordinates), and we observe that negating each of the entries of any tuple yields its additive inverse. Finally, property 6 follows since $1 \cdot (x_1, x_2, \ldots, x_n) = (1 \cdot x_1, 1 \cdot x_2, \ldots, 1 \cdot x_n) = (x_1, x_2, \ldots, x_n)$. This gives us that this is a vector space.

We denote the vector space above as $\mathbb{R}^n$. By the same reasoning, we have that $\mathbb{Q}^n, \mathbb{C}^n$ (defined analogously) are vector spaces (and more generally k^n for any field k) for $n \in \mathbb{N}$.

Here are some other examples of vector spaces.

Problem 2.1.1. Prove the following spaces are vector spaces.

1. The set of polynomials with complex coefficients (with the standard addition and multiplication operations), over the field $\mathbb{C}$.
2. $\mathbb{R}$, (with standard addition and multiplication operations), over the field $\mathbb{Q}$.

Here's an interesting non-example.

Problem 2.1.2. Determine all possible fields k such that $\mathbb{Z}$ can be made into a vector space over k, using the standard addition operations. In particular, you'll need to consider all possible scalar multiplication operations.

2.2 Coordinates and Bases

Throughout this section, we will fix a vector space V over a field k.

Definition 2.2.1. A **linear combination** of $v_1, v_2, \ldots, v_n \in V$ is an expression of the form $\sum_{i=1}^{n} s_i v_i$, where $s_i \in k$. By convention we say that we can take $n = 0$; in this case this is an empty sum, which we set to equal zero.

A **spanning set** is a set S such that every element can be written as a linear combination of some finite subset of S. We say that a module is **finite dimensional** if it has a finite spanning set, and **infinite dimensional** otherwise.

A set of elements of M is **linearly independent** if, for every finite subset of M, the only linear combination of these elements that equals zero is the linear combination where all of the coefficients s_i are 0. Notice that if M is finite then it suffices to check the above condition at the set M. By convention we say that the empty set is a linearly independent set.

A set of elements of V is said to be a **basis** if it is linearly independent and a spanning set.

Example. For instance, in the space of polynomials of degree at most 2 with coefficients in $\mathbb{C}$, the polynomials $1, x, x^2$ are a basis. Indeed, they are linearly independent, since if $a + bx + cx^2 = 0$ as polynomials, where $a, b, c \in \mathbb{C}$, then $a = b = c = 0$. Furthermore, every polynomial of degree at most 2, by definition, can be written in the form $a + bx + cx^2$, and so these elements $1, x, x^2$ are a basis.

As another example, note that $1+x, x^2, 2x^2+x+1$ is not a basis, since they are linearly dependent. Indeed, $2x^2 + x + 1 + (-2)x^2 + (-1)(x + 1) = 0$.

Problem 2.2.1. Find two distinct bases (the plural of basis) for the vector space of polynomials with real coefficients of degree at most 3, and prove they are bases.

Our main goal for this subsection is to prove that every finite dimensional vector space indeed has a basis, and in fact the length of this basis is the same, for a given vector space V. From here on out, assume that we are working within a given finite dimensional vector space V.

We begin by trying to compare the lengths of spanning sets and linearly independent sets. To do this, consider the following properties of spanning sets.

Problem 2.2.2. Suppose that S is a spanning set, and v is a vector that doesn't lie in S.

1. Show that $S \cup \{v\}$ is linearly dependent.
2. Suppose furthermore that v is nonzero. Then, show there exists a vector $w \in S$ such that $(S - \{w\}) \cup \{v\}$ is a spanning set.

From here, we consider the following procedure. Start with a linearly independent set L and a spanning set S; by assumption, we know that we can pick a spanning set S that is finite. We now consider replacing vectors in S with those that are in L.

Problem 2.2.3. Show that if $L \not\subseteq S$, we can replace a vector in S with one in L so that S remains a spanning set, and $S \cap L$ increases in size by one.

Problem 2.2.4. Using the above procedure, show that L must be finite, and that L must have at most as many elements as S. Conclude that the size of every linearly independent set is at most the size of every spanning set.

Using this size comparison, we are now ready to construct a basis for our vector space, and show they have the same size. The first result allows us to state that every vector space has a basis.

Problem 2.2.5. Prove the following.

1. Any spanning set with finitely many elements can be reduced to a basis. That is, we may remove elements from our spanning set such that the resulting set is a basis.
2. Any linearly independent set can be extended to a basis. That is, we may add elements to our linearly independent set so that the resulting set is a basis.

We are now ready to state the main result.

Problem 2.2.6. Show that any two bases of our finite dimensional vector space have the same size. This size is known as the **dimension** of the vector space, denoted as $\dim V$.

For instance, one can check that $\mathbb{R}^n$, as a vector space over $\mathbb{R}$, has dimension n (you may assume this throughout the rest of the power round). Similarly, the space of polynomials, with coefficients in $\mathbb{C}$, with degree at most 2, is a vector space with dimension 3, as we saw previously with this space having basis $1, x, x^2$.

Problem 2.2.7. Show that if W is a subspace of V, then the dimension of W is at most that of V.

2.3 Linear Transforms

Now that we've discussed vector spaces, we can consider maps between vector spaces. Just like with rings, we consider a special type of map between vector spaces that are **linear.**

Definition 2.3.1. A **linear transformation** between two vector spaces V, W over a common field k is a map $T : V \to W$ satisfying the following conditions:

1. For all vectors $v_1, v_2 \in V$, we have $T(v_1 + v_2) = T(v_1) + T(v_2)$.
2. For all $s \in k$ and $v \in V$, we have $T(sv) = sT(v)$.

Such a linear transformation is an **isomorphism** if it is both injective and surjective.

As a first example, the maps of the form $f(x) = kx$, for $k \in \mathbb{R}$, are all linear transformations from $\mathbb{R}$ to $\mathbb{R}$. Notice, however, that $f(x) = x + 1$ is not a linear transformation, since $f(1) + f(1) = 2 + 2 = 4$, but $f(1 + 1) = f(2) = 3$.

Notice that the second condition is sometimes unnecessary.

Problem 2.3.1. Suppose that $k = \mathbb{Q}$, and V, W are vector spaces over $\mathbb{Q}$. Show that if $T : V \to W$ satisfies $T(v_1 + v_2) = T(v_1) + T(v_2)$ for all $v_1, v_2 \in V$, then T is actually linear.

Now, given a linear transformation $T : V \to W$, we consider the following two sets associated with this linear transformation: the **kernel** and the **image.**

Definition 2.3.2. The kernel of a linear transformation, $\ker T$, is the set of elements $v \in V$ such that $T(v) = 0_W$. The image, $\operatorname{im} T$, is the set of elements $w \in W$ such that there exists a $v \in V$ so $T(v) = w$.

Example. Consider the map that sends a polynomial of degree at most 2, with coefficients in $\mathbb{C}$, to its value at 0 (lying in $\mathbb{C}$); we can easily check that this is a linear transformation. The kernel of this map is then just the set of polynomials that vanish at 0, namely those of the form $ax + bx^2$, for $a, b \in \mathbb{C}$, and the image is $\mathbb{C}$.

Proposition 2.3.3. *A linear transformation T is injective if and only if* $\ker T = \{0_V\}$.

Proof. First, we note that T being injective means that $\ker T$ only has one element. Furthermore, by linearity, $T(0_V) + T(0_V) = T(0_V)$, meaning that $T(0_V) = 0_W$, meaning that $\ker T = \{0_V\}$. For the other direction, if $\ker T = \{0_v\}$, suppose that $T(v_1) = T(v_2)$. By linearity, we have that $T(v_1) - T(v_2) = T(v_1) + (-1)T(v_2) = T(v_1) + T(-v_2) = T(v_1 - v_2) = 0$. But this means that $v_1 - v_2 \in \ker T$, or that $v_1 - v_2 = 0_T$, meaning that $v_1 = v_2$. This means that T is injective, which is what we wanted to show. □

Problem 2.3.2. Show that $\ker T$ is a subspace of V.

We now have the following result, which essentially states that finite-dimensional vector spaces are essentially determined by their dimension. Indeed, just like with rings, we can think of isomorphisms as simply being "relabellings" of the elements in our original space.

Problem 2.3.3. Suppose that V and W are finite dimensional vector spaces with the same dimension d. Prove that V, W are **isomorphic**; that is, there exists an isomorphism between them.

To show that this characterizes the space, we should also verify that two spaces that are different dimensions cannot be isomorphic. First, we verify the following.

Problem 2.3.4. Prove that an infinite dimensional vector space cannot be isomorphic to a finite dimensional vector space.

For a given linear transformation T, we can relate the dimension of its image and kernel in the following way. The following theorem is also known as the rank-nullity theorem.

Theorem 2.3.4. *Suppose that T is a linear transformation from V to W, where V is a finite dimensional vector space. Then,*

$$\dim \ker T + \dim \operatorname{im} T = \dim V.$$

Often, $\dim \ker T$ *is referred to as the* ***nullity*** *of* T*, and* $\dim \operatorname{im} T$ *the* ***rank.***

To do this, first consider a basis for $\ker T$. Say these vectors are $w_1, w_2, \ldots, w_n$.

Problem 2.3.5. To prove the theorem, prove the following:

1. Show that this basis of $\ker T$ can be extended to a basis of V.
2. Suppose that this extension adds vectors $w_{n+1}, w_{n+2}, \ldots, w_m$. Show that

$$T(w_{n+1}), T(w_{n+2}), \ldots, T(w_m)$$

form a basis for $\operatorname{im} T$, and from here prove the theorem.

Using the theorem, we also say the following.

Problem 2.3.6. Show that two finite dimensional vector spaces are isomorphic if and only if they have the same dimension.

This says essentially that, for a given field k, the finite dimensional vector spaces over that field are characterized exactly by the dimension of the space, up to isomorphism.

2.4 Matrices and Row Reduction

Sometimes it is useful to be able to talk explicitly about the vectors in a vector space V. This can be done by fixing a basis of our vector space V, and then describing each vector as being a linear combination of these basis vectors. In particular, given our basis $w_1, w_2, \ldots, w_n$, we represent $v = \sum_{i=1}^{n} a_i w_i$ as the column vector $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} \in k^n$.

Problem 2.4.1. Show that this above map is well-defined and is an isomorphism between V and k^n.

If we now specify bases $(v_1, v_2, \ldots, v_n)$ for V and $(w_1, w_2, \ldots, w_m)$ for W, we can now describe every linear transformation $T : V \to W$ as a **matrix**. Specifically, if $T(v_j) = \sum_{i=1}^{m} a_{i,j} w_i$, we can represent T as the following $m \times n$ array of numbers:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

We say that a_{ij} is the (i, j)th entry of this matrix.

We can then view the operation of the linear transformation entirely using the coordinates described by these bases, using the following multiplication rule:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} a_{1i} x_i \\ \sum_{i=1}^{n} a_{2i} x_i \\ \vdots \\ \sum_{i=1}^{n} a_{mi} x_i \end{pmatrix}.$$

For instance, given the vector space of polynomials of degree at most 2, we can see that this has a basis $1, 1 + x, 1 + x + x^2$. Consider the map that sends each polynomial to the vector $\begin{pmatrix} p(0) \\ p(1) \end{pmatrix}$. Then, the matrix that we get for this linear transformation is

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix}.$$

For instance, we note that $T(1 + x + x^2) = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$, giving us the third column.

We wish to relate the two operations of matrix multiplication and of applying our linear transformation in general.

Problem 2.4.2. Show that if we multiply the matrix of T with the coordinate representation of $v \in V$, we get the coordinate representation of $T(v)$. In this sense, our notion of matrix multiplication is consistent with the way our linear transformation acts on vectors.

Often, we want to represent T using a choice of bases that are as simple as possible. If we are allowed to change the bases of both V and W, this can take a particularly simple form.

Problem 2.4.3. Show that there exists bases for V, W such that the only nonzero entries of T are along the diagonal; that is, only the (i, i)th entries are nonzero for $i = 1, 2, \ldots, r$ for some nonnegative integer r. What is the value of r?

Although this is a nice result, often we run into situations where we cannot freely choose bases in the way the above result requires. First, if T is a map from a vector space to itself, we often only want to use one basis for both the input and output. This gives us significantly less flexibility; see section 5 for more details.

In other situations, we have a nice basis for V which we would like to preserve. As such, we are only allowed to choose a basis for W. In this latter situation, we can achieve a comparatively simple form using a method called **row reduction.**

The main algorithm for row reduction utilizes three operations, acting on rows of our matrix.

1. We can take a row and multiply every entry in the row by some nonzero scalar $c \in k$.
2. We can swap two rows (that is, if we are swapping rows i, j, then the old (i, k)th entry is the new (j, k)th entry for $k = 1, 2, \ldots, n$, and vice versa).
3. We can add a multiple of one row to another row.

For instance, we can apply some row operations to the matrix $\begin{pmatrix} 2 & 6 & 3 \\ 1 & 0 & 4 \\ 0 & -1 & 1 \end{pmatrix}$. If we subtract half the first row from the second, we get the matrix $\begin{pmatrix} 2 & 6 & 3 \\ 0 & -3 & 2.5 \\ 0 & -1 & 1 \end{pmatrix}$. If we then divide the first row by 2, we get the matrix $\begin{pmatrix} 1 & 3 & 1.5 \\ 0 & -3 & 2.5 \\ 0 & -1 & 1 \end{pmatrix}$.

Problem 2.4.4. Show that if we apply one of our row reduction operations to a matrix for T, we get another matrix for T, using a different basis for W (but the same basis for V). How do you relate the old basis to the new basis?

From here, we claim that we can reach the following form, known as **reduced row echelon form.** This form satisfies the following properties.

1. Every row with at least one nonzero entry has their leftmost nonzero entry as a 1. These 1s are known as **pivots.**
2. Each pivot is the only nonzero entry in its column.
3. The pivot of the ith row is left of the pivot of the jth row if $i < j$.
4. The rows with all zeros are on the bottom of the matrix.

For instance, with the same matrix as the above, we can continue our procedure: swapping rows two and three yields $\begin{pmatrix} 1 & 3 & 1.5 \\ 0 & -1 & 1 \\ 0 & -3 & 2.5 \end{pmatrix}$, then subtracting three times the second row from the third yields $\begin{pmatrix} 1 & 3 & 1.5 \\ 0 & -1 & 1 \\ 0 & 0 & -0.5 \end{pmatrix}$. Adding three times the second row to the first yields $\begin{pmatrix} 1 & 0 & 4.5 \\ 0 & -1 & 1 \\ 0 & 0 & -0.5 \end{pmatrix}$. Adding two times the third row to the second, and nine times the third row to the first, yields $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -0.5 \end{pmatrix}$. Multiplying the third row by -2 and the first by -1 yields the final matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, which is in reduced row echelon form.

Problem 2.4.5. Reduce the following matrices to reduced row echelon form.

1. $\begin{pmatrix} 1 & 2 & 3 \\ 6 & 5 & 4 \end{pmatrix}$
2. $\begin{pmatrix} 4 & 2 & -1 & -3 \\ 1 & 0 & -5 & 2 \\ 0 & 1 & 0 & 2 \end{pmatrix}$

Problem 2.4.6. Show that for any i, using the row operations on the matrix for T, if column i had at least one nonzero entry initially, then there is a sequence of row operations such that the resulting matrix only has one nonzero entry in column i, and it is a 1.

Problem 2.4.7. Using the above procedure, show that any matrix can be reduced to reduced row echelon form.

With the reduced row echelon form, we can more easily read off useful information about our linear transformation T.

Problem 2.4.8. Show that the number of pivots of T is equal to the rank of T, and the number of columns without pivots is equal to the nullity of T, without using the rank-nullity theorem. (One can prove the rank-nullity theorem by analyzing the reduced row echelon form of a matrix).

With the above method, we can everywhere replace the word "row" with "column" to get **column reduction.** This corresponds to changing the basis for the input space, which you may assume without proof.

3 Modules

We can generalize the definition of a vector space above to that of a module, as below.

Definition 3.0.1. Given a ring R, a **module** M is a set of elements equipped with two operations, addition $+ : M \times M \to M$ and scalar multiplication $\cdot : R \times M \to M$, satisfying the following properties:

1. M is closed under addition and scalar multiplication: that is, $\forall m_1, m_2 \in M$, $m_1 + m_2 \in M$, and for all $r \in R, m \in M$, we have $r \cdot m \in M$.
2. The operations $+, \cdot$ are associative: $\forall m_1, m_2, m_3 \in M$, we have that $(m_1 + m_2) + m_3 = m_1 + (m_2 + m_3)$, and for $r_1, r_2 \in R$ and $m \in M$, we have $r_1 \cdot (r_2 \cdot m) = (r_1 \cdot_R r_2) \cdot m$.
3. The operation $+$ is commutative.
4. The operation $+$ has an identity element, which we denote as 0.
5. Each element $m \in M$ has an additive inverse.
6. For all $m \in M$, $1_R \cdot m = m$.
7. We have the following distributive laws: $\forall r \in R$ and $m_1, m_2 \in M$, we have $r_1 \cdot (m_1 + m_2) = r_1 \cdot m_1 + r_1 \cdot m_2$, and for all $r_1, r_2 \in R$ and $m \in M$, we have $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$.

We also say that M in this case is an $R-$module. A **submodule** of M is a subset N that is also a module under the same operations as that of M.

Notice in particular that a vector space over a field is also module over that field, and any ring is a module over itself. Here is another example.

Example. The set of even integers is a module over $\mathbb{Z}$, using the standard addition on even integers and scalar multiplication being just multiplication in $\mathbb{Z}$. Properties 2, 3, 7 follow simply because we know that $\mathbb{Z}$ is a ring, and property 1 follows since we've previously argued that the sum of even integers is even, and the product of an even integer with another integer is even.

For property 4, we note that the identity for addition, 0, lies in $\mathbb{Z}$, and property 5 follows since we know that for each even integer, its negation is also even. Finally, for property 6, by the standard multiplication rule in $\mathbb{Z}$, multiplying any even integer by 1 yields the even integer again.

This example can be generalized.

Problem 3.0.1. Show that for any ring R and ideal I of R, I is an $R-$module under the addition and multiplication operations of the ring R.

Definition 3.0.2. Given an $R-$module M, a **linear combination** of $m_1, m_2, \ldots, m_n \in M$ is an expression of the form $\sum_{i=1}^{n} r_i m_i$, where $r_i \in R$.

A **generating set** of a module M is a set S such that every element can be written as a linear combination of some finite subset of S. We say that a module is **finitely generated** if it has a finite generating set.

A set of elements of M is **linearly independent** if the only linear combination of these elements that equals zero is the linear combination where all of the coefficients r_i are 0.

A set of elements of M is said to be a **free basis** of M if it is linearly independent and a generating set. In this case, if such a free basis exists, we say that M is a **free module**. Its **rank** is then the length of this free basis.

These definitions should be reminiscent of definitions of linear independence and span from our discussions of linear algebra. We need to explicitly point out when our modules are free for the following reason.

Example. Consider the ideal $I = \langle 2, 1+\sqrt{-5}\rangle$ inside the ring $R = \mathbb{Z}[\sqrt{-5}]$, the set of integers of the form $a+b\sqrt{-5}$ for some integers a, b. Notice that this ideal is an $R-$module by Problem 3.0.1. We show that this is not a free module.

To see this, suppose for the sake of contradiction that $\{r_1, r_2, \ldots, r_k\}$ was a free basis for I. If $k \geq 2$, then note that by linear independence that none of the elements can be zero. But then $(-r_2)r_1 + r_1 r_2 = 0$, meaning that this set is not linearly independent, contradiction.

Therefore, I would have to have a free basis with one element, say r_1. But then there exist elements $s_1, s_2 \in R$ such that $s_1 r_1 = 2$ and $s_2 r_1 = 1+\sqrt{-5}$. But suppose that $s_1 = a_1 + a_2\sqrt{-5}$ and $r_1 = b_1 + b_2\sqrt{-5}$, then $s_1 r_1 = (a_1 b_1 - 5a_2 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{-5}$. For this to equal 2, we need $a_1 b_2 = -a_2 b_1$. Note however that multiplying this by $(a_1 - a_2\sqrt{-5})(b_1 - b_2\sqrt{-5})$, which equals $(a_1 b_1 - 5a_2 b_2) - (a_1 b_2 + a_2 b_1)\sqrt{-5} = 2$, yields that $(a_1^2 + 5a_2^2)(b_1^2 + 5b_2^2) = 4$. For this to hold, as the a_i are integers, we need one pair of (a_1, a_2) to be $(\pm 1, 0)$ and the other to be $(\pm 2, 0)$. However, note that r_1 cannot be ± 2, since that implies that $s_2 = \pm\frac{1+\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$, contradiction.

But if $r_1 = \pm 1$, this means that $1 \in \langle 2, 1+\sqrt{-5}\rangle$, meaning that there exist $a+b\sqrt{-5}$ and $c+d\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ so $2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) = 1$, or that $(2a+c-5d) + (2b+c+d)\sqrt{-5} = 1$. But $c-5d$ would have to be odd and $c+d$ even, which is impossible.

Hence, no r_1 can exist, and therefore I must not be a free module, which is what we wanted to show.

Observe that if we are given a free module, the following property from linear algebra does carry over to the module case. You may assume that this proposition holds without proof.

Proposition 3.0.3. *Suppose that F is a free module over a nonzero ring R that is finitely generated. Then, any two free bases of F have the same length.*

Similarly to the vector space case, we can also consider maps between modules, in the following way.

Definition 3.0.4. A **module homomorphism** between $R-$modules M and N is a map $\phi : M \to N$ such that for all $m, m' \in M$ and $r \in R$, we have that $\phi(m +_M m') = \phi(m) +_N \phi(m')$, and $\phi(r \cdot_M m) = r \cdot_N \phi(m)$.

Definition 3.0.5. A module homomorphism is said to be an **isomorphism** if it is injective and surjective. Two modules are then **isomorphic** if there exists an isomorphism between them.

We also have the kernel and the image, defined similarly to the vector space case.

Definition 3.0.6. Let $\ker \phi = \{m \in M | \phi(m) = 0\}$, and $\text{im}\phi = \{\phi(m) | m \in M\}$.

Just like before, we will omit which objects are being mapped if it is clear from context what objects we are mapping. Similarly to the vector space case, we can verify that the kernel and image of a module homomorphism are both modules; you may use this throughout the rest of the power round without proof.

Problem 3.0.2. Show that any finitely generated free module is isomorphic to R^n for some $n \in \mathbb{N}$.

We finally have the notion of a quotient module and the direct sum of modules.

Definition 3.0.7. Given $R-$modules $M_1, M_2, \ldots, M_k$, the module $M_1 \oplus M_2 \oplus \ldots \oplus M_k$, sometimes written as $\bigoplus_{i=1}^{k} M_i$, is the set of elements $\{(m_1, m_2, \ldots, m_k) | m_i \in M_i \text{ for } i = 1, 2, \ldots, k\}$, equipped with addition and scalar multiplication coordinate-wise. That is,

$$(m_1, m_2, \ldots, m_k) + (m_1', m_2', \ldots, m_k') = (m_1 +_{M_1} m_1', m_2 +_{M_2} + m_2', \ldots, m_k +_{M_k} m_k')$$

and

$$r \cdot (m_1, m_2, \ldots, m_k) = (r \cdot_{M_1} m_1, r \cdot_{M_2} m_2, \ldots, r \cdot_{M_k} m_k).$$

For instance, to get the module R^n, the set of tuples of length n (whose entries are elements of R), we can do $R^n = R \oplus R \oplus \ldots \oplus R$; the addition and scalar multiplication operations of R^n are precisely those that are obtained by using this direct sum procedure.

Definition 3.0.8. Given two $R-$modules M, N, define for $m \in M$ the set $m + N$ as $\{m+n | n \in N\}$. Then, M/N is the module defined to be the set of elements $\{m+N | m \in M\}$, equipped with addition $(m_1+N)+(m_2+N) = (m_1+m_2)+N$ and $r \cdot (m_1+N) = (r \cdot m_1)+N$, for all $m_1, m_2 \in M$ and $r \in R$.

One can verify that the two above definitions are well-defined and actually give modules. For the purposes of this power round, however, you may assume these to be true.

We now begin to discuss some important properties of homomorphisms.

Problem 3.0.3. Given a submodule N of an $R-$module M, consider the map $\kappa_{M,N} : M \to M/N$ that sends m to $m+N$. Show that this map is a surjective homomorphism. What is the kernel of $\kappa_{M,N}$?

Problem 3.0.4. Given a homomorphism between $R-$modules M, N :

1. Show that there exists a homomorphism $\bar{\phi} : M/\ker\phi \to N$ such that

$$\bar{\phi}(\kappa_{M,\ker\phi}(m)) = \phi(m)$$

for all $m \in M$. Remember to check that the homomorphism that you construct is actually well-defined!

2. Show that $M/\ker\phi$ is isomorphic to imϕ.

4 The PID Structure Theorem

Although we've seen that modules in general can be quite complex, lacking the simplicity of vector spaces (in the sense that they aren't generally classified by a single number), modules over PIDs are the next best case.

Having built up the necessary ring and module theory over the previous sections, we are now ready to state and prove the main theorem of this power round!

Theorem 4.0.1. *Let R be a PID, and M be a finitely generated $R-$module. Then, there are positive integers k, r and nonzero elements $d_1, d_2, \ldots, d_k$ of R such that M is isomorphic to*

$$R^r \oplus \bigoplus_{i=1}^{k} R/\langle d_i \rangle.$$

Before we proceed onto the proof, we first need to understand some more important properties of PIDs and modules of PIDs. These properties arise in a more general class of rings, which are called **Noetherian rings.** The notion of being Noetherian will also be extended to modules.

One of the main benefits of having this concept of Noetherian modules is that it describes a certain "finiteness" condition that the module satisfies. Such a finiteness condition will allow us to conclude that certain algorithm stops, or that certain constructions (in particular, having a finite set of generators) are possible, which we will find useful in the proof of the PID Structure Theorem. As such, before proceeding to the proof of the theorem, we begin by discussing Noetherian modules in general.

4.1 Noetherian Rings and Modules

We first begin by introducing the notion of a Noetherian ring.

Definition 4.1.1. A **Noetherian** ring is a ring R satisfying the following property: suppose we have a chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$. Then, there exists some n such that $I_m = I_n$ for all $m \geq n$.

We first consider some examples of a Noetherian ring.

Example. For instance, $\mathbb{Z}$ is a Noetherian ring. Indeed, given any ideals $I_1 \subseteq I_2 \subseteq I_3 \ldots$, notice that, by Problem 1.2.3, each ideal is of the form $\langle i \rangle$ for some i. Say that $I_j = \langle i_j \rangle$. Then, observe that for $I_j \subseteq I_{j+1}$, we need $i_j \in I_{j+1}$, or that i_j is divisible by i_{j+1}.

We finally observe that if no such m exists, then we can pick a subset of the ideals $I_{j_1}, I_{j_2}, \ldots$ that forms a strictly increasing chain, namely where $I_{j_1} \subsetneq I_{j_2} \subsetneq I_{j_3} \subsetneq \ldots$. To do this, one can proceed inductively: pick one ideal to start with, I_{j_1}. Then, by assumption, not all the ideals are equal to I_{j_1}; let one such ideal be I_{j_2}. We can repeat this logic for I_{j_2} to get some I_{j_3}, and so on.

But then we have an infinite sequence of integers $i_{j_1}, i_{j_2}, i_{j_3}, \ldots$, where $i_{j_k}/i_{j_{k+1}}$ is an integer. Furthermore, since our ideal inclusions are proper, this integer cannot be 1 or -1, as otherwise the ideals would be equal (since $-1 \in \mathbb{Z}$, and an integer is a multiple of x if and only if it is a multiple of $-x$). In particular, we have that $|i_{j_k}| > |i_{j_{k+1}}|$ for each k. But then $|i_{j_1}|, |i_{j_2}|, |i_{j_3}|, \ldots$ is an infinite sequence of decreasing positive integers, which is impossible.

Therefore, $\mathbb{Z}$ is a Noetherian ring.

We also have the following equivalent way of defining a Noetherian ring, as follows, which is more reminiscent of the definition of a PID.

Problem 4.1.1. Prove the following.

1. Show that every ideal can be generated by a finite set of elements in a Noetherian ring. As a hint, suppose that an ideal existed that was not generated by finitely many elements. Can you find an increasing chain of ideals?
2. For any chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ of ideals, show that $\bigcup_{i=1}^{\infty} I_i$ is an ideal.
3. Suppose that ring R is such that every ideal can be generated by a finite set of elements. Prove that R is Noetherian. As a hint, consider the previous part, and consider a finite set that generates the union of ideals in the chain. Where do each of the elements in this finite set live?
4. Conclude that every PID is Noetherian.

While being a PID is a stronger condition than being Noetherian, throughout the proof of the PID Structure theorem we will find thinking about the Noetherian property to be useful.

We also have the notion of Noetherian modules, which are defined with a similar characteristic property to that of rings.

Definition 4.1.2. An $R-$module M is **Noetherian** if the following holds: for every sequence of submodules $M_1, M_2, \ldots$ of M so $M_1 \subseteq M_2 \subseteq \ldots$, there is some $n \in \mathbb{N}$ such that $M_m = M_n$ for all $m \geq n$.

Just like with the case of Noetherian rings, there is another, perhaps more natural way, of determining whether a module is Noetherian:

Problem 4.1.2. Prove the following statements.

1. Show that if M is a Noetherian module, then every submodule of M is finitely generated. (Hint: suppose some submodule N was not finitely generated. Then, if you pick any finite subset of N, the module that subset generates will not equal N. Keep adding elements to this finite subset; what happens?)
2. Suppose that every submodule of M is finitely generated. Prove that M is Noetherian.

The condition of being Noetherian means we don't have to be worried about whether submodules of our finitely generated module are also finitely generated; the condition of a module being Noetherian allows us to conclude that the submodules are Noetherian, and in particular finitely generated.

We can also relate modules being Noetherian to other modules being Noetherian.

Problem 4.1.3. Given an $R-$module M and a submodule N of M, show that if M is Noetherian, then $N, M/N$ are both Noetherian. (Hint: consider the map $\kappa_{M,N}$, and use the previous problem).

Problem 4.1.4. Prove the following.

1. Given a module M and a submodule N of M suppose that $M_1 \subseteq M_2$ are submodules such that $M_1 \cap N = M_2 \cap N$ and $\kappa_{M,N}(M_1) = \kappa_{M,N}(M_2)$. Show that $M_1 = M_2$.
2. Using the above result, show that if N and M/N are Noetherian, then M is also Noetherian.

This above problems really mean that the property of being Noetherian carries over to a lot of other different modules (which in turn means we know a lot of modules are finitely generated as a result).

The classification of when a module is Noetherian is particularly simple when we also have that it is a module over a Noetherian ring R.

Problem 4.1.5. Let R be a Noetherian ring, and let M be a module over R.

1. Show that if M is Noetherian, then M is finitely generated.
2. Show that R is an Noetherian $R-$module (hint: what are submodules of R?)
3. Let N be the submodule of R^n consisting of tuples whose last $n-m$ entries are all zero. Show that R^n/N is isomorphic to R^{n-m}, for positive integers $n \geq m$. Note that N is isomorphic to R^m; for the purposes of this power round you do not need to prove this.
4. Using the previous part, show that R^n is a Noetherian $R-$module for every positive integer n.
5. Show therefore that if M is finitely generated, then M is a Noetherian $R-$module.

4.2 Smith Normal Form

In this part, we apply some of the operations of row reduction and column reduction to a matrix A whose entries are in a PID R (where instead of multiplication by scalars in a field, we have multiplication by elements in R). Throughout this subsection and the next subsection, we let R be a fixed PID.

Instead of row and column operations, we have multiplication on the left and right by certain matrices, illustrated as follows.

Definition 4.2.1. An $n \times n$ matrix S, whose entries are in R, is **invertible** if there exists an $n \times n$ matrix T such that $ST = TS = I$, where I is the matrix given by having 1 along the diagonal and zero elsewhere.

For instance, each of the row operations from linear algebra can be viewed as multiplying our matrix on the left. If we start with the matrix $\begin{pmatrix} 4 & 6 & 2 \\ 1 & 3 & 5 \end{pmatrix}$, we can add twice the second row to the first by multiplying the matrix on the left by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. By the same reasoning, we can think of column operations as multiplying by an invertible square matrix on the right.

Observe also that the product of two invertible matrices (that are the same square dimension) is an invertible matrix; indeed, if S, S' are invertible matrices with inverses T, T', then $SS'(T'T) = SIT = ST = I$, and $(T'T)SS' = T'IS' = T'S' = I$.

Now, suppose we are given an $n \times m$ matrix A (where $n, m \geq 1$) whose (i,j)th entry is $a_{i,j}$. Then, in R^n, consider the submodule $N(A)$ generated by the m elements $\sum_{i=1}^{n} a_{i,j} e_i$, where $e_1, e_2, \ldots, e_n$ is some fixed free basis of R^n. We are interested in $R^n/N(A)$. We assume that $A \neq 0$ first.

We first show that multiplying by these invertible matrices correspond to simply performing changes of basis, meaning that we should have modules that are isomorphic. In particular, we have the following statements.

Problem 4.2.1. Suppose that we multiply A on the right by an $m \times m$ invertible matrix S to get the matrix A'. Show that $N(A') = N(A)$. (Hint: show that an element on the left-hand side lies on the right-hand side. Use invertibility).

Problem 4.2.2. Suppose that we multiply A on the left by an $n \times n$ invertible matrix S to get the matrix A'. Show that $R^n/N(A)$ and $R^n/N(A')$ are isomorphic. (Hint: what is an isomorphism between the two modules?)

We also observe here that this is false if we do not scale by a unit. For instance, letting our ring $R = \mathbb{Z}$ and $A = (1)$, notice that $R/N(A)$ is simply $\mathbb{Z}/\mathbb{Z} = \{0\}$, the trivial module. However, scaling by 2 yields $A' = (2)$, and so $R/N(A') = \mathbb{Z}/2\mathbb{Z}$, which is not isomorphic to the trivial module.

From here, we are interested in how simple a form for the matrix we are able to obtain using row and column operations.

Problem 4.2.3. As a first step, we want to reduce a column down to having a single nonzero entry in it, using row operations.

1. Suppose we have a matrix $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, where $r_1, r_2 \neq 0$. Show there exists a 2×2 invertible matrix S such that $S \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} r \\ 0 \end{pmatrix}$ for some element $r \in R$. How is r related to r_1, r_2?

2. Suppose now we have a matrix $\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$, where not all the r_i are zero. Show that there exists an $n \times n$ invertible matrix S such that $S \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, for some $r \in R$. How is r related to $r_1, r_2, \ldots, r_n$?

3. Given an $n \times m$ matrix A, for $n, m \geq 0$, show that there exists an $n \times n$ invertible matrix S and an $m \times m$ invertible matrix T so that SAT has no nonzero entries in the first row or first column, except for the $(1,1)$ entry. (Hint: suppose that the $(1,1)$ entry doesn't divide every entry in the first row or first column. Apply the previous part. Repeat, and use the fact that R is a PID, ergo Noetherian.)

Using this above procedure, we are able to bring our matrix A into a diagonal form.

Problem 4.2.4. Show that using row and column operations, one can reduce the matrix such that all nonzero entries lie on the diagonal (so $a_{i,j} \neq 0$ implies that $i = j$).

This is already a rather nice simplification. However, it turns out we are able to do more. There are two ways that we can further simplify our diagonal form for the matrix.

Problem 4.2.5. Show that we can further reduce the matrix so that the nonzero entries are $a_{1,1}, a_{2,2}, \ldots, a_{k,k}$ for some positive integer $1 \leq k \leq m$, and so that $a_{i,i}$ divides $a_{i-1,i-1}$ for $i = 2, 3, \ldots, k$. This is known as **Smith normal form.**

So if we allow both row and column operations, we can drastically simplify A, and furthermore we get the same quotient ring for $R^n/N(A)$, up to isomorphism.

4.3 Proof of the PID Structure Theorem

We can now use this idea of Smith normal form to prove the PID Structure theorem. Throughout this section, let M be a finitely generated R-module.

Problem 4.3.1. Show that there exists a surjective map ϕ from a free module F of finite rank to M.

Now, fix one such $\phi : F \to M$.

Problem 4.3.2. Show that $\ker \phi$ is finitely generated.

Since $\ker \phi$ is finitely generated, there is a finite set of generators $w_1, w_2, \ldots, w_m$. Furthermore, F is a free module of finite rank, so there is some free basis $e_1, e_2, \ldots, e_n$. By the definition of free basis, we can write $w_j = \sum_{i=1}^{n} a_{ij} e_i$ for $j = 1, 2, \ldots, m$.

This then suggests that we construct the matrix $n \times m$ matrix A, whose (i, j)th entry is $a_{i,j}$.

Problem 4.3.3. Suppose that the only nonzero entries of A are along the diagonal (that is, $a_{i,j} \neq 0$ implies that $i = j$). Show that M is then isomorphic to a module of the form

$$R^r \oplus \bigoplus_{i=1}^{k} R/\langle d_i \rangle,$$

and describe how you obtain the values d_i and r.

However, using the results of the previous section, we are now ready to prove the theorem.

Problem 4.3.4. Prove Theorem 4.0.1, and show that a choice of d_i can be made such that the d_i are all powers of prime elements.

5 Applications and Asides

In this section, we establish two corollaries of the PID Structure theorem, which are also interesting results in their own right. Before we do this, however, we first turn to an example where the theorem fails if our ring is not a PID.

5.1 A Counterexample

This theorem that we have just proven only applies to modules of PIDs, as we see from the following.

Problem 5.1.1. Find a $\mathbb{Z}[\sqrt{-5}]-$module that is not isomorphic to a module of the form

$$R^r \oplus \bigoplus_{i=1}^{k} R/\langle d_i \rangle,$$

where $R = \mathbb{Z}[\sqrt{-5}]$.

5.2 Abelian Groups

As a corollary, we can apply the theorem to what are known as **abelian groups.** We define these structures as follows.

Definition 5.2.1. A **abelian group** is a set G equipped with an operation, $+$, satisfying the following conditions:

1. G is closed under $+$.
2. The operation $+$ is associative and commutative: that is, for all $g_1, g_2, g_3 \in G$, $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$, and $g_1 + g_2 = g_2 + g_1$.
3. The operation $+$ has an identity element 0.
4. Every element of G has an inverse with respect to $+$. Written out, for each $g \in G$, there exists an element $h \in G$ such that $g + h = 0$.

A **subgroup** of a group G is a subset H of G that is a group under the same operation of H.

Note that, by definition, every ring is also an abelian group, by discarding the $\cdot$ operation.

Example. For instance, note that $\mathbb{Z}/n\mathbb{Z}$ is an abelian group for any positive integer n, using the remark above, as well as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, under the addition operation.

Note that $\mathbb{Z}$ is also an abelian group, with the set of even integers forming a subgroup.

We also have the following useful notions.

Definition 5.2.2. The **order** of an element $g \in G$ is the smallest positive integer n so that $\underbrace{g + g + \ldots + g}_{n \text{ times}} = 0$, if it exists. If it doesn't, we say that g has **infinite order.**

The **order** of a group G is the number of elements in the group.

Problem 5.2.1. Consider the group $\mathbb{Z}/8\mathbb{Z}$. How many elements are there of each order? What if you replace 8 with any positive integer n?

Many of the definitions and constructions that we introduced for rings and modules also carry over to abelian groups as well, such as the notion of group homomorphisms and group isomorphisms. For instance, we have that $\mathbb{Z}$ is an abelian group under addition, and for each positive integer n that $\mathbb{Z}/n\mathbb{Z}$ is also an abelian group under addition. We observe that every element in $\mathbb{Z}/n\mathbb{Z}$ has order that divides n, since if we add any element to itself n times, we get 0.

As a mild abuse of notation, in this section we will write $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ to mean the abelian groups with the normal addition operation, rather than considering the entire ring structure.

Definition 5.2.3. A subset S of abelian group G is a set of **generators** for G if every element of G can be written as a finite sum of elements in S. G is **finitely generated** if S can be made finite.

An abelian group G is **cyclic** if it can be generated by one element.

Definition 5.2.4. Given abelian groups $G_1, G_2, \ldots, G_n$, we define the abelian group

$$G_1 \oplus G_2 \oplus \ldots \oplus G_n = \bigoplus_{i=1}^{n} G_i$$

is defined as the set of tuples $\{(g_1, g_2, \ldots, g_n) | g_i \in G_i \text{ for } i = 1, 2, \ldots, n\}$, which we also denote as $G_1 \times G_2 \times \ldots \times G_n$, with addition defined as

$$(g_1, g_2, \ldots, g_n) + (g_1', g_2', \ldots, g_n') = (g_1 +_{G_1} g_1', g_2 +_{G_2} g_2', \ldots, g_n +_{G_n} g_n').$$

Problem 5.2.2. Show that $\mathbb{Z}/n\mathbb{Z}$ is cyclic for every positive integer n.

Problem 5.2.3. Show that $\mathbb{Z}[x]$, the set of polynomials with coefficients in $\mathbb{Z}$, is not a finitely generated abelian group under addition. (Hint: suppose you had a finite subset of $\mathbb{Z}[x]$. What elements can be written as a sum of these elements?)

Similarly to rings and modules, we have the notion of homomorphisms and isomorphisms of abelian groups, as follows.

Definition 5.2.5. A **group homomorphism** is a map $\phi : G_1 \to G_2$ between groups G_1 and G_2 such that for all $g, h \in G$, we have that $\phi(g) + \phi(h) = \phi(g + h)$, where the first addition is in group G_2 and the second addition is in the group G_1.

An **isomorphism** is a bijective homomorphism.

Example. As a simple example, we show that two cyclic groups that have the same finite order are isomorphic.

To do this, suppose that our cyclic groups are G_1 and G_2. Suppose that g_1 is a generator of G_1 and g_2 a generator of G_2. Let $\phi : G_1 \to G_2$ be the map that sends the sum of g_1 with itself n times to the sum of g_2 with itself n times (for instance, $\phi(g_1 + g_1) = g_2 + g_2$).

Since g_1 generates G_1, this specifies where ϕ sends every element of G_1. Furthermore, if G_1, G_2 both have order m, notice that g_1, g_2 have order m as well. Indeed, if we consider

the sequence $g_1, g_1+g_1, g_1+g_1+g_1, \ldots$, we will get a sequence where every element of G_1 appears, and that is periodic with period the order of g_1. But it will also need to be periodic with the order of G_1, meaning that g_1 has order m. The same logic applies for g_2.

In particular, this means that if the sum of g_1 with itself k times equals the sum of g_1 with itself l times, then $l-k$ is divisible by m. But then the sum of g_2 with itself k times equals the sum of g_2 with itself l times (so are equal). This means that ϕ is well-defined.

Finally, if h_x is the sum of g_1 with itself x times, then $\phi(h_x+h_y)$ equals the sum of g_2 with itself $x+y$ times. But $\phi(h_x)$ equals the sum of g_2 with itself x times, and $\phi(h_y)$ equals the sum of g_2 with itself y times, so $\phi(h_x)+\phi(h_y)=\phi(h_x+h_y)$, and ϕ is our homomorphism.

We can also see that this map is bijective, since it an inverse, which we can construct using the same procedure as above but with G_1, G_2 swapped. Thus, G_1, G_2 are isomorphic.

In order to apply the PID Structure Theorem, we need to find an appropriate module structure.

Problem 5.2.4. Show that every abelian group is a $\mathbb{Z}-$module, where one of the operations is $+$. What is the scalar multiplication?

Having given abelian groups a $\mathbb{Z}-$module structure, we are now ready to apply the PID structure theorem to prove the following.

Problem 5.2.5. Suppose that G is a finitely generated abelian group. Show that G is isomorphic as a group to

$$\mathbb{Z}^r \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z},$$

for some positive integers $d_1, d_2, \ldots, d_r$ and nonnegative integers r, n.

5.3 Jordan Canonical Form

As a second, significantly less straightforward application of the PID structure theorem, we have a way to find a relatively simple matrix for a linear transformation T from a finite dimensional vector space V to itself. In this particular case, we specify a single basis for V, and use this basis to represent the matrix of $T: V \to V$.

First, we will see how we can apply the PID structure theorem to obtain an interesting result, and then from there convert the result from the PID structure theorem into a statement about the linear transformation T.

To begin, given a linear transformation T on V, we will once again try to find a module structure. We already have the addition operation and scalar multiplication by $\mathbb{C}$, from the definition of a vector space.

Problem 5.3.1. Show that V is a $\mathbb{C}[x]-$module, where for a polynomial $p(x)=\sum_{i=0}^{n} a_i x^i$ we define $p(x)\cdot v = \sum_{i=0}^{n} a_i T^i v$ for each $v \in V$.

Since we know that $\mathbb{C}[x]$ is a PID, we can apply the PID structure theorem. Because we also have that V is a finite-dimensional vector space, we are actually able to say something a little bit stronger.

Problem 5.3.2. Show that, as $\mathbb{C}[x]-$modules and as vector spaces, V is isomorphic to

$$\bigoplus_{i=1}^{n} \mathbb{C}[x]/(x-\lambda_i)^{r_i},$$

for some complex numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ and positive integers $r_1, r_2, \ldots, r_n$. Again, you will need the Fundamental Theorem of Algebra (see Problem 1.1.5).

Our goal is to now understand how T behaves on the vector space $\mathbb{C}[x]/(x-\lambda_i)^{r_i}$. Let ϕ be the map from V to $\bigoplus_{i=1}^{n} \mathbb{C}[x]/(x-\lambda_i)^{r_i}$.

Problem 5.3.3. Prove the following.

1. Show that for each λ_i there exists a set of vectors $v_1, v_2, \ldots, v_{r_i} \in V$ such that $Tv_1 = \lambda_i v_1$, and for $j = 2, 3, \ldots, r_i$, we have that $Tv_j = \lambda_i v_j + v_{j-1}$, and that $v_1, v_2, \ldots, v_{r_i}$ are linearly independent.
2. Show furthermore that these sets can be chosen such that, if we combine all of these sets together, the resulting set of vectors is also linearly independent.
3. Show that this set of vectors must therefore be a basis for V.

From here, we are ready to prove the following.

Problem 5.3.4. Show that for any linear transformation T on a $\mathbb{C}-$vector space V, there exists a basis $v_1, v_2, \ldots, v_n$ such that, with respect to this basis, T has block matrix form

$$\begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_k \end{pmatrix},$$

where each of the J_i has the following form for some $\lambda_i \in \mathbb{C}$:

$$\begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \lambda_i \end{pmatrix},$$

with λ_i along the main diagonal and 1s along the diagonal immediately above it. This is known as the **Jordan canonical form** for a linear transformation/matrix.

For the block matrix form, one can think of a matrix as being divided up into rectangles, and then viewing those rectangles as "blocks." For instance, in the matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 5 & -4 \\ 0 & 0 & 1 & 2 \end{pmatrix}$, we can think of this matrix as having block matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, where A is the 2×2 matrix $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and B is the 2×2 matrix $\begin{pmatrix} 5 & -4 \\ 1 & 2 \end{pmatrix}$. We also think of the 0s in the block form as the zero matrices, rather than simply the number zero.

Team Number: _____

PUMaC 2022* Power Round Cover Sheet

Remember that this sheet comes first in your stapled solutions. You should submit solutions for the problems in increasing order. Write on one side of the page only. The start of a solution to a problem should start on a new page. Please mark which questions for which you submitted a solution to help us keep track of your solutions.

Problem Number	Points	Attempted?
1.1.1	15	
1.1.2	5	
1.1.3	5	
1.1.4	5	
1.1.5	10	
1.1.6	5	
1.2.1	10	
1.2.2	5	
1.2.3	10	
1.2.4	10	
1.2.5	10	
1.3.1	10	
1.3.2	10	
1.3.3	25	
1.3.4	10	
2.1.1	10	
2.1.2	10	
2.2.1	10	
2.2.2	20	
2.2.3	10	
2.2.4	10	
2.2.5	20	
2.2.6	5	
2.2.7	10	
2.3.1	15	
2.3.2	5	
2.3.3	15	
2.3.4	10	
2.3.5	15	
2.3.6	10	
2.4.1	15	
2.4.2	10	
2.4.3	15	

Problem Number	Points	Attempted?
2.4.4	30	
2.4.5	10	
2.4.6	10	
2.4.7	25	
2.4.8	20	
3.0.1	5	
3.0.2	15	
3.0.3	10	
3.0.4	20	
4.1.1	30	
4.1.2	25	
4.1.3	15	
4.1.4	25	
4.1.5	40	
4.2.1	10	
4.2.2	15	
4.2.3	20	
4.2.4	25	
4.2.5	30	
4.3.1	10	
4.3.2	5	
4.3.3	40	
4.3.4	30	
5.1.1	25	
5.2.1	25	
5.2.2	10	
5.2.3	15	
5.2.4	20	
5.2.5	15	
5.3.1	15	
5.3.2	10	
5.3.3	30	
5.3.4	10	