

- (1) The most common issues here were not doing computations in the general case (ie only doing the $n = 2$ case) and not proving all the computations in detail. It's useful to know how to write $n \times n$ matrices and how to prove facts about them. For instance, almost everyone used a matrix which was 0 in all spots but one, and multiplied it on the left and right. Here's how I'd present this.

Let E^{ij} be the $n \times n$ matrix

$$\begin{pmatrix} 0 & \dots & \dots & \dots & 0 \\ \vdots & \ddots & & & \vdots \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix}$$

with the 1 in the ij^{th} position. That is,

$$E_{ab}^{ij} = \begin{cases} 1 & (a, b) = (i, j) \\ 0 & \text{otherwise} \end{cases}$$

Let $A = (A_{ij})$ be an $n \times n$ matrix. We consider the product $E^{ij}A$ and claim that this is the matrix whose i^{th} row is the j^{th} row of A , and that all other rows are 0. Indeed, the ab^{th} entry of this product is the dot product of the a^{th} row of E^{ij} with the b^{th} column of A . If $i \neq a$, the a^{th} row of E^{ij} is 0, so all rows of the product are 0, except potentially the i^{th} row. For the i^{th} row, the ib^{th} entry is

$$(E^{ij}A)_{ib} = \sum_{k=1}^n E_{ik}^{ij} A_{kb}$$

And by definition, E_{ik}^{ij} is nonzero if and only if $k = j$. Hence, this sum simply becomes

$$(E^{ij}A)_{ib} = A_{jb}$$

so the i^{th} row of this product is indeed the j^{th} row of A .

This is quite a lot of detail, but it's good to include a lot when starting out. Once you become more comfortable with rigor, you can relax a bit. Oftentimes, good writing comes from choosing which details to include and which to skip, but for now I'd suggest including a lot so that you learn how to do so.

- (2) The typical argument goes as follows. Let I be a two sided ideal of $M_n(R)$. Define the ideal J of R via $J = \{a \in R : a \text{ is a coefficient in some } A \in I\}$. Prove that J is indeed an ideal of R . Prove that $I = M_n(J)$.

The most common mistake was in not proving the last step. By definition of J , it's clear that $I \subseteq M_n(J)$, but the converse is not so obvious. This is needed to show that all ideals of $M_n(R)$ are actually of this form, not just contained in an ideal of the form $M_n(J)$.

- (3) The most common mistake here was in assuming that ring multiplication is cancellative, i.e. that if $ab = ac$ then $b = c$. This isn't in general true. For one, if $a = 0$ then $ab = ac$ regardless of what b and c are. Furthermore, if the ring has zero divisors then multiplication by a is not injective (in fact, that's exactly what a being a zero divisor means). For example, take $R = \mathbb{Z}/6\mathbb{Z}$ and let $a = 2 + 6\mathbb{Z}$, $b = 3 + 6\mathbb{Z}$, and $c = 0 + 6\mathbb{Z}$. Then $ab = ac = 0 + 6\mathbb{Z}$ but $b \neq 0 + 6\mathbb{Z}$.

- (4) The typical argument went as follows. Let $\mathfrak{m}_a = \{f \in R : f(a) = 0\}$, where $R = C([0, 1])$. Take a maximal ideal $\mathfrak{m}$ of R . Suppose for all a that $\mathfrak{m} \neq \mathfrak{m}_a$. Derive a contradiction via compactness to conclude that this condition forces $\mathfrak{m}$ to contain a unit.

The most common issue was that the assumption used was almost always that $\mathfrak{m}$ is not contained in any $\mathfrak{m}_a$, meaning that the contradiction proof would only show that $\mathfrak{m} \subseteq \mathfrak{m}_a$ for some a . One must also show the reverse containment. This is a minor point really, since the proof is just one line: $\mathfrak{m}$ is maximal by hypothesis and each $\mathfrak{m}_a$ is maximal, and containment is the same as equality for maximal ideals. But one should check details like this.

Also, I think the cleanest way to prove that $\mathfrak{m}_a$ is a maximal ideal is to consider the map $R \rightarrow \mathbb{R}$ via $f \mapsto f(a)$. This is onto and its kernel is $\mathfrak{m}_a$, so by the first isomorphism theorem, $R/\mathfrak{m}_a$ is isomorphic to $\mathbb{R}$, a field. Thus, the kernel is maximal. This also immediately proves that $\mathfrak{m}_a$ is an ideal. I think this is a good technique in general, always think about what modding out by an ideal does and what maps you can define out of the quotient. If you have an ideal $I \subseteq R$, try to find a map $R \rightarrow S$ which vanishes on I , which then induces a map $R/I \rightarrow S$.

- (5) There weren't many mistakes in this one, so I'll just make a few remarks.

One, is that you need to prove Pascal's identity

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$$

This can be done by expanding both sides with factorials and doing some algebra. This is an important proof technique - you should know how to manually compute! But with many combinatorial identities, there are other perhaps more conceptual answers. Often, you can prove an identity by counting the same set in two ways.

In this case, $\binom{n+1}{k+1}$ counts the number of subsets of size $k+1$ in a set of size $n+1$. How can we split this into two disjoint counting problems - one for $\binom{n}{k}$ and another for $\binom{n}{k+1}$? Take a set A of size $n+1$ and fix an element $a \in A$. We are counting subsets S of A so that $|S| = k+1$. There are two disjoint possibilities - either S contains a or it does not. If $a \in S$ then determining S is the same as determining $S - \{a\}$ inside $A - \{a\}$. So the number of S with $a \in S$ is the number of size k subsets in $A - \{a\}$, which is $\binom{n}{k}$. On the other hand, if $a \notin S$ then $S \subseteq A - \{a\}$, so the possibilities for S here are all the $k+1$ sized subsets of $A - \{a\}$. There are $\binom{n}{k+1}$ of these. These two cases on S are disjoint, so we have shown $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

This proof is also useful because it gives a recursive algorithm to enumerate all the size k subsets of a given set A , you fix an element $a \in A$ and consider the subsets of size k in $A - \{a\}$ and the subsets of size $k-1$ in A . Both these are smaller problems, so this can be done recursively. Try this for some small examples to get a handle of it!

One additional subtlety to consider is what it even means to write $\binom{n}{k}r$ for r in some ring R . A ring R doesn't generally contain $\mathbb{Z}$, so we must interpret this correctly. It just means to add R to itself $\binom{n}{k}$ many times. In very fancy terms, there is a unique map $\mathbb{Z} \rightarrow R$ for any ring R , so any ring is a $\mathbb{Z}$ -algebra and thus inherits some notion of scalar multiplication by elements of $\mathbb{Z}$. More generally, any ring map $f : A \rightarrow B$ makes B into an A -algebra, which lets us treat elements of a as scalars in B via $a * b := f(a)b$.

- (6) (a) This was mostly correct, so I want to point out that this formula for $(1+x)^{-1}$ is basically

the geometric series formula. Indeed, we know the power series

$$\frac{1}{1+x} = \sum_{n \geq 0} (-1)^n x^n$$

This is a purely formal identity, so as long as plugging in $x = a$ makes sense, it works for any element a of any ring R . The issue of course is that this sum is infinite, so maybe we need a metric (really, a topology) on R to make sense of convergence. But in the nilpotent case, the series becomes finite!

- (b) The biggest issue was in not proving that the nilradical is closed under addition. Most people recognized that you have to use the binomial theorem, but why does that binomial expansion vanish? Generally, proving that a sum is 0 isn't very easy, so it requires justification. Here we get lucky that there's no clever cancellation needed - every term in the sum will be 0, but this should be proven.
- (c) First off, there were some common notational issues. When starting off, you should be completely rigorous and explicit without any real abuse of notation. It was very common to write something like "Let $x \in \mathbb{Z}/n\mathbb{Z}$ be nilpotent, so $x^k = 0$ for some $k \geq 1$. That is, $n|x^k$ for some $k \geq 1$ ". But here, x is not an integer. It's an equivalence class of integers under the $(\text{mod } n)$ relation. It is quite common to identify elements of quotient rings with some representing object, but this is in a literal sense logically incorrect (hence why we use the violent term *abuse* of notation). I'd suggest being careful and explicit about this. Instead, you could write "Let $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ be nilpotent. Then there is some $k \geq 1$ so that $n|x^k$ in $\mathbb{Z}$ ".

Similarly, it was common to see the divisibility relation in $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ conflated. That is, many wrote $6 | \bar{x}$ in $\mathbb{Z}/12\mathbb{Z}$. Strictly, one should write $\bar{6}$. One of the key reasons for abstract ring theory was making sense of what divisibility means, and the conclusion is that it fundamentally depends on your ring!

On that note, I'd suggest always writing ideals of a quotient ring using the correspondence principle. For instance, it was common to see

$$\text{nil}(\mathbb{Z}/12\mathbb{Z}) = \{\bar{x} \in \mathbb{Z}/12\mathbb{Z} : \bar{6} | \bar{x}\}$$

which is better written as $6\mathbb{Z}/12\mathbb{Z}$. This allows for a uniform notation, and is very useful in computation (such as when using the third isomorphism theorem). Additionally, this notation makes it easier to correctly abuse notation between a ring and its quotient. You will surely sometimes write an ideal in a quotient ring via an explicit generating set, but it's easiest to think of quotient rings via the correspondence principle.

Finally, there were some actual logical errors. Mostly, proofs were not completed. For instance, restating the definition like

$$\text{nil}(\mathbb{Z}/n\mathbb{Z}) = \{\bar{x} \in \mathbb{Z}/n\mathbb{Z} : \exists k \geq 1 \text{ such that } n|x^k \text{ in } \mathbb{Z}\}$$

isn't a sufficient answer. Here, we want an explicit ideal, i.e. one written as $d\mathbb{Z}/n\mathbb{Z}$ for an explicit divisor d of n .

Another common issue was not proving both containments in an equality. Namely, it was common to see "every element satisfying property P is nilpotent, thus the nilradical is the set of elements of $\mathbb{Z}/n\mathbb{Z}$ which satisfy property P ". Most often, people got the nilradical right, but to prove this rigorously also requires showing that every element of the nilradical satisfies property P .

- (7) The main issues were in proving $R \cong Re \times Re'$. Most people constructed a map $\phi : R \longrightarrow Re \times Re'$ via $r \mapsto (re, re')$. A common mistake was saying this is “obviously” injective and surjective. You should almost never use words like “obviously”, “trivially”, “clearly”, etc, at this stage (though it’s also somewhat poor form for acclaimed mathematicians to use them). In this case, there are subtleties that must be considered.

For injectivity, why can’t multiplication by e and e' lose information? Multiplying by a zero divisor does lose information (ie the multiplication map isn’t injective), so why doesn’t that happen here? Note that unless e or e' are 1, these idempotents *will* be zero divisors (as $ee' = 0$). So it is critical to use that they are idempotents and that they are orthogonal, but the phrase “obviously” makes it unclear that you’ve used these hypotheses.

Similarly, for surjectivity, a generic element of the codomain is of the form (ae, be') whereas a generic element of the image is of the form (re, re') . Why does a always represent elements of the codomain with $a = b$? This isn’t very obvious, or at least it wasn’t to me when I first thought about it!

Finally, a suggestion whenever you want to show an isomorphism is to consider the inverse. Sometimes this can make your argument a bit cleaner, since proving surjectivity will often look like defining an inverse (and injectivity means that “inverse” is actually well defined). Furthermore, it’s nice knowing both sides, ie how to go back and forth. In this case, the inverse is $Re \times Re' \longrightarrow R$ via $(a, b) \mapsto a + b$.

- (8) There weren’t really any notable mistakes here. One thing to note is that if you wanna sit around and check ring axioms, distributivity is somewhat notable. For any functions, the equation $(f + g) \circ h = f \circ h + g \circ h$ is true. The other distributivity, i.e. $f \circ (g + h) = f \circ g + f \circ h$ is where you use that f is a group homomorphism.