Math 533 Winter 2021, Lecture 6: Rings and ideals

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

1. Rings and ideals (cont'd)

1.1. Euclidean domains ([DF, §8.1]) (cont'd)

Last time, we have defined Euclidean domains, and we have seen multiple of examples and non-examples. Now, we claim that all Euclidean domains have a property that we have previously proved for $\mathbb{Z}$:

Proposition 1.1.1. Let R be a Euclidean domain. Then, any ideal of R is principal.

Proof. In Lecture 5, we proved that any ideal of $\mathbb{Z}$ is principal. The same argument we used for that can easily be adapted to prove Proposition 1.1.1. The main change is that you now need to take a nonzero $b \in I$ with smallest possible $N(b)$. (Here, N is a fixed Euclidean norm on R.) For details, see [DF, §8.1, proof of Proposition 1]. □

Remark 1.1.2. You might wonder why we required R to be an integral domain in the definition of a Euclidean domain. I don't know. In my opinion, we could just as well have dropped this requirement and merely required R to be a commutative ring instead. Proposition 1.1.1 would remain true, and we would gain a few more examples of Euclidean domains (although we should not be calling them "domains" any more). For example, for each positive integer n, the ring $\mathbb{Z}/n$ would be a Euclidean "domain" in this wider sense (with an Euclidean norm sending each coset $a + n\mathbb{Z}$ to the remainder of a divided by n).

See `https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf` for more about Euclidean domains.

1.2. Principal Ideal Domains ([DF, §8.1 and §8.2])

Proposition 1.1.1 is so useful that its conclusion (viz., that any ideal of R is principal) has been given its own name:

Definition 1.2.1. An integral domain R is said to be a **principal ideal domain** (for short, **PID**) if each ideal of R is principal.

Thus, Proposition 1.1.1 can be rewritten as follows:

Proposition 1.2.2. Any Euclidean domain is a PID.

The converse is not true, although counterexamples are hard to find. One of the simplest is the ring $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$, where $\alpha = \dfrac{1+\sqrt{-19}}{2}$. (See [DF, page 282] for a proof that this ring is a PID but not a Euclidean domain.)

Much of the basic theory of commutative rings can be viewed as a project to generalize the classical arithmetic of the integers to wider classes of "numbers". As part of this project, we shall now define gcds and lcms in commutative rings. Our definition will be stated for arbitrary commutative rings, but we will soon see that they behave particularly well for when the ring is a PID (which is why we are only doing this definition now). [1]

Definition 1.2.3. Let R be a commutative ring.

Let $a \in R$.

(a) A **multiple** of a means an element of the principal ideal aR.

(b) A **divisor** of a means an element $d \in R$ such that a is a multiple of d (that is, $a \in dR$). We write "$d \mid a$" for "d is a divisor of a".

Now, let $a \in R$ and $b \in R$.

(c) A **common divisor** of a and b means an element of R that is a divisor of a and a divisor of b at the same time.

(d) A **common multiple** of a and b means an element of R that is a multiple of a and a multiple of b at the same time.

(e) A **greatest common divisor** (short: **gcd**) of a and b means a common divisor d of a and b such that **every** common divisor of a and b is a divisor of d.

(f) A **lowest common multiple** (short: **lcm**) of a and b means a common multiple m of a and b such that **every** common multiple of a and b is a multiple of m.

The concepts of "multiple" and "divisor" we just introduced are straightforward generalizations of the corresponding concepts from arithmetic[2]. (You recover the latter concepts if you set $R = \mathbb{Z}$.) The notions of "gcd" and "lcm" are a bit subtler: If a and b are two integers, then their gcd $\gcd(a, b)$ in the sense of classical arithmetic is a gcd of a and b in the sense of Definition 1.2.3 **(e)**; however, so is $-\gcd(a, b)$. So our new notion of a gcd is slightly more liberal than the classical notion, in the sense that it allows for negative gcds. The same holds for lcms. Thus, gcds and lcms in our sense are not literally unique.

[1] The notions of "greatest common divisor" and "lowest common multiple" that we will now introduce are not literal generalizations the corresponding notions from classical arithmetic. See below for the exact relation.

[2] Here I am assuming that you are using the "right" definitions of the latter concepts. For example, every integer (including 0 itself) is a divisor of 0. Some authors dislike this and prefer to explicitly require 0 to not divide 0; in that case, of course, my definition does not agree with theirs.

This is one reason why we said "a gcd" and "a lcm" (rather than "the gcd" and "the lcm") in Definition 1.2.3. Another reason is that a and b might not have any gcd to begin with. (We will later see some examples where this happens.)

Before we explore gcds and lcms in arbitrary commutative rings, let us record the precise relation between them and the classical arithmetic notions:

Proposition 1.2.4. Let a and b be two integers. Let $g = \gcd(a,b)$ and $\ell = \operatorname{lcm}(a,b)$, where we are using the classical arithmetic definitions of gcd and lcm. Then:

(a) The gcds of a and b (in the sense of Definition 1.2.3 **(e)**) are g and $-g$.

(b) The lcms of a and b (in the sense of Definition 1.2.3 **(f)**) are ℓ and $-\ell$.

Proof. **(a)** It is known from classical arithmetic that g is a common divisor of a and b, and that every common divisor of a and b is a divisor of g. In other words, g is a gcd of a and b in the sense of Definition 1.2.3 **(e)**. It is easy to see that this property is inherited by $-g$ as well (since divisibilities don't change when we replace g by $-g$). Thus, both numbers g and $-g$ are gcds of a and b in the sense of Definition 1.2.3 **(e)**. It remains to show that they are the only gcds of a and b in this sense.

So let u be a gcd of a and b in the sense of Definition 1.2.3 **(e)**. We must show that $u \in \{g, -g\}$.

From the way we introduced u, we know that u is a common divisor of a and b, and that every common divisor of a and b is a divisor of u. The first of these two facts yields that $u \mid g$ (since any common divisor of a and b is a divisor of g); the second yields that $g \mid u$ (since g is a common divisor of a and b, and thus is a divisor of u). Combining $u \mid g$ and $g \mid u$, we find $u = \pm g$. In other words, $u \in \{g, -g\}$. This finishes our proof of part **(a)**.

(b) The proof is similar to that for part **(a)**. □

Now, what about gcds and lcms in other rings? The existence of a gcd is far from god-given, as the following example shows:

Example 1.2.5. Let R be the ring

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}.$$

Let $a = 4$ and $b = 2\left(1 + \sqrt{-3}\right)$. Then, a and b have no gcd in R; nor do they have an lcm in R. You will prove this in exercise 7 on homework set #2.

Uniqueness of gcds and lcms is a simpler question: They are rarely unique on the nose, but they are always unique up to multiplication by a unit when the ring is an integral domain. Before we show this, let me introduce a word for this:

Definition 1.2.6. Let R be a commutative ring. Let $a, b \in R$. We say that a is **associate** to b in R (and we write $a \sim b$) if there exists a unit u of R such that $a = bu$.

Instead of saying "a is associate to b", we shall also say that "a and b are associate". (This is justified by the fact – which we will prove in Proposition 1.2.7 – that $\sim$ is an equivalence relation.)

For example:

- Two integers a and b are associate in $\mathbb{Z}$ if and only if $a = \pm b$ (that is, if and only if $a = b$ or $a = -b$).
- Any two nonzero elements a and b of a field are associate in that field (since $\frac{a}{b}$ is a unit and satisfies $a = b \cdot \frac{a}{b}$).
- Let F be a field. Any nonzero polynomial $f \in F[x]$ is associate to a monic polynomial (since its leading coefficient is a unit).
- It is not hard to prove that the only units of the ring $\mathbb{Z}[i]$ are the four Gaussian integers $1, i, -1, -i$. Thus, two Gaussian integers α and β in $\mathbb{Z}[i]$ are associate if and only if $\alpha \in \{\beta, i\beta, -\beta, -i\beta\}$.

A general property of associateness is the following:

Proposition 1.2.7. Let R be a commutative ring. The relation $\sim$ is an equivalence relation.

Proof. This is fairly straightforward. We need to show that the relation $\sim$ is reflexive, symmetric and transitive.

Reflexivity: Any $a \in R$ satisfies $a \sim a$, since the unity 1_R is a unit and satisfies $a = a1_R$.

Symmetry: If $a, b \in R$ satisfy $a \sim b$, then they also satisfy $b \sim a$. Indeed, $a \sim b$ shows that there is a unit u of R such that $a = bu$; but this unit u clearly has an inverse u^{-1}, which is itself a unit and satisfies $b = au^{-1}$. But this shows that $b \sim a$.

Transitivity: If $a, b, c \in R$ satisfy $a \sim b$ and $b \sim c$, then they also satisfy $a \sim c$. Indeed, there exist two units u and v of R such that $a = bu$ and $b = cv$ (since $a \sim b$ and $b \sim c$); but the product uv of these two units is again a unit, and satisfies $a = \underbrace{b}_{=cv} u = cvu = cuv$, so that $a \sim c$. □

Note that an element a of a ring R is associate to 1 if and only if a is a unit.

If two elements a and b of a ring R are associate, then each is a multiple of the other (i.e., we have $a \mid b$ and $b \mid a$). When R is an integral domain, the converse holds as well:

Proposition 1.2.8. Let R be an integral domain. Let $a, b \in R$ be such that $a \mid b$ and $b \mid a$. Then, $a \sim b$.

Proof. From $a \mid b$, we see that there exists an $x \in R$ such that $b = ax$. Consider this x.

From $b \mid a$, we see that there exists a $y \in R$ such that $a = by$. Consider this y.

If $a = 0$, then the claim is easy (indeed, if $a = 0$, then $b = \underbrace{a}_{=0} x = 0$, so that $a = 0 = b$ and thus $a \sim b$). Hence, we WLOG assume that $a \neq 0$.

Now, $a = \underbrace{b}_{=ax} y = axy$. In other words, $a(1 - xy) = 0$. Since $a \neq 0$, we thus conclude $1 - xy = 0$ (since R is an integral domain). In other words, $xy = 1$. Thus, y is a unit (since R is commutative). Hence, from $a = by$, we obtain $a \sim b$. □

Note that Proposition 1.2.8 becomes false if we drop the "integral domain" condition. Some sophisticated counterexamples can be found at `https://math.stackexchange.com/questions/14270/` .

We can now state the uniqueness of gcds and lcms in a slick way:

Proposition 1.2.9. Let R be an integral domain. Let $a, b \in R$. Then:
(a) Any two gcds of a and b are associate (i.e., associate to each other).
(b) Any two lcms of a and b are associate (i.e., associate to each other).

Proof. **(a)** Let c and d be two gcds of a and b. We must show that $c \sim d$.

Any common divisor of a and b is a divisor of c (since c is a gcd of a and b); however, d is a common divisor of a and b (since d is a gcd of a and b). Thus, d is a divisor of c. In other words, $d \mid c$. The same argument, with the roles of c and d swapped, yields $c \mid d$. Hence, Proposition 1.2.8 (applied to c and d instead of a and b) yields $c \sim d$.

(b) Analogous to part **(a)**. □

From Proposition 1.2.9, we recover the fact that gcds and lcms of integers are unique up to sign (since two integers a and b are associate in $\mathbb{Z}$ if and only if $a = \pm b$).

We have now talked enough about uniqueness; when do gcds and lcms exist? The following fact covers one important case:

Theorem 1.2.10. Let R be a PID. Let $a, b \in R$. Then, there exist a gcd and an lcm of a and b.

This will follow from the following proposition, which characterizes lcms and partly characterizes gcds in terms of principal ideals:

Proposition 1.2.11. Let R be a commutative ring. Let $a, b, c \in R$.
(a) If $aR + bR = cR$, then c is a gcd of a and b.
(b) We have $aR \cap bR = cR$ if and only if c is an lcm of a and b.

Note that $aR + bR = cR$ is an equality between ideals (the $+$ sign on the left hand side is a sum of ideals); it is **not** to be confused with $a + b = c$. Confusingly, $a + b = c$ does **not** imply $aR + bR = cR$ (since there is no "distributivity law" that would equate $(a + b) R$ with $aR + bR$). Instead, it is easy to see that "$aR + bR = cR$" is equivalent to "a and b are multiples of c, and there exist two elements $u, v \in R$ satisfying $c = au + bv$".

Note the difference between the two parts of Proposition 1.2.11: Part **(b)** is an "if and only if", while part **(a)** is only an "if". This is no accident: Proposition 1.2.11 **(a)** cannot be extended to an "if and only if" statement. For example, in the polynomial ring $\mathbb{Q}[x, y]$, the two polynomials x and y have gcd 1; however, 1 is not a $\mathbb{Q}[x, y]$-linear combination of x and y.

Proof of Proposition 1.2.11. **(a)** Assume that $aR + bR = cR$. Thus, $c \in cR = aR + bR$. In other words, there exist $x, y \in R$ such that $c = ax + by$. Hence, if r is a common divisor of a and b, then $r \mid c$ [3]. Thus, we have shown that any common divisor of a and b is a divisor of c.

We have $a \in aR \subseteq aR + bR = cR$. In other words, $c \mid a$. Similarly, $c \mid b$. Hence, c is a common divisor of a and b. Combining this result with the result of the previous paragraph, we conclude that c is a gcd of a and b. This proves Proposition 1.2.11 **(a)**.

(b) Recall that an lcm of a and b was defined (in Definition 1.2.3 **(f)**) to be a common multiple m of a and b with the property that every common multiple of a and b is a multiple of m. Hence, we have the following chain of equivalences:

$$\begin{aligned}
&(c \text{ is an lcm of } a \text{ and } b) \\
&\iff \left(\begin{array}{c} c \text{ is a common multiple of } a \text{ and } b, \text{ and} \\ \text{every common multiple of } a \text{ and } b \text{ is a multiple of } c \end{array} \right) \\
&\iff (c \in aR \cap bR \text{ and every element of } aR \cap bR \text{ is a multiple of } c)
\end{aligned}$$

(since the common multiples of a and b are precisely the elements of $aR \cap bR$).

Now, let us look a bit closer at the statements on the right hand side. The statement "$c \in aR \cap bR$" is equivalent to "$cR \subseteq aR \cap bR$" (indeed, the set $aR \cap bR$ is an ideal of R, and thus it contains the element c if and only if it contains all multiples of c; in other words, it contains the element c if and only if it contains the subset cR). The statement "every element of $aR \cap bR$

[3] *Proof.* Let r be a common divisor of a and b. Thus, $r \mid a$ and $r \mid b$. In other words, we can write a and b in the forms $a = ra'$ and $b = rb'$ for some $a', b' \in R$. Using these a', b', we obtain $c = \underbrace{a}_{=ra'} x + \underbrace{b}_{=rb'} y = ra'x + rb'y = r(a'x + b'y)$, so that $r \mid c$. Qed.

is a multiple of c" is equivalent to "$aR \cap bR \subseteq cR$" (since cR is the set of all multiples of c). Thus, our chain of equivalences can be continued as follows:

$$\begin{aligned}
&(c \text{ is an lcm of } a \text{ and } b) \\
&\iff \left(\underbrace{c \in aR \cap bR}_{\iff cR \subseteq aR \cap bR} \text{ and } \underbrace{\text{every element of } aR \cap bR \text{ is a multiple of } c}_{\iff aR \cap bR \subseteq cR} \right) \\
&\iff (cR \subseteq aR \cap bR \text{ and } aR \cap bR \subseteq cR) \\
&\iff (aR \cap bR = cR) .
\end{aligned}$$

This proves Proposition 1.2.11 **(b)**. □

Proof of Theorem 1.2.10. The sum $aR + bR$ is an ideal of R, and thus is a principal ideal (since R is a PID). In other words, $aR + bR = cR$ for some $c \in R$. Consider this c. Hence, Proposition 1.2.11 **(a)** yields that c is a gcd of a and b. Hence, a gcd of a and b exists.

The intersection $aR \cap bR$ is an ideal of R, and thus is a principal ideal (since R is a PID). In other words, $aR \cap bR = cR$ for some $c \in R$. Consider this c. Hence, Proposition 1.2.11 **(b)** yields that c is an lcm of a and b. Hence, an lcm of a and b exists. Theorem 1.2.10 is now proven. □

So any two elements of a PID have a gcd and an lcm. If the PID is Euclidean, then the gcd can be computed by the Euclidean algorithm. (See [DF, pages 275–276] for an example.) The gcd and the lcm are determined by one another via the formula

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) \sim ab$$

(see exercise 3 on homework set #2 for a proof).

See `https://www.math.columbia.edu/~rf/factorization1.pdf` for more about PIDs.

1.3. Unique Factorization Domains ([DF, §8.3])

The notions of integral domains, of Euclidean domains and of PIDs are abstractions for certain properties that hold for the ring $\mathbb{Z}$: The first one abstracts the fact that products of nonzero integers are nonzero; the second abstracts division with remainder; the third abstracts the fact that each ideal of $\mathbb{Z}$ is principal. As we have seen, PIDs are a weaker form of Euclidean domains. Even weaker is the notion of a **UFD** (short for **Unique Factorization Domain**). This abstracts the existence and the uniqueness of a prime factorization for integers. How do we define it in arbitrary integral domain? What is a good analogue of a prime number in a general integral domain?

There are at least four such analogues. Let us introduce the first two:

Definition 1.3.1. Let R be a commutative ring. Let $r \in R$ be nonzero and not a unit.

(a) We say that r is **irreducible** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $ab = r$, at least one of a and b is a unit.

(b) We say that r is **prime** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $r \mid ab$, we have $r \mid a$ or $r \mid b$.

Let us see what these concepts mean when $R = \mathbb{Z}$. Both notions "irreducible" and "prime" smell like prime numbers, but it is worth being precise: Not only the prime numbers $2, 3, 5, 7, 11, \ldots$ themselves, but also their negatives $-2, -3, -5, -7, -11, \ldots$ fit both bills (i.e., they are irreducible and prime in $\mathbb{Z}$). Let us be more explicit:

Proposition 1.3.2. Let $r \in \mathbb{Z}$. Then, we have the following equivalences:

$$(r \text{ is prime in } \mathbb{Z}) \iff (r \text{ is irreducible in } \mathbb{Z}) \iff (|r| \text{ is a prime number}).$$

Proof. It suffices to prove the three implications

$$(r \text{ is prime in } \mathbb{Z}) \Longrightarrow (r \text{ is irreducible in } \mathbb{Z});$$
$$(r \text{ is irreducible in } \mathbb{Z}) \Longrightarrow (|r| \text{ is a prime number});$$
$$(|r| \text{ is a prime number}) \Longrightarrow (r \text{ is prime in } \mathbb{Z}).$$

All of them are LTTR. (The first one is actually a particular case of Proposition 1.3.3 further below. For the other two, it is recommended to WLOG assume that $r \geq 0$, since it is easy to see that none of the three statements involved changes when r is replaced by $-r$.) □

Thus, in the ring $\mathbb{Z}$, being prime and being irreducible is the same thing. What about arbitrary integral domains? Here it is not quite the case, as the following two examples show:

- In the ring $\mathbb{Z}\left[\sqrt{-5}\right]$, the element 3 is irreducible but not prime (in $\mathbb{Z}\left[\sqrt{-5}\right]$). (See [DF, §8.3] for the proof.)
- Here is an example using polynomials: Define a subset R of the univariate polynomial ring $\mathbb{Q}[x]$ by[4]

$$\begin{aligned} R &= \left\{ f \in \mathbb{Q}[x] \mid \text{the } x^1\text{-coefficient of } f \text{ is } 0 \right\} \\ &= \left\{ f \in \mathbb{Q}[x] \mid \text{the derivative of } f \text{ at } 0 \text{ is } 0 \right\} \\ &= \left\{ a_0 + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \mid n \geq 0 \text{ and } a_0, a_2, a_3, \ldots, a_n \in \mathbb{Q} \right\}. \end{aligned}$$

[4]The "x^1-coefficient" of a polynomial f means the coefficient of f before x^1. For example, the x^1-coefficient of $(x+1)^6$ is 6, whereas the x^1-coefficient of $x^2 + 1$ is 0.

It is not hard to see that R is a subring of $\mathbb{Q}[x]$. (Indeed, if f and g are two polynomials whose x^1-coefficients are 0, then the same holds for $f+g$ and $f-g$ and fg. This is easiest to see by computing $f+g$ and $f-g$ and fg and checking that there is no way an x^1-monomial can appear in the results.)

When we study polynomials later on, we will prove that $\mathbb{Q}[x]$ is an integral domain. (This is in fact pretty easy: When you multiply two nonzero polynomials in $\mathbb{Q}[x]$, their leading terms get multiplied, so their degrees get added; thus, the product cannot be 0.) Thus, the ring R (being a subring of the integral domain $\mathbb{Q}[x]$) must itself be an integral domain (since a subring of an integral domain is always itself an integral domain[5]).

Now, the ring R contains no polynomials of degree 1. However, if $a, b \in \mathbb{Q}[x]$ are two polynomials satisfying $x^3 = ab$, then $3 = \deg\left(x^3\right) = \deg(ab) = \deg a + \deg b$, which means that one of the polynomials a and b is either a constant (and thus a unit in R) or has degree 1 (and thus cannot lie in R). This quickly shows that the element x^3 of R is irreducible in R. However, this element is not prime in R (since $x^3 \mid x^2x^2$ but $x^3 \nmid x^2$).

In each of these two examples, we found an irreducible element that is not prime. Can we do the opposite? No, as the following fact shows:

Proposition 1.3.3. Let R be an integral domain. Then, any prime element of R is irreducible.

Proof. Let $r \in R$ be prime. We must show that r is irreducible.

So let $a, b \in R$ satisfy $ab = r$. We must show that at least one of a and b is a unit.

We have $ab = r$, so $r \mid ab$. Since r is prime, we thus obtain $r \mid a$ or $r \mid b$ (by the definition of "prime"). Assume WLOG that $r \mid a$ (since otherwise, we have $r \mid b$, so we can swap a with b to achieve $r \mid a$). Hence, $a = rx$ for some $x \in R$. Consider this x. Now, $r = \underbrace{a}_{=rx} b = rxb$, so $r(1-xb) = r - rxb = 0$, and thus $1 - xb = 0$ (since $r \neq 0$ and since R is an integral domain). In other words, $xb = 1$. This shows that b is a unit (since R is commutative). Thus we have shown that at least one of a and b is a unit. This completes the proof that r is irreducible. □

In a PID, the converse of Proposition 1.3.3 also holds:

Proposition 1.3.4. Let R be a PID. Let $r \in R$. Then, r is prime if and only if r is irreducible.

Proof. We already showed the "only if" part in Proposition 1.3.3. We thus only need to prove the "if" part.

[5] This is obvious if you recall the definition of an integral domain.

Assume that r is irreducible. We must show that r is prime.

Let $a, b \in R$ satisfy $r \mid ab$. We must prove that $r \mid a$ or $r \mid b$.

Assume the contrary. Thus, we have neither $r \mid a$ nor $r \mid b$.

There is an $h \in R$ such that $ab = rh$ (since $r \mid ab$). Consider this h.

Since R is a PID, the ideal $aR + rR$ is principal; in other words, there exists some $g \in R$ such that $gR = aR + rR$. Consider this g. Hence, $a \in aR \subseteq aR + rR = gR$; in other words, $g \mid a$.

Also, $r \in rR \subseteq aR + rR = gR$; in other words, g is a divisor of r. However, r is irreducible, and thus every divisor of r is either a unit or associate to r [6]. Thus, g is either a unit or associate to r (since g is a divisor of r). However, if g was associate to r, then we would have $r \mid g \mid a$, which would contradict the fact that we don't have $r \mid a$. Thus, g cannot be associate to r, and so g must be a unit. Therefore, $1 = gg^{-1} \in gR = aR + rR$. Hence, there exist $u, v \in R$ such that $1 = au + rv$.

The same argument (using b instead of a) shows that there exist $u', v' \in R$ such that $1 = bu' + rv'$.

Now, consider these four elements u, v, u', v'. Multiplying $1 = au + rv$ with $1 = bu' + rv'$ yields

$$\begin{aligned} 1 &= (au + rv)\left(bu' + rv'\right) = \underbrace{ab}_{=rh} uu' + rvbu' + aurv' + rvrv' \\ &= rhuu' + rvbu' + aurv' + rvrv' = r\underbrace{\left(huu' + vbu' + auv' + vrv'\right)}_{\in R} \in rR. \end{aligned}$$

In other words, there exists some $s \in R$ such that $1 = rs$. This shows that r is a unit. This contradicts the fact that r is irreducible. Thus, the proof of Proposition 1.3.4 is complete. □

So we have generalized (in two ways, to boot) the notion of a prime number. Let us now generalize prime factorization:

Definition 1.3.5. Let R be an integral domain.

(a) An **irreducible factorization** of an element $r \in R$ means a tuple $(p_1, p_2, \ldots, p_n)$ of irreducible elements $p_1, p_2, \ldots, p_n$ of R such that $r \sim p_1 p_2 \cdots p_n$. (Note that this tuple $(p_1, p_2, \ldots, p_n)$ can be empty; in this case, the product $p_1 p_2 \cdots p_n$ is empty and thus equals to 1. Thus, the empty tuple is an irreducible factorization of any unit of R.)

(b) We say that R is a **unique factorization domain** (or, for short, **UFD**) if each nonzero $r \in R$ satisfies the following two statements:

1. There exists an irreducible factorization of r.

[6] *Proof.* Let d be a divisor of r. We must show that d is either a unit or associate to r.

Indeed, there exists some $q \in R$ such that $r = dq$ (since d is a divisor of r). Consider this q. Since r is irreducible, at least one of d and q is a unit. Hence, d is either a unit or associate to r (because if q is a unit, then d is associate to r (since $r = dq$ yields $r \sim d$ and thus $d \sim r$)).

2. The irreducible factorization of r is unique up to associates. This means the following: If $(p_1, p_2, \ldots, p_n)$ and $(q_1, q_2, \ldots, q_m)$ are two irreducible factorizations of r (so that $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_m$ are irreducible elements of R satisfying $r \sim p_1 p_2 \cdots p_n$ and $r \sim q_1 q_2 \cdots q_m$), then we have $n = m$ and there is a bijection $\alpha : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ such that $p_i \sim q_{\alpha(i)}$ for each $i \in \{1, 2, \ldots, n\}$.

My notion of an irreducible factorization differs slightly from that in [DF] (in that [DF] requires $r = p_1 p_2 \cdots p_n$, whereas we only require $r \sim p_1 p_2 \cdots p_n$); I hold mine to be slightly better-behaved (for example, $-1 \in \mathbb{Z}$ would not have an irreducible factorization in the [DF] sense). But my definition of a UFD is equivalent to the one in [DF], as can be easily seen.

In the next lecture, we will see that every PID is a UFD, and there are more UFDs than PIDs.