Math 332 Winter 2023, Lecture 13: Rings

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

1. Rings and ideals (cont'd)

1.12. The Chinese Remainder Theorem

1.12.1. Introduction

In §1.10.3 (Lecture 12), we saw some examples of direct products. These examples were rather transparent: The direct product structure of each ring was obvious from how the ring was defined (usually signalled by the fact that its elements are pairs or tuples, and by a word like "entrywise" or "pointwise").

However, this is not always the case! The ring $\mathbb{Z}/6$ does not look like a direct product at all (its elements are $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$; these don't look like tuples in any nontrivial way), and yet it is isomorphic to a direct product: I claim that

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

Specifically, there is a ring isomorphism

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

Of course, you can check this by hand, but this is not an isolated incident. The reason why this isomorphism exists is that 2 and 3 are coprime (i.e., that $\gcd(2,3) = 1$). More generally, the following holds:

Theorem 1.12.1 (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 concretely, there is a ring isomorphism

$$\begin{aligned} \mathbb{Z}/(nm) &\to (\mathbb{Z}/n) \times (\mathbb{Z}/m), \\ \overline{r} &\mapsto (\overline{r}, \overline{r}) \qquad (\text{that is, } r + nm\mathbb{Z} \mapsto (r + n\mathbb{Z},\ r + m\mathbb{Z})). \end{aligned}$$

(As usual, the notation $\overline{r}$ is intuitive and confusing at the same time. It stands for the residue class of r modulo an ideal, but what ideal that is depends on the context. In the above context of a map from $\mathbb{Z}/(nm)$ to $(\mathbb{Z}/n) \times (\mathbb{Z}/m)$, it should be clear that the first $\overline{r}$ has to be a residue class modulo nm (since it is an element of $\mathbb{Z}/(nm)$), whereas the other two $\overline{r}$'s are residue classes modulo n and modulo m, respectively (since they form the pair $(\overline{r}, \overline{r})$, which belongs to $(\mathbb{Z}/n) \times (\mathbb{Z}/m)$). In general, I will rely on the context to disambiguate such notations.)

Rather than prove Theorem 1.12.1 directly, I will generalize it and then prove the generalization. Specifically, I will replace $\mathbb{Z}$ by an arbitrary commutative ring R, and replace the integers n and m by two ideals I and J of R. The assumption "n and m are coprime" will be replaced by the condition "$I + J = R$".

1.12.2. The Chinese Remainder Theorem for two ideals

The latter condition actually has a standard name:

Definition 1.12.2. 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 generalize Theorem 1.12.1 to ideals:

Theorem 1.12.3 (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 concretely, there is a ring isomorphism

$$\begin{aligned} R/(IJ) &\to (R/I) \times (R/J), \\ \overline{r} &\mapsto (\overline{r}, \overline{r}) \qquad \text{(that is, } r + IJ \mapsto (r + I, \ r + J)\text{)}. \end{aligned}$$

As we will soon see, parts **(b)** and **(c)** of this theorem generalize Theorem 1.12.1 (while part **(a)** generalizes the fact that $\operatorname{lcm}(n, m) = \pm nm$ for any two coprime integers n and m).

Let us now prove Theorem 1.12.3. We agree to understand the notation $R/I \times R/J$ as $(R/I) \times (R/J)$, so that we need to write fewer parentheses. Also, the notation R/IJ will mean $R/(IJ)$. Thus, we can restate Theorem 1.12.3 **(b)** as $R/IJ \cong R/I \times R/J$.

Proof of Theorem 1.12.3. We have $1 \in R = I + J$ (since I and J are comaximal). In other words, we can write 1 as

$$1 = i + j \qquad \text{for some } i \in I \text{ and some } j \in J.$$

Consider these i and j.

(a) Recall that the ideal IJ consists of all finite sums of (I,J)-products. But any (I,J)-product lies in both I and J (since it has a factor in I and a factor in J, but both I and J are ideals and thus satisfy the second ideal axiom). Thus, any (I,J)-product lies in $I\cap J$. Hence, any finite sum of (I,J)-products also lies in $I\cap J$. In other words, $IJ\subseteq I\cap J$.

Let us now prove that $I\cap J\subseteq IJ$.

So let $a\in I\cap J$. Then, $a\in I$ and $a\in J$. Now,

$$a=a\cdot\underbrace{1}_{=i+j}=a\cdot(i+j)=\underbrace{ai}_{=ia}+aj=ia+aj.$$

This is a sum of two (I,J)-products (indeed, ia is an (I,J)-product since $i\in I$ and $a\in J$; moreover, aj is an (I,J)-product since $a\in I$ and $j\in J$). Hence, this belongs to IJ (by the definition of IJ). In other words, $a\in IJ$.

So we have shown that $a\in IJ$ for each $a\in I\cap J$. Hence, $I\cap J\subseteq IJ$. Combined with $IJ\subseteq I\cap J$ (which was proved above), this results in $IJ=I\cap J$. This proves part **(a)** of Theorem 1.12.3.

(c) First, we define a map

$$\begin{aligned} f:R&\to(R/I)\times(R/J),\\ r&\mapsto(\overline{r},\overline{r}) \end{aligned}$$

(where the $(\overline{r},\overline{r})$ means $(r+I,\ r+J)$, as explained above). It is straightforward to see that this map f is a ring morphism. Its kernel is

$$\begin{aligned} \operatorname{Ker} f&=\left\{r\in R\ \mid\ (\overline{r},\overline{r})=0_{(R/I)\times(R/J)}\right\}\\ &=\{r\in R\ \mid\ (r+I,\ r+J)=(0+I,\ 0+J)\}\\ &\qquad\qquad\left(\text{since }(\overline{r},\overline{r})=(r+I,\ r+J)\text{ and }0_{(R/I)\times(R/J)}=(0+I,\ 0+J)\right)\\ &=\{r\in R\ \mid\ r+I=0+I\text{ and }r+J=0+J\}\\ &=\{r\in R\ \mid\ r\in I\text{ and }r\in J\}\\ &=I\cap J=IJ\qquad\text{(by Theorem 1.12.3 }\textbf{(a)}). \end{aligned}$$

Now I claim that the image of f is the whole ring $(R/I)\times(R/J)$ (that is, the map f is surjective).

Indeed, recall that $1=i+j$. Hence, $1-i=j\in J$. Therefore, $\overline{1}=\overline{i}$ in R/J (because two elements $u,v\in R$ satisfy $\overline{u}=\overline{v}$ in R/J if and only if $u-v\in J$). In other words, $\overline{i}=\overline{1}$ in R/J. Similarly, $\overline{j}=\overline{1}$ in R/I.

On the other hand, $\overline{i}=\overline{0}$ in R/I (since $i\in I$), and $\overline{j}=\overline{0}$ in R/J (since $j\in J$).

Now, for every $x \in R$ and $y \in R$, we have[1]

$$\begin{aligned}
f(yi+xj) &= f(y)\,f(i)+f(x)\,f(j) \qquad \text{(since } f \text{ is a ring morphism)} \\
&= (\overline{y},\overline{y})\left(\underbrace{\overline{i}}_{=\overline{0}},\underbrace{\overline{i}}_{=\overline{1}}\right)+(\overline{x},\overline{x})\left(\underbrace{\overline{j}}_{=\overline{1}},\underbrace{\overline{j}}_{=\overline{0}}\right) \\
&\qquad \text{(by the definition of } f\text{)} \\
&= (\overline{y},\overline{y})\left(\overline{0},\overline{1}\right)+(\overline{x},\overline{x})\left(\overline{1},\overline{0}\right) \\
&= \left(\overline{y}\cdot\overline{0},\ \overline{y}\cdot\overline{1}\right)+\left(\overline{x}\cdot\overline{1},\ \overline{x}\cdot\overline{0}\right) \qquad \left(\begin{array}{c}\text{since multiplication in a}\\ \text{direct product is entrywise}\end{array}\right) \\
&= \left(\overline{0},\overline{y}\right)+\left(\overline{x},\overline{0}\right) \\
&= \left(\overline{0}+\overline{x},\ \overline{y}+\overline{0}\right) \qquad \left(\begin{array}{c}\text{since addition in a}\\ \text{direct product is entrywise}\end{array}\right) \\
&= (\overline{x},\overline{y}). \qquad (1)
\end{aligned}$$

However, **any** element of $(R/I)\times(R/J)$ can be written as $(\overline{x},\overline{y})$ for some $x,y\in R$. Using (1), we can rewrite this as follows: Any element of $(R/I)\times(R/J)$ can be written as $f(yi+xj)$ for some $x,y\in R$. In particular, this means that any element of $(R/I)\times(R/J)$ is a value of the map f. In other words, the map f is surjective. Hence, its image is

$$f(R)=(R/I)\times(R/J).$$

So we know that f is a ring morphism with kernel $\operatorname{Ker} f = IJ$ and image $f(R)=(R/I)\times(R/J)$. But the first isomorphism theorem for rings (Theorem 1.9.10 **(c)** in Lecture 11) says that the map

$$\begin{aligned}
f' : R/\operatorname{Ker} f &\to f(R), \\
\overline{r} &\mapsto f(r)
\end{aligned}$$

is well-defined and is a ring isomorphism.

Since $\operatorname{Ker} f = IJ$ and $f(R)=(R/I)\times(R/J)$ and $f(r)=(\overline{r},\overline{r})$ for all $r\in R$, we can rewrite this as follows: The map

$$\begin{aligned}
f' : R/IJ &\to (R/I)\times(R/J), \\
\overline{r} &\mapsto (\overline{r},\overline{r})
\end{aligned}$$

is well-defined and is a ring isomorphism. This proves part **(c)** of Theorem 1.12.3. Thus, part **(b)** follows. □

[1]In the following, the notation $\overline{r}$ (for a given $r\in R$) means the residue class of r modulo I if it stands in the first entry of a pair, and means the residue class of r modulo J if it stands in the second entry of a pair.

1.12.3. Application to integers

Now, we can get Theorem 1.12.1 (the Chinese Remainder Theorem for two integers) as a corollary of Theorem 1.12.3 (the Chinese Remainder Theorem for two ideals):

Proof of Theorem 1.12.1. Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$. Then, Proposition 1.11.3 **(a)** in Lecture 12 yields $IJ = nm\mathbb{Z}$.

Also, Proposition 1.11.3 **(c)** in Lecture 12 yields

$$I + J = \underbrace{\gcd(n, m)}_{\substack{=1 \\ \text{(since } n \text{ and } m \text{ are coprime)}}} \mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}.$$

In other words, the ideals I and J are comaximal. Hence, we can apply Theorem 1.12.3. In particular, Theorem 1.12.3 **(b)** yields that

$$R/IJ \cong (R/I) \times (R/J), \qquad \text{that is,}$$
$$\mathbb{Z}/nm \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m)$$

(since $IJ = nm\mathbb{Z}$ and $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$). Likewise, Theorem 1.12.3 **(c)** yields the specific isomorphism we are looking for. $\square$

Exercise 1. Apply this to $n = 6$ and $m = 5$ to obtain a ring isomorphism

$$\mathbb{Z}/30 \to (\mathbb{Z}/6) \times (\mathbb{Z}/5).$$

Find the preimage of $(\overline{2}, \overline{3})$ under this isomorphism. (The first step is to write 1 as $i + j$ where $i \in 6\mathbb{Z}$ and $j \in 5\mathbb{Z}$.)

More generally, if n and m are two coprime integers, then the **extended Euclidean algorithm** is a fairly efficient algorithm for writing 1 as $i + j$ with $i \in n\mathbb{Z}$ and $j \in m\mathbb{Z}$ (that is, for writing 1 as a sum of a multiple of n and a multiple of m). For this algorithm, see, e.g., the Wikipedia page or any textbook on elementary number theory (e.g., [LeLeMe18, §9.2.2] explains the algorithm on an example, and [Stein09, Algorithm 2.3.7] gives a simple recursive implementation).

References

[LeLeMe18] Eric Lehman, F. Thomson Leighton, Albert R. Meyer, *Mathematics for Computer Science*, revised Tuesday 6th June 2018. `https://courses.csail.mit.edu/6.042/spring18/mcs.pdf` .

[Stein09] William Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer 2009.