Math 214 Fall 2022 Number Theory I

Unique Factorization into Primes

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

9-26-2022

Outline

A helpful Lemma

(All numbers below are integers unless otherwise stated).

Lemma: A prime number p divides either a or b if it divides ab.

This lemma can also be extended to any size product.

Actually if a number behaves like this , it has to be prime! For example, if we have a composite number mn with m, n both not equal to -1 or 1 then it will divide mn but it won't divide m or n ! This property can be generalized to rings other than the integers.
In fact, our usual understanding of primes as divisible only by itself or 1 is the definition of *irreducible.*
In any integral domain, prime elements (according to property in lemma) are also irreducible.
In unique factorization domain, irreducibles are also prime.

Proof of lemma

In $\mathbb{Z}$ **:** It uses the algebraic definition of GCD!

If p divides ab and doesn't divide a then
$gcd(p, a) = 1 \implies 1 = px + ay$ for some integers x, y.
Now $b = pbx + aby$ says p divides b !

In any PID R: (First proof): The ideal generated by p and a, namely $(p, a) = \{px + ay, x, y \in R\}$ actually equals a principal ideal $(d), d \in R$ because R is a PID. Key is that $(p, a) = d \implies p \in (d), a \in (d)$. Therefore $d|p, d|a$. This means d has to be a unit because otherwise it has to be p (because p is irreducible, its only factors are units or itself), and it cannot be p because p doesn't divide a. Now, $(p, a) = (d) \implies d = px + ay$ for some $x, y \in R$. Multiplying all by b we get $bd = pbx + aby \implies p|b$. ($d$ is a unit, so it can be "cancelled out").

Proof of lemma – continued

The second, more commonly seen proof, is just one line: Since R is a PID, the ideal (p) is maximal because p is irreducible but then (p) also prime because a maximal ideal in a commutative ring with 1 is also a prime ideal. The key here is that the ideal is maximal. In fact, in a PID an ideal (π) is maximal iff π is irreducible.

Notice how it doesn't use $px + ay$ argument at all. Of course, it is all about the ideals, so not totally different.

Unique factorization into primes in $\mathbb{Z}$

Unique Factorization Theorem in $\mathbb{Z}$:

Every integer can factored, upto multiplication by ± 1 and upto re-ordering, uniquely as a product of primes.

Many rings, or even sets, have factorization into irreducible (or prime) elements but not always unique.
The Gaussian Integers $\mathbb{Z}[i]$ has unique factorization but in the ring $\mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \times 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.
In the textbook it is shown how one could create factorization among even integers into "primes" but it won't be unique.
For example, $72 = 18 \times 2 \times 2 = 12 \times 6$ and $18, 2, 12, 6$ are all primes according to the definition given there (basically 2 times an odd number).

Unique factorization into primes in any PID

Unique Factorization Theorem in any PID :

R is a PID then all $r \in R$ can factored, upto multiplication by units and upto re-ordering, uniquely as a product of irreducibles.

NOTE: As in lemma earlier, irreducibles and primes are the same in ED or PID. Using lemma, easy to prove uniqueness once you have a factorization into irreducibles,

First though you need to show that all elements can be factored into irreducibles. The key is the so called Ascending Chain Condition (ACC): Every chain of ideals the form $I_1 \subseteq I_2 \subseteq I_3 \subseteq .... \subseteq I_n \subseteq ...$ terminates. To show factorization using this construct a chain of ideals of the form $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq ....$ as follows: If r is irreducible then $r = a_1 b_1$ with a_1, b_1 non-units, and if neither a_1 nor b_1 is irreducible then $a_1 = a_2 b_2$ and so on.

Some facts about rings

Proofs can be found in any Algebra text.

1. Euclidean domain (ED) is also a principal ideal domain (PID) and a PID is a unique factorization domain (UFD). Will prove that ED is UFD.
2. $\mathbb{Z}, \mathbb{Z}[i]$, and the polynomial ring $F[x]$ for any field F are examples of ED.
3. $R[x]$ is ED iff R is a field (use the fact that (x) is a maximal ideal).
4. UFD need not be ED: $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID (and thus UFD) but it's not ED.
5. In ED, irreducible elements are prime (recall that converse is true in any integral domain). Use the lemma (as established for a general ED). You only need the expression of gcd as a linear combination.

More facts about rings

Proofs can be found in any Algebra text.

1. Factorization into irreducibles (although not uniqueness, in general) is possible in a more general setting called **Noetherian rings** (not all of which need to be PID or ED) : Rings whose ideals are all finitely generated.
2. The condition of being Noetherian is equivalent to satisfying ACC.
3. If R is Noetherian, so is $R[x]$.
4. $\mathbb{Z}[x]$ is a UFD although not a PID ($(2, x)$ is not principal).