Math 332 Winter 2023, Lecture 4: Rings

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

1. Rings and ideals (cont'd)

1.3. Subrings (cont'd)

1.3.2. Examples (cont'd)

Here are some more examples of subrings:

- There are myriad rings between $\mathbb{Q}$ and $\mathbb{R}$. One example is the ring

$$\mathbb{S} = \mathbb{Q}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$$

  we defined in Lecture 2. Another example is the ring

$$\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}.$$

  Another is

$$\mathbb{Q}\left[\sqrt[3]{2}\right] = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}$$

  (exercise: check that this is a subring of $\mathbb{R}$!). Another is

$$\mathbb{Q}[\pi] = \Big\{a + b\pi + c\pi^2 + d\pi^3 + \cdots \mid a, b, c, d, \ldots \in \mathbb{Q} \text{ and only finitely many of } a, b, c, d, \ldots \text{ are } \neq 0\Big\}.$$

- There are no rings between $\mathbb{R}$ and $\mathbb{C}$. Any subring of $\mathbb{C}$ that contains $\mathbb{R}$ as a subset must be either $\mathbb{R}$ or $\mathbb{C}$. (This is not hard to prove, but I won't do it here.)

- There are rings between $\mathbb{Z}$ and $\mathbb{C}$ that are neither subrings nor "superrings" of $\mathbb{R}$.

  A particularly important one is the ring $\mathbb{Z}[i]$ of **Gaussian integers**.

  A **Gaussian integer** is a complex number of the form $a + bi$, where a and b are integers (and where i is the imaginary unit $\sqrt{-1}$). For instance, $3 + 5i$ and $7 - 9i$ are Gaussian integers.

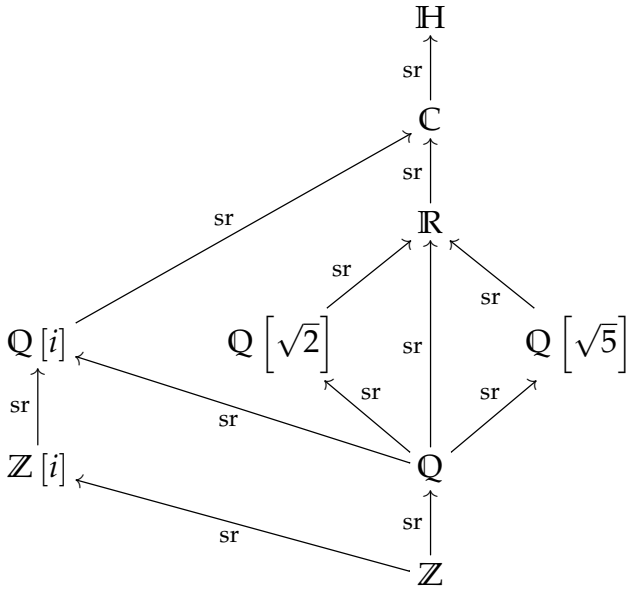
  It is easy to see that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ and contains $\mathbb{Z}$ as a subring. But $\mathbb{Z}[i]$ is neither a subring of $\mathbb{Q}$ or of $\mathbb{R}$, nor contains any of $\mathbb{Q}$ and $\mathbb{R}$ as a subring.

  Visually, if you think of the complex numbers as the points in the Euclidean plane, then you can think of the Gaussian integers as the integer

lattice points – i.e., the points whose both coordinates are integers. (See, e.g., the first picture in the "The Gaussian Integers" section of Bill Casselman's note *Circles and Squares*.)

Likewise, there is a ring $\mathbb{Q}[i]$ of **Gaussian rationals**, which are defined just like the Gaussian integers but with $a, b \in \mathbb{Q}$ instead of $a, b \in \mathbb{Z}$. The ring $\mathbb{Q}[i]$ is sandwiched between $\mathbb{Q}$ and $\mathbb{C}$.

Here is a diagram representing the subring relations between some of the rings discussed above:



(where an arrow of the form "$A \xrightarrow{\text{sr}} B$" means "$A$ is a subring of B"). Of course, there are many further rings that would fit into this diagram (for example, the ring of all rational numbers $\frac{a}{b}$ with $b \in \mathbb{Z}$ odd would fit between $\mathbb{Z}$ and $\mathbb{Q}$), but it is already fairly crowded.

- Recall the ring of functions from $\mathbb{Q}$ to $\mathbb{Q}$. Similarly, there is a ring of functions from $\mathbb{R}$ to $\mathbb{R}$. The latter ring has a subring that consists of all **continuous** functions from $\mathbb{R}$ to $\mathbb{R}$. Why is it a subring? Because the (pointwise) sum and the (pointwise) product of two continuous functions are continuous, as is the (pointwise) negation of a continuous function, as are the constant-0 and constant-1 functions.

- Let $n \in \mathbb{N}$, and let R be any ring. Recall the matrix ring

$$R^{n\times n} = \left\{ \text{all } n \times n\text{-matrices } \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \text{ with } a_{i,j} \in R \right\}.$$

(Its addition and its multiplication are matrix addition and matrix multiplication.)

Define a subset $R^{n\leq n}$ of $R^{n\times n}$ by

$$\begin{aligned} R^{n\leq n} &= \left\{\text{all upper-triangular } n\times n\text{-matrices in } R^{n\times n}\right\} \\ &= \left\{ \text{all } n\times n\text{-matrices } \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix} \text{ with } a_{i,j}\in R \right\}. \end{aligned}$$

This subset is a subring of $R^{n\times n}$ (since the sum and the product of two upper-triangular matrices are again upper-triangular, and since $-A$ is upper-triangular when A is upper-triangular, and since the zero matrix $0_{n\times n}$ and the identity matrix I_n are upper-triangular). (I call this subring $R^{n\leq n}$ because the nonzero entries in such a matrix all have the form $a_{i,j}$ with $i\leq j$.)

Likewise, the subset $R^{n\geq n}$ of $R^{n\times n}$ defined by

$$\begin{aligned} R^{n\geq n} &= \left\{\text{all lower-triangular } n\times n\text{-matrices in } R^{n\times n}\right\} \\ &= \left\{ \text{all } n\times n\text{-matrices } \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \text{ with } a_{i,j}\in R \right\} \end{aligned}$$

is a subring of $R^{n\times n}$.

On the other hand, the subset

$$\begin{aligned} R^{n\times n}_{\text{symm}} &= \left\{\text{all symmetric matrices in } R^{n\times n}\right\} \\ &= \left\{ \text{all } n\times n\text{-matrices } \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \text{ with } a_{i,j}=a_{j,i}\in R \right\} \end{aligned}$$

is not a subring of $R^{n\times n}$ (unless R is trivial or $n\leq 1$). The problem here is that the product of two symmetric matrices is not always symmetric: for example, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ is not a symmetric matrix.

See homework set #1 Exercise 6 for another subring of $R^{n\times n}$.

More examples can be found in the text (§2.3). I particularly recommend §2.3.3 for an application of a subring of $\mathbb{Z}^{2\times 2}$ to the Fibonacci sequence.

1.4. Zero divisors and integral domains

The following definition shouldn't come as a surprise:

Definition 1.4.1. An element of a ring R is said to be **nonzero** if it is $\neq 0_R$.

As we saw in §1.2.2 (Lecture 3), it can happen that a product of two nonzero elements of a ring is zero. Let us give this phenomenon a name:

Definition 1.4.2. Let R be a commutative ring. A nonzero element $a \in R$ is called a **zero divisor** if there exists a nonzero $b \in R$ such that $ab = 0$.

For example, in the ring $\mathbb{Z}/6$, the elements $\overline{2}, \overline{3}, \overline{4}$ are zero divisors, since

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0} = 0_{\mathbb{Z}/6};$$
$$\overline{3} \cdot \overline{2} = \overline{6} = \overline{0} = 0_{\mathbb{Z}/6};$$
$$\overline{4} \cdot \overline{3} = \overline{12} = \overline{0} = 0_{\mathbb{Z}/6}.$$

On the other hand, the elements $\overline{1}$ and $\overline{5}$ are not zero divisors. More generally, in any commutative ring R, the elements 1_R and -1_R are never zero divisors.

Note that the above definition is slightly controversial, as some authors prefer to call 0 a zero divisor. Either convention has good reasons speaking in its favor. Fortunately, the concept of "zero divisor" is not very important, but mostly serves to motivate the following definition:

Definition 1.4.3. Let R be a commutative ring. Assume that $0 \neq 1$ in R (this means $0_R \neq 1_R$, of course). We say that R is an **integral domain** if all nonzero $a, b \in R$ satisfy $ab \neq 0$.

In other words, a commutative ring R with $0 \neq 1$ is an integral domain if and only if it has no zero divisors.

Examples:

- The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.
- The ring $\mathbb{Z}/n$ is an integral domain if and only if n is 0 or a prime or minus a prime. We will prove this later.
- The ring $\mathbb{S}' = \left\{ a + b\sqrt{5} \mid a, b \in \mathbb{Q} \right\}$ with "coefficientwise" multiplication $*$ (defined in Lecture 2) is not an integral domain, since $\left(0 + 1\sqrt{5}\right) * \left(1 + 0\sqrt{5}\right) = 0 + 0\sqrt{5} = 0$.
- The ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$ is not an integral domain, since we can find two functions that are not identically 0 but whose product is identically 0. (For example, take the function that sends each x

to $\begin{cases} 1, & \text{if } x = 2; \\ 0, & \text{if } x \neq 2, \end{cases}$ and multiply it by the function that sends each x to $\begin{cases} 1, & \text{if } x = 3; \\ 0, & \text{if } x \neq 3. \end{cases}$)

- We required integral domains to be commutative. If we didn't, then the ring $\mathbb{H}$ of Hamilton quaternions would be an integral domain, but the matrix ring $\mathbb{Q}^{2\times 2}$ would not be.

1.5. Units and fields

1.5.1. Units and inverses

By definition, any ring R has an addition, a subtraction and a multiplication. On the other hand, a division is not guaranteed. Even in the ring $\mathbb{Z}$, you usually cannot divide. However, any ring R has **some** elements that you can divide by; for example, you can always divide by 1 and by -1. Let us give such elements a name:

Definition 1.5.1. Let R be a ring.

(a) An element $a \in R$ is said to be a **unit** of R (or **invertible** in R) if there exists a $b \in R$ such that $ab = ba = 1$. In this case, b is unique and is known as the **inverse** (or **reciprocal**, or **multiplicative inverse**) of a, and is denoted by a^{-1}.

(b) We let $R^\times$ denote the set of all units of R.

Some comments:

- Of course, the "1" here means 1_R.
- We required $ab = ba = 1$ rather than just $ab = 1$ because R is not commutative in general. When R is commutative, of course, $ab = 1$ suffices.
- The uniqueness of b is a nice exercise in using associativity of multiplication. (For the proof, see §2.5.1 in the text.)
- Don't confuse "unit" (= invertible element) with "unity" (= neutral element for multiplication). The unity is always a unit, but not every unit is the unity!

Here are some examples of units:

- The units of the ring $\mathbb{Q}$ are all the nonzero elements of $\mathbb{Q}$. This is because every nonzero element of $\mathbb{Q}$ has a reciprocal, and this reciprocal again belongs to $\mathbb{Q}$.

  The same holds for $\mathbb{R}$ and for $\mathbb{C}$.

- The units of the ring $\mathbb{Z}$ are 1 and -1 (and these numbers are their own inverses). No other integer is a unit of $\mathbb{Z}$. For instance, 2 is not a unit, since its reciprocal $\frac{1}{2}$ is not in $\mathbb{Z}$. And of course, 0 is not a unit either, since it has no reciprocal.
- The units of the matrix ring $\mathbb{R}^{n\times n}$ are the invertible $n \times n$-matrices. You have seen many ways to characterize them in your linear algebra class.
- In the ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$, the units are the functions that never take the value 0. Inverses are computed pointwise. (This kind of inverse is **not** what is known as an inverse function.)

Next time, we'll describe the units of $\mathbb{Z}/n$ and talk about general properties of inverses.