Proof of Theorem 24 (which we started last time). The last thing we did last time was to check \( f \), as defined, was a homomorphism.

\[
\begin{align*}
    f([a]_{MN} + [b]_{MN}) &= f([a + b]_{MN}) = ([a + b], [a + b]_N) = ([a]_{M} + [b]_{M}, [a]_{N} + [b]_{N}) \\
    &= ([a]_{M}, [a]_{N}) + ([b]_{M}, [b]_{N}) = f([a]_{MN}) + f([b]_{MN}) \\
    f([a]_{MN} \times [b]_{MN}) &= f([ab]_{MN}) = ([ab], [ab]_N) = ([a]_{M} \times [b]_{M}, [a]_{N} \times [b]_{N}) \\
    &= ([a]_{M}, [a]_{N}) \times ([b]_{M}, [b]_{N}) = f([a]_{MN}) \times f([b]_{MN})
\end{align*}
\]

Now, once we know \( f \) is a homomorphism, all we need to check is that \( f \) is bijective. That is, we must check \( f \) is surjective and injective. To check it is injective, we use the test we gave above. Suppose that \( f([a]_{MN}) = ([a]_{M}, [a]_{N}) \) is the 0 element in \( \mathbb{Z}/M \times \mathbb{Z}/N \). Then \([a]_{M} = 0\), which means \( a \) is a multiple of \( M \). Similarly \( a \) is a multiple of \( N \). It follows that \( a \) is a multiple of \( MN \), so \([a]_{MN} = 0\).

To check it is surjective, we use the following argument. By Euclid, there are numbers \( k, l \) such that \( kM + lN = 1 \). Then given any \([ab], [a]_{N}\) in \( \mathbb{Z}/M \times \mathbb{Z}/N \), we must show it is in the image of \( f \). But

\[
\begin{align*}
    f([kMa + lNb]_{MN}) &= ([kMa + lNb]_{M}, [kMa + lNb]_{N}) \\
    &= ([kMa + (1 - kM)b]_{M}, [(1 - lN)a + lNb]_{N}) \\
    &= ([kM(a - b) + b]_{M}, [a + lN(b - a)]_{N}) \\
    &= ([b]_{M}, [a]_{N})
\end{align*}
\]

This completes the proof.

\[\square\]

§3. Unique factorization in rings.—Although integral domains are significantly more ‘like \( \mathbb{Z} \)’ than general rings are, they can still differ from \( \mathbb{Z} \) in many important respects. In particular, the unique factorization properties which we studied in the first section of the course could easily go awry. Nonetheless, unique factorization will ‘work’ for many domains. In this section, we will try to understand a little about some domains it works for, and why. First, we must introduce some terminology.

**Definition 1.** Suppose \( R \) is a ring. An element \( u \) in \( R \) is called a unit if there is some \( u' \) such that \( uu' = 1 \). (So, for instance, a field is precisely a ring in which every nonzero element is a unit.) An non-unit element \( t \) is irreducible if whenever we can write \( t = ab \), either \( a \) or \( b \) is a unit.

Our goal, for this section of the course, is to look for reasons why a ring might have the property that every element can be uniquely factorized into irreducible elements. When we say ‘uniquely’, we mean that the expression is unique up to \((a)\) reordering and \((b)\) multiplying the primes in the list by units.

Our first goal, as in §1, is to see why every element can be factorized into irreducible elements at all. The key idea is a notion of size.

**Definition 2.** Suppose \( R \) is an integral domain. A size function is a function \( f : R \to \mathbb{Z}_{\geq 0} \) with the properties that

- \( f(ab) = f(a)f(b) \) for all \( a, b \in R \)
- for \( a \in R \), \( f(a) = 0 \) implies \( a \) is 0
- for \( a \in R \), \( f(a) = 1 \) implies \( a \) is a unit