Math 332 Winter 2023, Lecture 5: Rings

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

1. Rings and ideals (cont'd)

1.5. Units and fields (cont'd)

1.5.1. Units and inverses (cont'd)

Recall the last definition we made in Lecture 4:

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.

We then gave some examples for units (and non-units).

Our next example we state as a proposition:

Proposition 1.5.2. Let $n \in \mathbb{Z}$. Then:

(a) The units of the ring $\mathbb{Z}/n$ are precisely the residue classes $\overline{a}$ where $a \in \mathbb{Z}$ is coprime to n.

(b) Let $a \in \mathbb{Z}$. Then, $\overline{a}$ is a unit of $\mathbb{Z}/n$ if and only if a is coprime to n.

Proof. Clearly, it suffices to prove part **(b)**.

(b) We prove the "if" ($\Longleftarrow$) and "only if" ($\Longrightarrow$) direction separately:

$\Longleftarrow$: Assume that $a \in \mathbb{Z}$ is coprime to n. We must prove that $\overline{a}$ is a unit of $\mathbb{Z}/n$.

Since a is coprime to n, we have $\gcd(a, n) = 1$. But Bezout's theorem yields that there exist $x, y \in \mathbb{Z}$ such that $xa + yn = \gcd(a, n)$. Consider these x, y.

We have $xa + yn = \gcd(a, n) = 1$. In other words, $xa - 1 = -yn$, which is a multiple of n. Therefore, $xa \equiv 1 \mod n$. In terms of residue classes, this is saying that $\overline{xa} = \overline{1}$. In other words, $\overline{x} \cdot \overline{a} = \overline{1}$. Since $\mathbb{Z}/n$ is commutative, this entails $\overline{a} \cdot \overline{x} = \overline{1}$ as well. Thus, $\overline{x}$ is an inverse of $\overline{a}$ in $\mathbb{Z}/n$. Therefore, $\overline{a}$ is a unit of $\mathbb{Z}/n$.

$\Longrightarrow$: Assume that $\overline{a}$ is a unit of $\mathbb{Z}/n$. We must prove that a is coprime to n.

Since $\overline{a}$ is a unit of $\mathbb{Z}/n$, it has an inverse $\overline{x}$. This inverse $\overline{x}$ satisfies $\overline{xa} = \overline{x} \cdot \overline{a} = \overline{1}$, which means that $xa \equiv 1 \mod n$. In other words, xa differs from 1 by a multiple of n. Hence,[1] $\gcd(xa, n) = \gcd(1, n) = 1$. This shows that xa

[1] We are using the following fact here: If α, β, γ are three integers satisfying $\alpha \equiv \beta \mod \gamma$, then $\gcd(\alpha, \gamma) = \gcd(\beta, \gamma)$. In other words, when we compute the greatest common divisor of two integers, we can add any multiple of one integer to the other.

and n are coprime. Since a divides xa, this also entails that a and n are coprime (since any common divisor of a and n would also divide xa and thus would be a common divisor of xa and n). In other words, a is coprime to n. □

Here are some examples of Proposition 1.5.2:

- The units of the ring $\mathbb{Z}/12$ are $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ (because among the integers $0, 1, \ldots, 11$, it is the four numbers $1, 5, 7, 11$ that are coprime to 12).
- The units of the ring $\mathbb{Z}/5$ are $\overline{1}, \overline{2}, \overline{3}, \overline{4}$.
- The only unit of the ring $\mathbb{Z}/2$ is $\overline{1}$.

Now here is a general property of units in any ring:

Theorem 1.5.3. Let R be a ring. Then, the set $R^\times$ is a multiplicative group. More precisely: $(R^\times, \cdot, 1)$ is a group.

Proof. It suffices to show the following facts:

1. The unity 1 of R belongs to $R^\times$.
2. If $a, b \in R^\times$, then $ab \in R^\times$.
3. If $a \in R^\times$, then a has an inverse in $R^\times$.

Once these three facts are proved, all other group axioms for $R^\times$ follow from the ring axioms for R. So let us prove these three facts:

Proof of Fact 1: The element 1 has an inverse, namely 1 itself.

Proof of Fact 2: Let $a, b \in R^\times$. Why is $ab \in R^\times$?

Since $a, b \in R^\times$, there are inverses a^{-1} and b^{-1} for a and b.

I claim that $b^{-1}a^{-1}$ is an inverse for ab. Indeed, this follows from

$$b^{-1} \underbrace{a^{-1} \cdot a}_{=1} b = b^{-1}b = 1 \qquad \text{and} \qquad a \underbrace{b \cdot b^{-1}}_{=1} a^{-1} = aa^{-1} = 1.$$

Thus, the element ab is a unit (since it has an inverse), i.e., we have $ab \in R^\times$.

Proof of Fact 3: Let $a \in R^\times$. Then, a has an inverse a^{-1} (by the definition of a unit). We need to check that this inverse a^{-1} also belongs to $R^\times$.

But a^{-1} has an inverse, namely a (since $aa^{-1} = 1$ and $a^{-1}a = 1$). Thus, $a^{-1} \in R^\times$ follows.

Theorem 1.5.3 is now proved. □

Thus, every ring R produces **two** groups: the additive group $(R, +, 0)$ and the multiplicative group $(R^\times, \cdot, 1)$ (standardly called the **group of units** of R). The latter usually has fewer elements than the former, since it only contains the units of R.

Theorem 1.5.4 (Shoe-sock theorem)**.** Let R be a ring. Let a, b be two units of R. Then, ab is a unit of R, and its inverse is

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Proof. See the proof of Fact 2 in the proof of Theorem 1.5.3. □

Theorem 1.5.5. Let R be a ring. Let a be a unit of R. Then, a^{-1} is a unit of R, and its inverse is $\left(a^{-1}\right)^{-1} = a$.

Proof. See the proof of Fact 3 in the proof of Theorem 1.5.3. □

1.5.2. Fields

As we saw, many rings (such as $\mathbb{Z}$) have few units, but many other rings (such as $\mathbb{Q}$ or $\mathbb{R}$) have many. The rings of the latter kind are known as "fields":

Definition 1.5.6. Let R be a commutative ring. Assume that $0 \neq 1$ in R. We say that R is a **field** if every nonzero element of R is a unit.

Examples:

- The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. The ring $\mathbb{Z}$ is not (e.g., since 2 is not a unit).
- The ring $\mathbb{S} = \mathbb{Q}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$ (from Lecture 2) is a field. Indeed, if $a + b\sqrt{5}$ is a nonzero element of $\mathbb{S}$, then $a + b\sqrt{5}$ is a unit, since its inverse is

  $$\begin{aligned}\left(a + b\sqrt{5}\right)^{-1} &= \frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{\left(a + b\sqrt{5}\right)\left(a - b\sqrt{5}\right)} \\ &= \frac{a - b\sqrt{5}}{a^2 - 5b^2} = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5} \in \mathbb{S}.\end{aligned}$$

  (Strictly speaking, we need to make sure that $a - b\sqrt{5}$ is nonzero. The reason why this is true is that $\sqrt{5}$ is irrational, so $a + b\sqrt{5} \neq 0$ entails that a and b are not both 0 and therefore we easily obtain $a - b\sqrt{5} \neq 0$.)
- The Hamilton quaternions $\mathbb{H}$ would be a field if they were commutative. Indeed, it is not hard to see that every nonzero quaternion $a + bi + cj + dk \in \mathbb{H}$ is a unit. However, $\mathbb{H}$ is not commutative, thus does not qualify as a field.

  A noncommutative ring R with $0 \neq 1$ whose all nonzero elements are units is called a **division ring** or a **skew-field**. So $\mathbb{H}$ is a skew-field.

- Let n be a positive integer. Then, $\mathbb{Z}/n$ is a field if and only if n is prime. (See below for a proof.)

1.6. Fields and integral domains: some connections

The notions of fields and integral domains are related:

Proposition 1.6.1. **(a)** Every field is an integral domain.

(b) Every **finite** integral domain is a field. (Of course, "finite" means "finite as a set".)

Proof. **(a)** Let F be a field. Why is F an integral domain?

Let $a, b \in F$ be nonzero. We must prove that $ab \neq 0$.

Since a is nonzero, a is a unit (since F is a field), thus has an inverse a^{-1}. If we had $ab = 0$, then we would have $a^{-1} \cdot \underbrace{ab}_{=0} = a^{-1} \cdot 0 = 0$, which would contradict $\underbrace{a^{-1} \cdot a}_{=1} b = b \neq 0$. So we have $ab \neq 0$.

Thus, F is an integral domain.

(b) Let R be a **finite** integral domain. We must show that R is a field.

Let $a \in R$ be nonzero. Our goal is to show that a is a unit, i.e., has an inverse.

Consider the map

$$R \to R,$$
$$x \mapsto ax.$$

This map is injective (because if $x, y \in R$ satisfy $ax = ay$, then $a(x-y) = ax - ay = 0$, so that $x - y = 0$ since R is an integral domain[2], and therefore $x = y$). However, the Pigeonhole Principle for Injections says that if a map between two finite sets of the same size is injective, then it is bijective. Hence, our map

$$R \to R,$$
$$x \mapsto ax$$

is bijective. In particular, it must take the unity 1 as a value. In other words, there exists some $x \in R$ such that $ax = 1$. This x must therefore also satisfy $xa = 1$ (since R is an integral domain, thus commutative), and thus is an inverse of a. So a is a unit, and we are done. □

Without the word "finite", Proposition 1.6.1 **(b)** would fail, since $\mathbb{Z}$ is an integral domain but not a field. Other examples of this nature are polynomial rings.

[2]Indeed, if we had $x - y \neq 0$, then we would obtain $a(x-y) \neq 0$ (since $a \neq 0$ and $x - y \neq 0$, and since R is an integral domain), which would contradict $a(x-y) = 0$.

Corollary 1.6.2. Let n be a positive integer. Then, the following equivalences hold:

$$(\mathbb{Z}/n \text{ is an integral domain}) \iff (\mathbb{Z}/n \text{ is a field}) \iff (n \text{ is prime}).$$

Proof. The first of these two $\iff$ signs follows from Proposition 1.6.1. So we only need to prove the second $\iff$ sign.

$\Longrightarrow$: Assume that $\mathbb{Z}/n$ is a field. Then, all its nonzero elements are units. In other words, the residue classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ are units. Equivalently, the numbers $1, 2, \ldots, n-1$ are coprime to n (because of Proposition 1.5.2 **(b)**). Hence, n is prime (why?).

$\Longleftarrow$: Assume that n is prime. Then, the only positive divisors of n are 1 and n. Hence, the numbers $1, 2, \ldots, n-1$ are coprime to n (because if a is any of these numbers, then $\gcd(a, n)$ must be a positive divisor of n, but the only positive divisors of n are 1 and n; hence, we must have either $\gcd(a, n) = 1$ or $\gcd(a, n) = n$; but the second possibility is ruled out by the fact that $\gcd(a, n) \leq a < n$). In other words, the residue classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ are units (by Proposition 1.5.2 **(b)**). This yields that $\mathbb{Z}/n$ is a field (since $n > 1$ entails that $\overline{0} \neq \overline{1}$ in $\mathbb{Z}/n$). □

The group of units $(\mathbb{Z}/p)^\times$ of the field $\mathbb{Z}/p$ (where p is a prime) has a nice application: Fermat's Little Theorem. See §2.6.3 in the text for details.

1.6.1. Division

As we know, rings have addition, subtraction and multiplication, but not always division. Nevertheless, when b is a unit of a ring, it makes sense to define $\frac{a}{b}$ to be the product ab^{-1}. Unfortunately, it makes just as much sense to define it to be $b^{-1}a$ instead. Usually, $ab^{-1} \neq b^{-1}a$. Thus, even if b is a unit, it is ill-advised to define $\frac{a}{b}$ for arbitrary rings R. (If you really want to, you can talk about "left division" and "right division", but you should distinguish between the two.)

However, when R is commutative, this ambiguity disappears, and the notation $\frac{a}{b}$ becomes useful. Thus, we do introduce it:

Definition 1.6.3. Let R be a commutative ring. Let $a \in R$ and $b \in R^\times$. Then, $\frac{a}{b}$ means the element $ab^{-1} = b^{-1}a \in R$. This element is also written a/b, and is called the **quotient** of a by b. The operation $(a, b) \mapsto \frac{a}{b}$ is called **division**.

In particular, in a field, we can divide by any nonzero element.

Division satisfies the rules that you would expect: If R is a commutative ring, and if $a, c \in R$ and $b, d \in R^{\times}$, then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd};$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$
$$\frac{a}{b} \Big/ \frac{c}{d} = \frac{ad}{bc} \qquad \left(\text{if } c \in R^{\times}\right);$$

etc.. And of course, division undoes multiplication: When $b \in R^{\times}$, we have the equivalence

$$\left(\frac{a}{b} = c\right) \iff (a = bc).$$