Math 332 Winter 2023, Lecture 12: Rings

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

1. Rings and ideals (cont'd)

1.10. Direct products of rings

1.10.1. Direct products of two rings

Here is a way to generate a new ring out of two existing rings:

Proposition 1.10.1. Let R and S be two rings. Then, the Cartesian product

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

becomes a ring if we endow it with the entrywise addition

$$(r,s) + (r',s') = (r+r',\ s+s')$$

and the entrywise multiplication

$$(r,s) \cdot (r',s') = (rr',\ ss')$$

and the zero $(0_R, 0_S)$ and the unity $(1_R, 1_S)$.

Definition 1.10.2. This ring is denoted by $R \times S$ and is called the **direct product** of R and S.

Proof of Proposition 1.10.1. We need to check the ring axioms. For instance, let us check associativity of multiplication: This means proving that $a(bc) = (ab)c$ for all $a, b, c \in R \times S$. In other words (since the elements of $R \times S$ are pairs), this means proving that

$$(r,s)\left((r',s')(r'',s'')\right) = \left((r,s)(r',s')\right)(r'',s'')$$

for all $(r,s), (r',s'), (r'',s'') \in R \times S$. To prove this, just multiply out:

$$(r,s)\left((r',s')(r'',s'')\right) = (r,s)(r'r'',\ s's'') = \left(r(r'r''),\ s(s's'')\right)$$

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 two equalities are equal, since $r(r'r'') = (rr')r''$ and $s(s's'') = (ss')s''$. Thus, the left hand sides are equal as well. So associativity of multiplication in $R \times S$ follows from the analogous properties of R and of S. The same holds for all the other ring axioms. Thus, Proposition 1.10.1 follows. □

1.10.2. Direct products of any number of rings

More generally, we can define a direct product $R_1 \times R_2 \times \cdots \times R_n$ 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 (the family can be infinite):

Proposition 1.10.3. 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

$$(r_i)_{i \in I} + (s_i)_{i \in I} = (r_i + s_i)_{i \in I}$$

and the entrywise multiplication

$$(r_i)_{i \in I} \cdot (s_i)_{i \in I} = (r_i s_i)_{i \in I}$$

and the zero $\left(0_{R_i}\right)_{i \in I}$ and the unity $\left(1_{R_i}\right)_{i \in I}$.

We recall that a family is a generalization of a list or a sequence; it is a collection of objects (the "entries" of the family) indexed by elements of a given set I (the "indexing set"). Such a family can be written as $(s_i)_{i \in I}$, where s_i denotes the i-th entry of the family (i.e., the entry indexed by i). Programmers know families under the name "dictionaries" or "associative arrays". The simplest examples of families are:

- n-tuples: If $I = \{1, 2, \ldots, n\}$, then a family $(r_i)_{i \in I}$ is the n-tuple $(r_1, r_2, \ldots, r_n)$.
- infinite sequences: If $I = \mathbb{N} = \{0, 1, 2, \ldots\}$, then a family $(r_i)_{i \in I}$ is the sequence $(r_0, r_1, r_2, \ldots)$.
- sequences infinite on both sides: If $I = \mathbb{Z}$, then a family $(r_i)_{i \in I}$ is the "infinite-on-both-sides sequence" $(\ldots, r_{-2}, r_{-1}, r_0, r_1, r_2, \ldots)$.

In particular, any map f from a set I to a set S can be viewed as a family $(f(i))_{i \in I} \in \prod_{i \in I} S$ (whose entries are the values of f). However, families can be more general than maps, in that the values of a map have to all belong to the same set (the target of the map), whereas each entry of a family can come from a different set.

Definition 1.10.4. The ring defined in Proposition 1.10.3 is denoted by $\prod_{i \in I} R_i$ and is called the **direct product** of the rings R_i.

Some particular cases of this:

- 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 its elements $(r_i)_{i \in I}$ can be written as $(r_1, r_2, \ldots, r_n)$. Thus, the elements of this ring in this case are the n-tuples $(r_1, r_2, \ldots, r_n)$ whose entries belong to $R_1, R_2, \ldots, R_n$ respectively. In particular, for $n = 2$, this recovers the definition of $R \times S$ in Definition 1.10.2.
- 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 introduced for the ring of all functions from I to R (with pointwise addition and multiplication); however, these two notations are identical for a good reason: The two rings are the same. Indeed, a function f from I to R is the same as a choice of value $f(i)$ for each $i \in I$, and this is the same thing as a family $(f(i))_{i \in I}$ of elements of R. So a function from I to R is precisely an element of $\prod_{i \in I} R$. Pointwise addition/multiplication of functions corresponds precisely to entrywise addition/multiplication of families, so the two rings are the same (not just as sets but as rings).
- 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.

Proof of Proposition 1.10.3. Analogous to the proof of Proposition 1.10.1: Replace (r, r') by $(r_i)_{i \in I}$, and so on. □

1.10.3. Examples

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 entrywise:
$$(r, s, t) + (r', s', t') = (r + r',\ s + s',\ t + t')$$
and multiplied entrywise:
$$(r, s, t) \cdot (r', s', t') = (rr',\ ss',\ tt').$$
Note that this ring is **not** an integral domain, since (for example) $(0, 1, 2) \cdot (1, 0, 0) = (0, 0, 0)$.

- 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 the triples (r,s,t), whereas the latter consists of the pairs $((r,s),t)$). However, they are isomorphic through the rather obvious ring isomorphism

$$\begin{aligned} R \times S \times T &\to (R \times S) \times T, \\ (r,s,t) &\mapsto ((r,s),t). \end{aligned}$$

  (Proving this is completely straightforward if you understand the definitions.)

  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 operation (on rings) is "associative up to isomorphism".

- The ring $\mathbb{C}$ consists of complex numbers, which are defined as pairs of real numbers (the real part and the imaginary part). 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. However, $\mathbb{C}$ is **not** $\mathbb{R} \times \mathbb{R}$ as rings, because multiplication of complex numbers is not entrywise[1]. Actually, the rings $\mathbb{C}$ and $\mathbb{R} \times \mathbb{R}$ are not even isomorphic, since $\mathbb{C}$ is an integral domain (even a field) whereas $\mathbb{R} \times \mathbb{R}$ is not (since it has $(1,0) \cdot (0,1) = (0,0)$).

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

$$R^{n=n} = \left\{ \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} \;\mid\; a_1, a_2, \ldots, a_n \in R \right\}.$$

  For example,

$$R^{2=2} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \;\mid\; a, d \in R \right\}.$$

  It is easy to see that $R^{n=n}$ is a subring of $R^{n \times n}$. Moreover, we have $R^{n=n} \cong$

[1] Let's be explicit: In $\mathbb{C}$, multiplication is given by

$$(a,b) \cdot (c,d) = (ac - bd,\ ad + bc).$$

In $\mathbb{R} \times \mathbb{R}$, multiplication is given by

$$(a,b) \cdot (c,d) = (ac,\ bd).$$

These are very much not the same.

R^n as rings (where R^n is as in Definition 1.10.4). Specifically, the map

$$R^n \to R^{n=n},$$
$$(a_1, a_2, \ldots, a_n) \mapsto \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$$

is a ring isomorphism. (For example, this map respects multiplication because diagonal matrices are multiplied entry by entry.)

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

1.10.4. Direct products and idempotents

Direct products of rings are closely related to idempotents. We will briefly discuss this in the case of a product $R \times S$ of two rings R and S.

Indeed, if R and S are two rings, then the pairs $a := (1_R, 0_S)$ and $b := (0_R, 1_S)$ are idempotents in $R \times S$. If R and S are nontrivial rings, then these are "nontrivial" idempotents (i.e., they equal neither the zero $0_{R\times S} = (0_R, 0_S)$ nor the unity $1_{R\times S} = (1_R, 1_S)$). Thus, nontrivial direct products have nontrivial idempotents. Incidentally, these idempotents allow you to reconstruct the original rings R and S: namely, the principal ideals $a(R \times S)$ and $b(R \times S)$ are themselves rings[2] that are isomorphic to R and S (respectively).

For commutative rings, this road from direct products to idempotents can also be walked backwards: If you know a nontrivial idempotent (i.e., an idempotent distinct from 0 and 1) in a commutative ring R, then R can be decomposed as a direct product of two nontrivial rings (or, more precisely: R is isomorphic to such a direct product). More concretely:

Proposition 1.10.5. Let e be an idempotent in a commutative ring R. Then, the principal ideals eR and $(1-e)R$ themselves are rings (with addition, multiplication and zero inherited from R, and with unities e and $1-e$, respectively), and there is a ring isomorphism

$$(eR) \times ((1-e)R) \to R,$$
$$(a, b) \mapsto a + b.$$

Note that we need commutativity for this to work. For example, the matrix ring $\mathbb{R}^{2\times 2}$ has lots of idempotents (any projection matrix, such as $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, is an idempotent), but is not a nontrivial direct product.

[2] with addition, multiplication and zero inherited from $R \times S$, and with respective unities a and b

1.11. Ideal arithmetic

It is easy to see that if I and J are two ideals of a ring R, then their intersection $I \cap J$ is an ideal of R as well (but their union $I \cup J$ usually isn't). But this is not the only way to build new ideals of a ring from old. Here are two other ways:

Definition 1.11.1. 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 of R, 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 our definition of $I + J$, as it involved an additional step (viz., taking finite sums). The purpose of this step was to ensure that IJ is closed under addition. For $I + J$, we did not need to do this, because $I + J$ (as we defined it) is already closed under addition: For any $i_1, i_2 \in I$ and $j_1, j_2 \in J$, we have

$$(i_1 + j_1) + (i_2 + j_2) = \underbrace{(i_1 + i_2)}_{\in I} + \underbrace{(j_1 + j_2)}_{\in J}.$$

Meanwhile, the sum of two (I,J)-products is generally not an (I,J)-product (even though a counterexample isn't that easy to find).

Here is an assortment of facts about the above-defined operations on ideals:

Proposition 1.11.2. Let R be a ring.

(a) Let I and J be two ideals of 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 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 $\{0_R\}$. That is,

$$(I + J) + K = I + (J + K) \qquad \text{for any three ideals } I, J, K \text{ of } R,$$
$$I + \{0_R\} = \{0_R\} + I = I \qquad \text{for any ideal } I \text{ of } R.$$

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

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

(f) Addition and intersection of ideals are commutative:

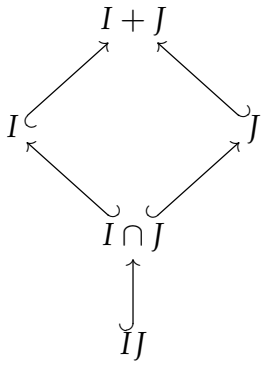
$$I + J = J + I \qquad \text{and} \qquad I \cap J = J \cap I \qquad \text{for any ideals } I, J \text{ of } R.$$

(g) If R is commutative, then $IJ = JI$ for any two ideals I and J of R.

Proof. Exercises. Some will be on the homework! □

Proposition 1.11.2 shows that the operations $+$, $\cap$ and $\cdot$ on the set of all ideals of R satisfy a number of laws similar to the basic laws of arithmetic. This is known as **ideal arithmetic**. However, ideals cannot be subtracted (i.e., you cannot reconstruct I from J and $I + J$), so the ideals of R do not form a ring.

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



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

In order to understand ideal arithmetic better, let us see how its operations (addition, intersection and multiplication) behave for principal ideals of $\mathbb{Z}$:

Proposition 1.11.3. 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 $I + J = \gcd(n, m)\,\mathbb{Z}$.
(d) We have $I \subseteq J$ if and only if $m \mid n$.
(e) We have $I = J$ if and only if $|n| = |m|$.

Proof. **(a)** Let $c \in nm\mathbb{Z}$. Then, $c = nmd$ for some integer d. Consider this d. Then, $n = n \cdot 1 \in I$ (since $I = n\mathbb{Z}$) and $md \in J$ (since $J \in m\mathbb{Z}$). Hence, the product $n\,(md)$ is an (I, J)-product. In other words, c is an (I, J)-product (since $c = nmd = n\,(md)$). Thus, c is a finite sum of (I, J)-products (of just one, to be specific). In other words, $c \in IJ$.

Forget that we fixed c. We thus have shown that every $c \in nm\mathbb{Z}$ satisfies $c \in IJ$. 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).

Combining this with $nm\mathbb{Z} \subseteq IJ$ (which we have shown above), we obtain $IJ = nm\mathbb{Z}$. Thus, Proposition 1.11.3 **(a)** is proven.

(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, we let $k \in \gcd(n, m)\,\mathbb{Z}$. Thus, $k = \gcd(n, m) \cdot c$ for some integer c. Consider this c.

Bezout's theorem from elementary number theory (see, e.g., [19s, Theorem 2.9.12]) shows that $\gcd(n, m) = xn + ym$ for some integers x and y. Consider

these x and y. Then,

$$k = \underbrace{\gcd(n,m)}_{=xn+ym} \cdot c = (xn+ym) \cdot c = xnc + ymc \in I + J$$

(since $xnc = nxc \in n\mathbb{Z} = I$ and $ymc = myc \in m\mathbb{Z} = J$).

We thus have shown that $k \in I + J$ for each $k \in \gcd(n,m)\,\mathbb{Z}$. In other words, $\gcd(n,m)\,\mathbb{Z} \subseteq I + J$. Combining this with $I + J \subseteq \gcd(n,m)\,\mathbb{Z}$, we obtain $I + J = \gcd(n,m)\,\mathbb{Z}$. This proves Proposition 1.11.3 **(c)**.

(d) If $I \subseteq J$, then $n = n \cdot 1 \in n\mathbb{Z} = I \subseteq J = m\mathbb{Z}$, which means that n is a multiple of m; but this is just saying that $m \mid n$. Conversely, if $m \mid n$, then every multiple of n is a multiple of m, which means that $n\mathbb{Z} \subseteq m\mathbb{Z}$, which we can rewrite as $I \subseteq J$ (since $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$). Combining these two implications, we see that we have $I \subseteq J$ if and only if $m \mid n$. This proves Proposition 1.11.3 **(d)**.

(e) We have $I = J$ if and only if we have both $I \subseteq J$ and $J \subseteq I$. But $I \subseteq J$ is equivalent to $m \mid n$ (by Proposition 1.11.3 **(d)**), whereas $J \subseteq I$ is equivalent to $n \mid m$ (similarly). Thus, we have $I = J$ if and only if we have both $m \mid n$ and $n \mid m$. But the latter statement ("both $m \mid n$ and $n \mid m$") is equivalent to $|n| = |m|$, by basic properties of integers. Thus, Proposition 1.11.3 **(e)** follows. □

References

[19s] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
`http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`