Math 4527 (Number Theory 2)

Lecture #24 of 37 $\sim$ March 17, 2021

Principal Ideal Domains + Unique Factorization Domains

- Principal Ideal Domains
- Unique Factorization Domains

This material represents §8.1.7-8.1.8 from the course notes.

Recall, I

Last time, we discussed Euclidean domains:

Definition

A Euclidean domain (or domain with a division algorithm) is an integral domain R that possesses a norm N with the property that, for every a and b in R with $b \neq 0$, there exist some q and r in R such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$.

Some Euclidean domains are $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$ for F a field. We can compute gcds in Euclidean domains using the Euclidean algorithm.

We also showed that every ideal in a Euclidean domain is principal.

Principal Ideal Domains, I

We have seen that every ideal in a Euclidean domain is principal. We now expand our attention to the more general class of rings in which every ideal is principal.

Definition

A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Examples:

1. Every Euclidean domain is a PID, so $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$ are all PIDs.
2. $\mathbb{Z}[x]$ is not a PID because $(2, x)$ is not principal.
3. $\mathbb{Z}[\sqrt{-5}]$ is not a PID because $(2, 1+\sqrt{-5})$ is not principal.
4. There exist PIDs that are not Euclidean domains (although this is not so easy to prove). One example is the quadratic integer ring $\mathcal{O}_{\sqrt{-19}} = \mathbb{Z}[(1+\sqrt{-19})/2]$.

Principal Ideal Domains, II

Like in Euclidean domains, we can show that any two elements in a PID have a greatest common divisor.

- The substantial advantage of a Euclidean domain over a general PID is that we have an algorithm for computing greatest common divisors in Euclidean domains, rather than merely knowing that they exist, as is the case in PIDs.

Principal Ideal Domains, III

Proposition (GCDs in PIDs)

If R is a principal ideal domain and $a, b \in R$ are nonzero, then any generator d of the principal ideal (a, b) is a greatest common divisor of a and b. (In particular, any two elements in a principal ideal domain always possess at least one gcd.) Furthermore, there exist elements $x, y \in R$ such that $d = ax + by$.

Proof:

- We showed already that if (a, b) is principal, then any generator is a gcd of a and b. This shows the first two statements.
- Furthermore, if $(a, b) = (d)$ then $d \in (a, b)$ implies that $d = ax + by$ for some $x, y \in R$ by our description of the ideal (a, b).

Principal Ideal Domains, IV

Our goal now is to show that principal ideal domains (like the prototypical examples $\mathbb{Z}$ and $F[x]$) have the property that every nonzero element can be written as a finite product of irreducible elements, up to associates and reordering.

- To show this, we will use essentially the same structure of argument as in $\mathbb{Z}$ and $F[x]$: first we will prove that every element can be factored into a product of irreducibles, and then we will prove that the factorization is unique.

Principal Ideal Domains, V

So, we must show that (i) factorizations exist, and (ii) are unique.

- For the existence, if r is a reducible element then we can write $r = r_1 r_2$ where neither r_1 nor r_2 is a unit. If both r_1 and r_2 are irreducible, we are done: otherwise, we can continue factoring (say) $r_1 = r_{1,1} r_{1,2}$ with neither term a unit. If $r_{1,1}$ and $r_{1,2}$ are both irreducible, we are done: otherwise, we factor again.
- We need to ensure that this process will always terminate: if not, we would obtain an infinite ascending chain of ideals $(r) \subset (r_1) \subset (r_{1,1}) \subset \cdots$, so first we will prove that this cannot occur.
- Then to establish uniqueness, we use the same argument as in $\mathbb{Z}$ and $F[x]$: this requires showing that if p is irreducible, then $p|ab$ implies $p|a$ or $p|b$: in other words, that p is prime.

Principal Ideal Domains, VI

First we establish the necessary result about ascending chains of ideals:

Theorem (Ascending Chains in PIDs)

If R is a principal ideal domain and the ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$ form an ascending chain, then there exists some positive integer N after which the chain is stationary: $I_n = I_N$ for all $n \geq N$.

Remark: A ring satisfying this "ascending chain condition" is called Noetherian, after Emmy Noether, who pioneered much of commutative algebra.

- Noetherian rings are quite important because of this finiteness property, which is (in a sense that one can make precise) a sort of algebraic version of compactness.

Principal Ideal Domains, VII

Proof:

- Suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an ascending chain in a PID R, and let J be the union of the ideals in the chain.
- On your last homework, you showed that that the union of an ascending chain of ideals is also an ideal, so J is an ideal.
- Since R is a PID, we see $J = (a)$ for some $a \in R$. But since J is a union, this means $a \in I_N$ for some N.
- But now, for each $n \geq N$, we see $(a) = I_N \subseteq I_n \subseteq J = (a)$.
- We must have equality everywhere, so $I_n = I_N$ for all $n \geq N$, and the chain stabilizes.

Principal Ideal Domains, VIII

Next, we show that irreducible elements are prime:

Proposition (Irreducibles are Prime in a PID)

Every irreducible element in a principal ideal domain is prime.

<u>Proof</u>:

- Suppose that p is irreducible. We show that (p) is prime.
- So suppose (a) is an ideal containing (p): then $p \in (a)$ so $p = ra$ for some $r \in R$. But since p is irreducible, we either have $p|r$ or $p|a$, which is to say, either $r \in (p)$ or $a \in (p)$.
- If $a \in (p)$ then $(a) \subseteq (p)$ and so $(a) = (p)$.
- Otherwise, if $r \in (p)$ then $r = sp$ for some $s \in R$, and then $p = ra$ implies $p = spa$, so since $p \neq 0$ we see $sa = 1$ and therefore a is a unit, and so $(a) = R$.
- Thus, (a) is either (p) or R, meaning that (p) is a maximal ideal, hence also a prime ideal.

Principal Ideal Domains, IX

In fact, our proof shows more than we claimed; namely, that nonzero prime ideals are maximal in PIDs:

Proposition (Prime Implies Maximal in a PID)

Every nonzero prime ideal in a principal ideal domain is maximal.

Proof:

- Suppose that $I = (p)$ is a nonzero prime ideal of R, and suppose that (a) is an ideal containing I.
- Since $p \in (a)$, we see that $p = ra$ for some $r \in R$. But then $ra \in (p)$, so since (p) is a prime ideal we either have $r \in (p)$ or $a \in (p)$.
- By the same argument as on the previous slide, this means (a) is either (p) or R, meaning that (p) is a maximal ideal.

Principal Ideal Domains, X

Now we can establish that principal ideal domains have unique factorization:

Theorem (Unique Factorization in PIDs)

If R is a principal ideal domain, then every nonzero nonunit $r \in R$ can be written as a finite product of irreducible elements. Furthermore, this factorization is unique up to associates: if $r = p_1 p_2 \cdots p_d = q_1 q_2 \cdots q_k$ for irreducibles p_i and q_j, then $d = k$ and there is some reordering of the factors such that p_i is associate to q_i for each $1 \leq i \leq k$.

This is just a matter of putting together the pieces we have already established and doing some bookkeeping.

Principal Ideal Domains, XI

Proof:

- Suppose $r \in R$ is not zero and not a unit.
- If r is irreducible, we already have the required factorization. Otherwise, $r = r_1 r_2$ for some nonunits r_1 and r_2. If both r_1 and r_2 are irreducible, we are done: otherwise, we can continue factoring (say) $r_1 = r_{1,1} r_{1,2}$ with neither term a unit. If $r_{1,1}$ and $r_{1,2}$ are both irreducible, we are done: otherwise, we factor again.
- We claim that this process must terminate eventually: otherwise (as follows by the axiom of choice), we would have an infinite chain of elements x_1, x_2, x_3, ... , such that $x_1 | r$, $x_2 | x_1$, $x_3 | x_2$, and so forth, where no two elements are associates.

Principal Ideal Domains, XII

Proof (continued):

- But if we have $x_1 | r$, $x_2 | x_1$, $x_3 | x_2$, and so forth, where no two elements are associates, then we get an infinite chain of ideals $(r) \subset (x_1) \subset (x_2) \subset \cdots$ with each ideal properly contained in the next. But this is impossible, since every ascending chain of ideals in R must become stationary.
- Thus, the factoring process must terminate, and so r can be written as a product of irreducibles.
- We establish uniqueness by induction on the number of irreducible factors of $r = p_1 p_2 \cdots p_n$.
- If $n = 1$, then r is irreducible. If r had some other nontrivial factorization $r = qc$ with q irreducible, then q would divide r hence be associate to r (since irreducibles are prime). But this would mean that c is a unit, which is impossible.

Principal Ideal Domains, XIII

Proof (continued more):

- Now suppose $n \geq 2$ and that $r = p_1 p_2 \cdots p_d = q_1 q_2 \cdots q_k$ has two factorizations into irreducibles.
- Since $p_1 | (q_1 \cdots q_k)$ and p_1 is irreducible hence prime, repeatedly applying the fact that p irreducible and $p|ab$ implies $p|a$ or $p|b$ shows that p_1 must divide q_i for some i.
- By rearranging we may assume $q_1 = p_1 u$ for some u: then since q_1 is irreducible (and p_1 is not a unit), u must be a unit, so p_1 and q_1 are associates.
- Cancelling then yields the equation $p_2 \cdots p_d = (uq_2) \cdots q_k$, which is a product of fewer irreducibles.
- By the induction hypothesis, such a factorization is unique up to associates. This immediately yields the desired uniqueness result for r as well, so we are done.

Principal Ideal Domains, XIV

So, we have just established that every principal ideal domain has unique factorization, in the precise sense that every nonzero nonunit can be uniquely written as a product of irreducible elements up to associates.

- Of course, this theorem does not actually tell us how to compute these factorizations: it just assures us that if we simply start factoring an element, we will eventually be able to terminate with a factorization into irreducibles, and this factorization will be unique up to associates.

In general, how we could actually go about computing factorizations will depend on the ring.

- Consider, for example, how different the questions of factoring the integer 11729581 in $\mathbb{Z}$, the element $97 + 65i$ inside $\mathbb{Z}[i]$, the polynomial $x^{2021} + 7x + 9$ inside $\mathbb{F}_{11}[x]$, and the polynomial $x^5 + 4x + 2$ inside $\mathbb{C}[x]$ are....

Unique Factorization Domains, I

Now we will study the more general class of integral domains having unique factorization:

Definition

An integral domain R is a unique factorization domain (UFD) if every nonzero nonunit $r \in R$ can be written as a finite product $r = p_1 p_2 \cdots p_d$ of irreducible elements, and this factorization is unique up to associates: if $r = p_1 p_2 \cdots p_d = q_1 q_2 \cdots q_k$ for irreducibles p_i and q_j, then $d = k$ and there is some reordering of the factors such that p_i is associate to q_i for each $1 \leq i \leq k$.

Examples:

1. Every principal ideal domain is a unique factorization domain: thus $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$ are unique factorization domains.
2. As we essentially proved already, the polynomial ring $\mathbb{Z}[x]$ is a UFD, even though it is not a PID.

Unique Factorization Domains, II

There are two ways an integral domain can fail to be a unique factorization domain: one way is for some element to have two inequivalent factorizations, and the other way is for some element not to have any factorization.

- Both of these situations can occur independently of one another, as I will show via example.

Unique Factorization Domains, III

Examples:

3. The ring $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain because we have a non-unique factorization given by $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$.
   - Note that each of $1 \pm \sqrt{-5}$, 2, and 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$ since their norms are 6, 4, and 9 respectively and there are no elements in $\mathbb{Z}[\sqrt{-5}]$ of norm 2 or 3.
   - Also, none of 2, 3, and $1 \pm \sqrt{-5}$ are associate to one another, since the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.
   - Thus, 6 has two inequivalent factorizations into irreducibles in $\mathbb{Z}[\sqrt{-5}]$.

Unique Factorization Domains, IV

Examples:

4. The ring $\mathbb{Z}[2i]$ is not a unique factorization domain because we have a non-unique factorization $4 = 2 \cdot 2 = 2i \cdot 2i$.
   - Note that both 2 and $2i$ are irreducible since their norms are both 4 and there are no elements in $\mathbb{Z}[2i]$ of norm 2.
   - Also, 2 and $2i$ are not associate since $i \notin \mathbb{Z}[2i]$.
   - Thus, 4 has two inequivalent factorizations into irreducibles in $\mathbb{Z}[2i]$.

Unique Factorization Domains, V

Examples:

5. The ring $\mathbb{Z} + x\mathbb{Q}[x]$ of polynomials with rational coefficients and integral constant term is not a unique factorization domain because not every element has a factorization.
   - This is a little trickier to see.
   - Explicitly, the element x is not irreducible since $x = 2 \cdot \frac{1}{2}x$ and neither 2 nor $\frac{1}{2}x$ is a unit.
   - However, x cannot be written as a finite product of irreducible elements: any such factorization would necessarily consist of a product of constants times a rational multiple of x, but no rational multiple of x is irreducible in $\mathbb{Z} + x\mathbb{Q}[x]$.
   - So, no matter how much we attempt to factor x, we can never finish.

Unique Factorization Domains, VI

We showed last time that in a PID, the irreducible elements are the same as the prime elements. This turns out also to be true in unique factorization domains:

Proposition (Irreducibles are Prime in a UFD)

Every irreducible element in a unique factorization domain is prime.

Thus, we may interchangeably refer to "prime factorizations" or "irreducible factorizations" in a UFD, since these amount to the same thing.

Unique Factorization Domains, VII

Proof:

- Suppose that p is an irreducible element of R and that $p|ab$ for some elements $a, b \in R$. We must show that $p|a$ or $p|b$.
- Since R is a unique factorization domain, we may write $a = q_1 q_2 \cdots q_d$ and $b = r_1 r_2 \cdots r_k$ for some irreducibles q_i and r_j: then $q_1 q_2 \cdots q_d r_1 r_2 \cdots r_k = ab$.
- But since the factorization of ab into irreducibles is unique, we see that p must be associate to one of the q_i or one of the r_j.
- If p is associate to one of the q_i, then it necessarily divides a, and if it is associate to one of the r_i, it necessarily divides b. Thus, $p|a$ or $p|b$, as required.

Unique Factorization Domains, VIII

Like in $\mathbb{Z}$, we can also describe greatest common divisors in terms of prime factorizations:

Proposition (Divisibility in UFDs)

If a and b are nonzero elements in a unique factorization domain R, then there exist units u and v and prime elements $p_1, p_2, \dots, p_k$ no two of which are associate so that $a = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = vp_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ for some nonnegative integers a_i and b_i. Furthermore, a divides b if and only if $a_i \le b_i$ for all $1 \le i \le k$, and the element $d = p_1^{\min(a_1,b_1)} \cdots p_k^{\min(a_k,b_k)}$ is a greatest common divisor of a and b.

This is, up to mild wrangling with units, exactly the same statement as the standard formula for the gcd in terms of prime factorizations in $\mathbb{Z}$. The proof is just bookkeeping.

Unique Factorization Domains, IX

Proof:

- Since R is a UFD, we can write a as a product of irreducibles. As follows from a trivial induction, we can then "collapse" these factorizations by grouping together associates and factoring out the resulting units to obtain a factorization of the form $a = up_1^{a_1} p_2^{a_2} \cdots p_d^{a_d}$.
- We can repeat the process with b, and then add any further irreducibles that appear in its factorization to the end of the list, to obtain the desired factorizations $a = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = vp_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ for nonnegative integers a_i and b_i.

Unique Factorization Domains, X

Proof (continued):

- So we have $a = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = vp_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$.
- If $a|b$ then we have $b = ar$ for some $r \in R$, so that $vp_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} r$.
- But since p_i divides the right-hand side at least a_i times, by cancellation we see that p_i must also divide the left-hand side at least a_i times.
- Furthermore, since each of the terms excluding p_i is not associate to p_i, by a trivial induction we conclude that $b_i \geq a_i$ for each i.
- Conversely, if $a_i \leq b_i$ for each i, then we can just write $r = vu^{-1} p_1^{b_1 - a_1} \cdots p_k^{b_k - a_k}$ and then $b = ar$.

Unique Factorization Domains, XI

Proof (finally):

- So we have $a = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = vp_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$.
- Finally, to compute the gcd, it is easy to see by the previous result that $d = p_1^{\min(a_1,b_1)} \cdots p_k^{\min(a_k,b_k)}$ divides both a and b.
- If d' is any other common divisor, then since d' divides a we see that any irreducible occurring in the prime factorization of d' must be associate to those appearing in the prime factorization of a, hence (by collapsing the factorization as above) we can write $d' = wp_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ for some nonnegative integers d_i and some unit w.
- Then since d' is a common divisor of both a and b we see that $d_i \leq a_i$ and $d_i \leq b_i$, whence $d_i \leq \min(a_i, b_i)$ for each i: then d' divides d, so d is a greatest common divisor as claimed.

Unique Factorization Domains, XII

We also recover one of the other fundamental properties of relatively prime elements and gcds:

Corollary (Relatively Prime Elements and GCDs)

In any unique factorization domain, d is a gcd of a and b if and only if a/d and b/d are relatively prime. Furthermore, if a and b are relatively prime and $a|bc$, then $a|c$.

Example:

- Inside $\mathbb{Z}[i]$, $1+i$ is a gcd of $3+i$ and $4+6i$, because $1+i$ is a common divisor, and the two elements $(3+i)/(1+i) = 2-i$ and $(4+6i)/(1+i) = 5+i$ are relatively prime because $5+i-(2+i)(2-i) = i$ is a unit.

Unique Factorization Domains, XIII

Proof:

- Apply the previous proposition to write $a = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = vp_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ for some nonnegative integers a_i and b_i, irreducibles p_i, and units u and v.
- Then $d = p_1^{\min(a_1,b_1)} \cdots p_k^{\min(a_k,b_k)}$ is a gcd of a and b, and it is easy to see that the exponent of p_i in a/d or b/d is zero for each i: thus, the only common divisors of a/d and b/d are units, so a/d and b/d are relatively prime.
- Inversely, if $d' = wp_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ is any other common divisor of a and b, and $d_i < \min(a_i, b_i)$ for some i, then p_i is a common divisor of a/d' and b/d' and thus the latter are not relatively prime.
- For the second statement, consider the irreducible factors of bc: since a and b have no irreducible factors in common, every irreducible factor of c must divide a.

Roadmap

We've now developed enough of the general theory of various kinds of rings to be able to dig back into number-theoretic questions about the quadratic integer rings in a more serious way.

- We will get more into this topic next time.
- But our goal for the rest of the chapter is to work out a lot of very explicit things about the quadratic integer rings: the structure of their maximal and prime ideals, the relationship between ideals and factorizations, when these rings have non-unique factorizations, etc.

Summary

We introduced principal ideal domains and established some of their properties.

We introduced unique factorization domains and established some of their properties.

Next lecture: The Chinese Remainder Theorem for rings, factorization in quadratic integer rings.