Math 533 Winter 2021, Lecture 4: Rings and ideals

website: `https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

1. Rings and ideals (cont'd)

1.1. Quotient rings ([DF, §7.1]) (cont'd)

I am going to use a result that I forgot to state last time: a characterization of injectivity in terms of kernels.

Lemma 1.1.1. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, f is injective if and only if $\operatorname{Ker} f = \{0_R\}$.

Proof. You probably have seen the analogous results for groups or vector spaces. If so, then you can just recall the analogous result for groups, and apply it to the additive groups $(R, +, 0)$ and $(S, +, 0)$ (since the ring morphism f is clearly a group morphism from $(R, +, 0)$ to $(S, +, 0)$).

If not, here is the proof: The $\Longrightarrow$ direction is easy (assume that f is injective; then, each $x \in \operatorname{Ker} f$ satisfies $f(x) = 0 = f(0)$ and thus $x = 0$ because f is injective; thus $\operatorname{Ker} f \subseteq \{0_R\}$; but this entails $\operatorname{Ker} f = \{0_R\}$ since 0_R always lies in $\operatorname{Ker} f$). For the $\Longleftarrow$ direction, assume that $\operatorname{Ker} f = \{0_R\}$. Now, if $a, b \in R$ satisfy $f(a) = f(b)$, then $f(a - b) = f(a) - f(b) = 0$ and thus $a - b \in \operatorname{Ker} f = \{0_R\}$, so that $a - b = 0$ and thus $a = b$. But this means that f is injective. This proves the $\Longleftarrow$ direction and thus completes the proof of the lemma. □

Now, let us recall the last theorem we proved in the previous lecture:

Theorem 1.1.2 (Universal property of quotient rings)**.** Let R be a ring. Let I be an ideal of R.

Let S be a ring. Let $f : R \to S$ be a ring morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Consider the canonical projection $\pi : R \to R/I$. Then, there is a unique ring morphism $f' : R/I \to S$ satisfying $f = f' \circ \pi$.

Recall again how this morphism f' was defined: It satisfies

$$f'(r + I) = f(r) \qquad \text{for each } r \in R. \tag{1}$$

In other words, $f'(\overline{r}) = f(r)$ for each $r \in R$ (since $\overline{r}$ is a synonym for the coset $r + I$). Thus, roughly speaking, f' sends a residue class where f would send any element of this residue class.

Using the universal property of quotient rings, we can get the following fact:

Theorem 1.1.3 (First isomorphism theorem for rings)**.** Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Recall that $\operatorname{Ker} f$ is an ideal of R, and that $\operatorname{Im} f = f(R)$ is a subring of S. We have

$$R/\operatorname{Ker} f \cong f(R).$$

More precisely, the universal property of quotient rings (applied to $I = \operatorname{Ker} f$) yields a ring morphism $f' : R/\operatorname{Ker} f \to S$, which (if we restrict its target to its actual image $f(R)$) is a ring isomorphism from $R/\operatorname{Ker} f$ to $f(R)$.

Before I prove this theorem, let me clarify what I mean by "if we restrict its target". If $g : U \to V$ is a map from a set U to a set V, then V is called the **target** (or **codomain**) of g. However, the image $g(U)$ of g might well be smaller than V. For example, the map

$$\mathbb{Z} \to \mathbb{Z}, \qquad n \mapsto 2n \tag{2}$$

has target $\mathbb{Z}$, but its image is only $2\mathbb{Z}$ (the set of all even integers). If $g : U \to V$ is a map, and if W is a subset of V such that $g(U) \subseteq W$ (for example, in the example we just gave, we could take $W = 2\mathbb{Z}$), then we can **restrict the target** of g to W, which means we replace the target of g by W. Thus, we obtain a map from U to W that takes the same values as g on all inputs (i.e., it sends each $u \in U$ to $g(u)$, just like the map g does), but has codomain W instead of V. If $W = g(U)$, then this new map from U to W will be surjective. For example, if we restrict the target of the map (2) to $2\mathbb{Z}$, then we obtain the map

$$\mathbb{Z} \to 2\mathbb{Z}, \qquad n \mapsto 2n,$$

which is surjective.

In the theorem above, we restrict the target of the map $f' : R/\operatorname{Ker} f \to S$ to $f(R)$, thus obtaining a map $R/\operatorname{Ker} f \to f(R)$. (This presupposes that the image of f' is contained in $f(R)$ – but this is indeed the case, as we will show in the proof of the theorem. Better yet, the image of f' **is** $f(R)$.)

All this said, let's prove the theorem now:

Proof of the theorem. We know that f' is a ring morphism from $R/\operatorname{Ker} f$ to S. Its image is

$$\begin{aligned} f'(R/\operatorname{Ker} f) &= \left\{ f'(x) \mid x \in R/\operatorname{Ker} f \right\} = \left\{ \underbrace{f'(r + \operatorname{Ker} f)}_{\substack{= f(r) \\ \text{(by (1))}}} \mid r \in R \right\} \\ &\qquad \left(\begin{array}{c} \text{since the elements } x \in R/\operatorname{Ker} f \text{ are precisely} \\ \text{the cosets } r + \operatorname{Ker} f \text{ for } r \in R \end{array} \right) \\ &= \left\{ f(r) \mid r \in R \right\} = f(R). \end{aligned}$$

Thus, in particular, $f'(R/\operatorname{Ker} f) \subseteq f(R)$. Hence, we can restrict the target of f' to $f(R)$. The resulting map $f'' : R/\operatorname{Ker} f \to f(R)$ is a ring morphism from $R/\operatorname{Ker} f$ to $f(R)$, and is furthermore surjective (because its image is $f'(R/\operatorname{Ker} f) = f(R)$).

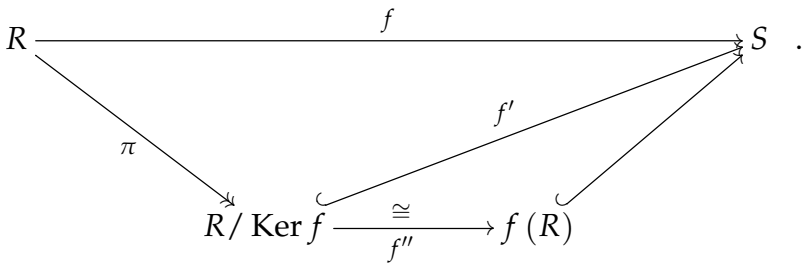
Now, we shall prove that f'' is injective. Indeed, this is equivalent to f' being injective (since f'' differs from f' only in its choice of target). According to the previous lemma, we can show that f' is injective by showing that $\operatorname{Ker} f' = \left\{0_{R/\operatorname{Ker} f}\right\}$ (since f' is a ring morphism). So let us show this. Clearly, $\left\{0_{R/\operatorname{Ker} f}\right\} \subseteq \operatorname{Ker} f'$ (since $f'\left(0_{R/\operatorname{Ker} f}\right) = 0$ and thus $0_{R/\operatorname{Ker} f} \in \operatorname{Ker} f'$), so we only need to check that $\operatorname{Ker} f' \subseteq \left\{0_{R/\operatorname{Ker} f}\right\}$.

So let $x \in \operatorname{Ker}(f')$. Thus, $x \in R/\operatorname{Ker} f$, so $x = r + \operatorname{Ker} f$ for some $r \in R$ (since every element of $R/\operatorname{Ker} f$ has this form). Consider this r. From $x = r + \operatorname{Ker} f$, we obtain $f'(x) = f'(r + \operatorname{Ker} f) = f(r)$ (by (1)), so that $f(r) = f'(x) = 0$ (since $x \in \operatorname{Ker}(f')$). This entails $r \in \operatorname{Ker} f$. Hence, $r + \operatorname{Ker} f = 0 + \operatorname{Ker} f = 0_{R/\operatorname{Ker} f}$, so $x = r + \operatorname{Ker} f = 0_{R/\operatorname{Ker} f}$.

Forget that we fixed x. We thus have shown that $x = 0_{R/\operatorname{Ker} f}$ for each $x \in \operatorname{Ker}(f')$. In other words, $\operatorname{Ker} f' \subseteq \left\{0_{R/\operatorname{Ker} f}\right\}$. As we have explained above, this completes the proof that f' is injective. Hence, f'' is injective.

Now, we know that the morphism $f'' : R/\operatorname{Ker} f \to f(R)$ is injective and surjective. Hence, this morphism is bijective, thus invertible. Hence, it is a ring isomorphism (since we have already shown that an invertible ring morphism is always a ring isomorphism). □

So we have proved the first isomorphism theorem for rings. Let us illustrate it with a commutative diagram:



Let me explain what you are seeing here: On top is the original ring morphism $f : R \to S$. The other four arrows are

- the canonical projection $\pi : R \to R/\operatorname{Ker} f$, sending each $r \in R$ to its residue class $r + \operatorname{Ker} f \in R/\operatorname{Ker} f$;
- the morphism $f' : R/\operatorname{Ker} f \to S$ obtained from the universal property of quotient rings;
- the isomorphism $f'' : R/\operatorname{Ker} f \to f(R)$ claimed by the theorem (obtained by restricting the target of f');

- the canonical inclusion $f(R) \to S$ (which just sends each element to itself).

The special shapes of the arrows signify certain properties:

- An arrow of shape $\hookrightarrow$ stands for an injective map. (And indeed, the canonical inclusion $f(R) \to S$ is injective. So is the morphism f', as we have shown in the proof above.)
- An arrow of shape $\twoheadrightarrow$ stands for a surjective map. (And indeed, the canonical projection π is surjective.)
- An arrow with a $\cong$ sign above (or below) it stands for an isomorphism. (And indeed, our f'' is an isomorphism.)

The diagram is commutative. Indeed, the top triangle is commutative because $f = f' \circ \pi$; the bottom triangle is commutative since the maps f'' and f' agree in all their values (and since the canonical inclusion $f(R) \to S$ sends each element to itself).

Note that all five arrows in our diagram are ring morphisms; we say that we have a **diagram of rings**.

Thus, the first isomorphism theorem for rings shows that each ring morphism can be decomposed (in a natural way) into a composition of a surjective ring morphism, a ring isomorphism and an injective ring morphism.

There are also a second, third and fourth isomorphism theorems. You will meet them soon. (In particular, the second and the third isomorphism theorems appear as exercises 9 and 8 on homework set #2.)

1.2. Direct products of rings ([DF, §7.6])

Here is a way of building new rings from old[1]:

Proposition 1.2.1. Let R and S be two rings. Then, the Cartesian product

$$R \times S = \{\text{all pairs } (r,s) \text{ with } r \in R \text{ and } s \in S\}$$

becomes a ring if we endow it with the entrywise addition and multiplication operations (i.e., addition defined by $(r,s) + (r',s') = (r+r', s+s')$, and multiplication defined by $(r,s) \cdot (r',s') = (rr', ss')$) and the zero $(0_R, 0_S)$ and the unity $(1_R, 1_S)$.

Definition 1.2.2. This ring is denoted by $R \times S$ and called the **direct product** of R and S.

[1] There are several other such ways. We will see a few in this course.

Proof of the Proposition. Straightforward. For example, in order check the associativity of multiplication, we need to check that

$$(r,s)\left((r',s')(r'',s'')\right) = \left((r,s)(r',s')\right)(r'',s'') \quad \text{for all } (r,s),(r',s'),(r'',s'') \in R \times S.$$

We can do this by computing both sides and comparing: We have

$$(r,s)\left((r',s')(r'',s'')\right) = (r,s)(r'r'',s's'') = \left(r(r'r''), s(s's'')\right) \quad \text{and}$$
$$\left((r,s)(r',s')\right)(r'',s'') = (rr',ss')(r'',s'') = \left((rr')r'', (ss')s''\right).$$

The right hand sides of these equalities are equal, since $r(r'r'') = (rr')r''$ and $s(s's'') = (ss')s''$. Thus, the left hand sides are equal as well; this proves the associativity of multiplication. All other axioms follow similarly. □

More generally, we can define direct products $R_1 \times R_2 \times \cdots \times R_n$ of any number of rings in the same way (but using n-tuples instead of pairs). Even more generally, we can define the direct product $\prod_{i \in I} R_i$ of any family of rings (including infinite families):

Proposition 1.2.3. Let I be any set. Let $(R_i)_{i \in I}$ be a family of rings (i.e., let R_i be a ring for each $i \in I$). Then, the Cartesian product

$$\prod_{i \in I} R_i = \left\{\text{all families } (r_i)_{i \in I} \text{ with } r_i \in R_i \text{ for each } i \in I\right\}$$

becomes a ring if we endow it with the entrywise addition and multiplication operations (i.e., addition defined by $(r_i)_{i \in I} + (s_i)_{i \in I} = (r_i + s_i)_{i \in I}$, and multiplication defined by $(r_i)_{i \in I} \cdot (s_i)_{i \in I} = (r_i s_i)_{i \in I}$) and the zero $\left(0_{R_i}\right)_{i \in I}$ and the unity $\left(1_{R_i}\right)_{i \in I}$.

Definition 1.2.4. This ring is denoted by $\prod_{i \in I} R_i$ and called the **direct product** of the rings R_i.

If $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then this ring is also denoted by $R_1 \times R_2 \times \cdots \times R_n$, and we identify a family $(r_i)_{i \in I} = (r_i)_{i \in \{1,2,\ldots,n\}}$ with the n-tuple $(r_1, r_2, \ldots, r_n)$. (Thus, the elements of $R_1 \times R_2 \times \cdots \times R_n$ are n-tuples whose entries belong to $R_1, R_2, \ldots, R_n$, respectively.)

If all the rings R_i are equal to some ring R, then their direct product $\prod_{i \in I} R_i = \prod_{i \in I} R$ is also denoted R^I. Note that this is the same notation that we previously used for the ring of all functions from I to R (with entrywise addition and multiplication); however, the notations don't really clash, since these two rings are the same (at least if we identify a function $f : I \to R$ with the family $(f(i))_{i \in I}$).

If $n \in \mathbb{N}$, and if R is a ring, then the ring $R^{\{1,2,\ldots,n\}} = \underbrace{R \times R \times \cdots \times R}_{n \text{ times}}$ is also called R^n.

Here are some examples of direct products:

- The ring $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ consists of all triples (r, s, t) of integers. They are added and multiplied entrywise: For example, $(r, s, t) \cdot (r', s', t') = (rr', ss', tt')$.

  Note that this ring is **not** an integral domain, since $(0, 1, 0) \cdot (1, 0, 0) = (0, 0, 0)$.

- If R, S and T are three rings, then the direct products $R \times S \times T$ and $(R \times S) \times T$ are not quite the same (e.g., the former consists of triples (r, s, t), while the latter consists of nested pairs $((r, s), t)$); but they are isomorphic through a rather obvious isomorphism: Namely, the map

$$R \times S \times T \to (R \times S) \times T,$$
$$(r, s, t) \mapsto ((r, s), t)$$

  is a ring isomorphism. This is a quick test of understanding – if you understand the definitions, then this should be completely obvious to you. Similarly, the rings $R \times S \times T$ and $R \times (S \times T)$ are isomorphic. You can easily generalize this to direct products of more than three rings. We say that the direct product of rings is "associative up to isomorphism".

- The ring $\mathbb{C}$ consists of complex numbers, which are defined as pairs of real numbers. Thus, $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ as sets. Since complex numbers are added entrywise, we even have $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ as additive groups (i.e., the additive groups $(\mathbb{C}, +, 0)$ and $(\mathbb{R} \times \mathbb{R}, +, 0)$ are identical). However, $\mathbb{C}$ is **not** $\mathbb{R} \times \mathbb{R}$ as rings (because complex numbers are not multiplied entrywise). Even worse, $\mathbb{C}$ is not even isomorphic to $\mathbb{R} \times \mathbb{R}$ as rings. One way to see this is by noticing that $\mathbb{C}$ is an integral domain (even a field) whereas $\mathbb{R} \times \mathbb{R}$ is not (for example, $(1, 0) \cdot (0, 1) = (0, 0)$). Another way to see this is by noticing that $-1_{\mathbb{C}}$ is a square in $\mathbb{C}$, but $-1_{\mathbb{R} \times \mathbb{R}} = (-1, -1)$ is not a square in $\mathbb{R} \times \mathbb{R}$.

  Note that these arguments make sense because isomorphic rings "behave the same" as far as their properties are concerned – at least those properties that can be stated in terms of the ring itself. For example, if R and S are two isomorphic rings, and if one of R and S is a field, then so is the other. For yet another example, if R and S are two isomorphic rings, and R has (say) 15 units, then so does S. For yet another example, if R and S are two isomorphic rings, and R satisfies some property like "$x(x + 1_R)(x - 1_R) = 0$ for all $x \in R$", then so does S (with 1_R replaced by 1_S). The only properties of a ring that are not preserved under

isomorphism are properties that refer to specific "outside" objects (for example, the rings $R \times S \times T$ and $(R \times S) \times T$ from the previous example are isomorphic, but the former contains the triple $(1,1,1)$ whereas the latter doesn't). This all is a general feature of isomorphisms of any sorts of objects – not just of rings but also of groups, vector spaces and topological spaces.

- Let R be any ring. Let $n \in \mathbb{N}$. Let D_n be the set of all **diagonal** matrices in the matrix ring $R^{n \times n}$. For example,

$$D_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in R \right\} = \left\{ \operatorname{diag}(a,b) \mid a, b \in R \right\},$$

where we are using the notation

$$\begin{aligned} \operatorname{diag}(a_1, a_2, \ldots, a_n) &= (\text{the diagonal matrix with diagonal } (a_1, a_2, \ldots, a_n)) \\ &= \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}. \end{aligned}$$

Then, it is easy to see that D_n is a subring of $R^{n \times n}$. Moreover, $D_n \cong R^n$ as rings (where, as we recall, $R^n = \underbrace{R \times R \times \cdots \times R}_{n \text{ times}} = R^{\{1,2,\ldots,n\}}$). Indeed, the map

$$\begin{aligned} R^n &\to D_n, \\ (a_1, a_2, \ldots, a_n) &\mapsto \operatorname{diag}(a_1, a_2, \ldots, a_n) \end{aligned}$$

is a ring isomorphism. For example, it respects multiplication, since

$$\operatorname{diag}(a_1, a_2, \ldots, a_n) \cdot \operatorname{diag}(b_1, b_2, \ldots, b_n) = \operatorname{diag}(a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

for any $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in R^n$.

It is easy to see that a direct product of commutative rings is commutative.

1.3. A few operations on ideals ([DF, §7.3])

Next, we shall see three ways to build new ideals of a ring from old:

Definition 1.3.1. Let I and J be two ideals of a ring R.
(a) Then, $I + J$ denotes the subset

$$\{i + j \mid i \in I \text{ and } j \in J\} \text{ of } R.$$

(b) Next, we define a further subset IJ, also denoted $I \cdot J$. Unlike $I + J$, this will **not** be defined as $\{i \cdot j \mid i \in I \text{ and } j \in J\}$. Instead, $IJ = I \cdot J$ will be defined as the set

$$\{\text{all finite sums of } (I,J)\text{-products}\},$$

where an (I,J)**-product** means a product of the form ij with $i \in I$ and $j \in J$. In other words,

$$IJ = \{i_1 j_1 + i_2 j_2 + \cdots + i_k j_k \mid k \in \mathbb{N} \text{ and } i_1, i_2, \ldots, i_k \in I \text{ and } j_1, j_2, \ldots, j_k \in J\}.$$

Note that our definition of IJ was more complicated than the one of $I + J$, as it involved an additional step (viz., taking finite sums). The purpose of this step is to ensure that IJ is closed under addition (which will later be used to argue that IJ is an ideal of R). It is forced to us if we try to construct an ideal of R that contains all (I,J)-products. We could have added the same step to our definition of $I + J$, but it would not have changed anything, since a finite sum of (I,J)-sums (i.e., of sums of the form $i + j$ with $i \in I$ and $j \in J$) can be rewritten as a single (I,J)-sum:

$$\begin{aligned}
&(i_1 + j_1) + (i_2 + j_2) + \cdots + (i_k + j_k) \\
&= \underbrace{(i_1 + i_2 + \cdots + i_k)}_{\substack{\in I \\ \text{(since } I \text{ is closed under addition)}}} + \underbrace{(j_1 + j_2 + \cdots + j_k)}_{\substack{\in J \\ \text{(since } J \text{ is closed under addition)}}}.
\end{aligned}$$

For (I,J)-products, however, this is not generally the case (although you won't find a counterexample for $R = \mathbb{Z}$).

We will use the following assortment of facts (see Exercise 8 on homework set #1 for proofs):[2]

Proposition 1.3.2. (a) Let I and J be two ideals of a ring R. Then, $I + J$ and $I \cap J$ and IJ are ideals of R as well.

(b) Let I and J be two ideals of a ring R. Then, $IJ \subseteq I \cap J \subseteq I \subseteq I + J$ and $IJ \subseteq I \cap J \subseteq J \subseteq I + J$.

(c) The set of all ideals of R is a monoid with respect to the binary operation $+$, with neutral element $\{0_R\} = 0R$. That is,

$$\begin{aligned}
(I + J) + K &= I + (J + K) && \text{for any three ideals } I, J, K \text{ of } R; \\
I + \{0_R\} &= \{0_R\} + I = I && \text{for any ideal } I \text{ of } R.
\end{aligned}$$

[2] Recall that if R is any ring, then the one-element set $\{0_R\}$ and the entire ring R are ideals of R. Both of these ideals are principal ($\{0_R\} = 0_R R$ and $R = 1_R R$); they "bookend" all ideals of R (in the sense that $\{0_R\} \subseteq I \subseteq R$ for each ideal I of R).

(d) The set of all ideals of R is a monoid with respect to the binary operation $\cap$, with neutral element $R = 1R$. That is,

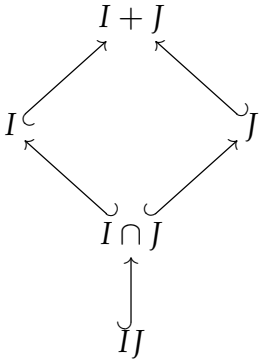
$$(I \cap J) \cap K = I \cap (J \cap K) \qquad \text{for any three ideals } I, J, K \text{ of } R;$$
$$I \cap R = R \cap I = I \qquad \text{for any ideal } I \text{ of } R.$$

(e) The set of all ideals of R is a monoid with respect to the binary operation $\cdot$, with neutral element $R = 1R$. That is,

$$(IJ)\,K = I\,(JK) \qquad \text{for any three ideals } I, J, K \text{ of } R;$$
$$IR = RI = I \qquad \text{for any ideal } I \text{ of } R.$$

This is known as **ideal arithmetic**. Keep in mind that it has no subtraction and no division.

Here is a diagram showing the inclusions between the ideals $IJ, I \cap J, I + J, I, J$:



(Recall that an arrow of type $X \hookrightarrow Y$ means a canonical inclusion from X to Y, which entails that $X \subseteq Y$.)

The following proposition tells us how ideal arithmetic looks like when we apply it to principal ideals of $\mathbb{Z}$:

Proposition 1.3.3. Let $n, m \in \mathbb{Z}$. Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$. Then:
(a) We have $IJ = nm\mathbb{Z}$.
(b) We have $I \cap J = \operatorname{lcm}(n, m)\,\mathbb{Z}$.
(c) We have $I + J = \gcd(n, m)\,\mathbb{Z}$.

Proof. **(a)** From $n \in I$ and $m \in J$, we see that nm is an (I, J)-product. Thus, nm is a finite sum of (I, J)-products (of just one, to be precise). In other words, $nm \in IJ$. Since IJ is an ideal of $\mathbb{Z}$, this entails that every multiple of nm also belongs to IJ; in other words, $nm\mathbb{Z} \subseteq IJ$.

Conversely: If $i \in I$ and $j \in J$, then $i = nx$ for some $x \in \mathbb{Z}$ (since $i \in I = n\mathbb{Z}$) and $j = my$ for some $y \in \mathbb{Z}$ (since $j \in J = m\mathbb{Z}$) and therefore $ij = (nx)\,(my) = nm\,(xy) \in nm\mathbb{Z}$. Thus, every (I, J)-product belongs to $nm\mathbb{Z}$ (because an (I, J)-product always has the form ij for some $i \in I$ and $j \in J$). Hence, any sum of

(I, J)-products also belongs to $nm\mathbb{Z}$ (since $nm\mathbb{Z}$ is closed under addition). In other words, $IJ \subseteq nm\mathbb{Z}$ (since any element of IJ is a sum of (I, J)-products). So $IJ = nm\mathbb{Z}$ (since we already have seen that $nm\mathbb{Z} \subseteq IJ$).

(b) We have

$$\begin{aligned} I \cap J &= \{\text{all elements of } I \text{ that also belong to } J\} \\ &= \{\text{all multiples of } n \text{ that also are multiples of } m\} \\ &\qquad \left(\begin{array}{c} \text{since } I = n\mathbb{Z} = \{\text{all multiples of } n\} \\ \text{and } J = m\mathbb{Z} = \{\text{all multiples of } m\} \end{array} \right) \\ &= \{\text{all common multiples of } n \text{ and } m\} \\ &= \{\text{all multiples of } \operatorname{lcm}(n, m)\} \\ &\qquad \left(\begin{array}{c} \text{since a result in elementary number theory} \\ \text{says that the common multiples of } n \text{ and } m \\ \text{are precisely the multiples of } \operatorname{lcm}(n, m) \end{array} \right) \\ &= \operatorname{lcm}(n, m)\, \mathbb{Z}. \end{aligned}$$

(c) First, we shall show that $I + J \subseteq \gcd(n, m)\, \mathbb{Z}$. Indeed, any element of I is a multiple of n (since $I = n\mathbb{Z}$), thus a multiple of $\gcd(n, m)$ (since n is a multiple of $\gcd(n, m)$). Similarly, any element of J is a multiple of $\gcd(n, m)$. Thus, an element of $I + J$ is a sum of two multiples of $\gcd(n, m)$, and therefore itself a multiple of $\gcd(n, m)$. In other words, any element of $I + J$ belongs to $\gcd(n, m)\, \mathbb{Z}$. In other words, $I + J \subseteq \gcd(n, m)\, \mathbb{Z}$.

Now, we need to prove that $\gcd(n, m)\, \mathbb{Z} \subseteq I + J$. For this, it suffices to show that $\gcd(n, m) \in I + J$, because $I + J$ is an ideal (and thus will contain any multiple of $\gcd(n, m)$ once we know it contains $\gcd(n, m)$). But Bezout's theorem shows that $\gcd(n, m) = xn + ym$ for some integers x and y. Thus, $\gcd(n, m) \in I + J$ (since $xn \in n\mathbb{Z} = I$ and $ym \in m\mathbb{Z} = J$). This finishes our proof of $\gcd(n, m)\, \mathbb{Z} \subseteq I + J$. Combining this with $I + J \subseteq \gcd(n, m)\, \mathbb{Z}$, we obtain $I + J = \gcd(n, m)\, \mathbb{Z}$. □

1.4. The Chinese Remainder Theorem ([DF, §7.6])

The above examples of direct products were not very surprising; these were rings defined in a way that makes the product structure already quite evident. For example, the ring of diagonal $n \times n$-matrices was a direct product because you can easily see that the diagonal entries of diagonal matrices don't "interfere" with each other when the matrices are multiplied. Keywords like "entry-wise", "pointwise" and "coordinatewise" tend to signal that some structure is a direct product. The 6-element ring $\mathbb{Z}/6$, on the other hand, does not look at all like a direct product. Yet, it is isomorphic to a direct product:

$$\mathbb{Z}/6 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/3)\,.$$

Specifically, there is a ring isomorphism

$$\mathbb{Z}/6 \to (\mathbb{Z}/2) \times (\mathbb{Z}/3),$$

which sends

$$\begin{aligned}
&\overline{0} \mapsto (\overline{0}, \overline{0}) \qquad (\text{that is, } 0 + 6\mathbb{Z} \mapsto (0 + 2\mathbb{Z},\ 0 + 3\mathbb{Z})),\\
&\overline{1} \mapsto (\overline{1}, \overline{1}),\\
&\overline{2} \mapsto (\overline{2}, \overline{2}) = (\overline{0}, \overline{2}),\\
&\overline{3} \mapsto (\overline{3}, \overline{3}) = (\overline{1}, \overline{0}),\\
&\overline{4} \mapsto (\overline{4}, \overline{4}) = (\overline{0}, \overline{1}),\\
&\overline{5} \mapsto (\overline{5}, \overline{5}) = (\overline{1}, \overline{2}).
\end{aligned}$$

The reason why this works is that 2 and 3 are coprime. More generally:

Theorem 1.4.1 (The Chinese Remainder Theorem for two integers)**.** Let n and m be two coprime integers. Then,

$$\mathbb{Z}/(nm) \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m) \qquad \text{as rings.}$$

More precisely, there is a ring isomorphism

$$\mathbb{Z}/(nm) \to (\mathbb{Z}/n) \times (\mathbb{Z}/m)$$

that sends each residue class $\overline{r}$ to $(\overline{r}, \overline{r})$ (or, to use somewhat less ambiguous notation, sends each residue class $r + nm\mathbb{Z}$ to the pair $(r + n\mathbb{Z}, r + m\mathbb{Z})$).

Rather than prove this theorem in this form, I will generalize it and then prove the generalization. After all, this is a course on rings, not just on $\mathbb{Z}/n$. So I will state and prove a "Chinese Remainder Theorem" for arbitrary rings. Thus, I will replace $\mathbb{Z}$ by an arbitrary ring R. I will replace the integers n and m by two ideals I and J of R (since ideals are what we can quotient rings by)[3]. I will replace the "n and m are coprime" condition by the condition "$I + J = R$". Indeed, two integers n and m are coprime if and only if the corresponding principal ideals $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ of $\mathbb{Z}$ satisfy $I + J = \mathbb{Z}$ (this follows easily from the proposition at the end of the previous section[4]). Two ideals I and J of a ring R satisfying $I + J = R$ are said to be **comaximal**:

[3] I could also replace the integers n and m by two elements of R, but that would be less general: Quotienting by an element is tantamount to quotienting by a principal ideal, and principal ideals are just one kind of ideals.

[4] *Proof.* Let n and m be two integers. Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ be the corresponding principal ideals of $\mathbb{Z}$. Then, part **(c)** of the proposition just mentioned yields $I + J = \gcd(n, m)\,\mathbb{Z}$. If n and m are coprime, then $\gcd(n, m) = 1$, so this rewrites as $I + J = 1\mathbb{Z} = \mathbb{Z}$. Conversely, if $I + J = \mathbb{Z}$, then $1 \in \mathbb{Z} = I + J = \gcd(n, m)\,\mathbb{Z}$, which shows that 1 is a multiple of $\gcd(n, m)$; but this entails that $\gcd(n, m) = 1$, and therefore n and m are coprime. Thus, we have shown that n and m are coprime if and only if $I + J = \mathbb{Z}$.

Definition 1.4.2. Let I and J be two ideals of a ring R. We say that I and J are **comaximal** if $I + J = R$.

Now we can state the general version of the Chinese Remainder Theorem – and while we generalize it, we can also add a part **(a)** to it:

Theorem 1.4.3 (The Chinese Remainder Theorem for two ideals)**.** Let I and J be two comaximal ideals of a commutative ring R. Then:
(a) We have $I \cap J = IJ$.
(b) We have $R/(IJ) \cong (R/I) \times (R/J)$.
(c) More precisely, there is a ring isomorphism

$$R/(IJ) \to (R/I) \times (R/J)$$

that sends each residue class $r + IJ$ to the pair $(r + I, r + J)$.

Next time, we will prove this.