Math 1560 - Notes 1

Ian Benway

1 February 2022

1 Unique Factorization

1.1 Notation

We write "a divides b" as $a|b$, and likewise "a does not divide b" as $a \nmid b$.

1.2 Order

A positive integer $p \geq 2$ is said to be **prime** if its only divisors are 1 and p. (Note that negative integers can also be prime.)

For nonzero $n \in \mathbb{Z}$ and a prime p, there is a nonnegative integer a such that $p^a|n$ but $p^{a+1} \nmid n$. This is called the **order** of n at p (written as $ord_p n$). For the edge case $n = 0$, set $ord_p 0 = \infty$. Then, $ord_p n = 0 \Leftrightarrow p \nmid n$.

1.3 Warmup Lemma (Weak Factorization)

Lemma 1. *Every nonzero integer can be written as a product of primes (except for -1).*

Proof. Suppose this isn't true. Let N be the smallest integer ≥ 2 that can't be written as a product of primes. We have that N is not prime, so then we must have some a and b such that $N = ab$. Well, since N is the smallest integer that can't be written as a product of primes, both a and b must have prime factors. Say $a = wx$ and $b = yz$ for some prime w, x, y, z. Then $N = ab = wxyz$. Contradiction! □

This let's us write

$$n = (-1)^{\varepsilon} \cdot \prod_{\substack{p \\ \text{positive prime}}} p^{a(p)}$$

where $\varepsilon = 0$ or 1 and $a(p)$ is a nonnegative integer.

1.4 Unique Factorization Theorem

Theorem 1. *For every nonzero integer n, there is a prime factorization*

$$n = (-1)^{\varepsilon} \cdot \prod_{\substack{p \\ \text{positive prime}}} p^{a(p)}$$

where $\varepsilon, a(p)$ are uniquely determined. Moreover, $a(p) = ord_p n$.

Note that now we just have to prove uniqueness. We will need a little Abstract Algebra...

Review of Abstract Algebra (Math 1530)

Recall:

Lemma 2. *If $a, b \in \mathbb{Z}$ and $b > 0$, then there exist $q, r \in \mathbb{Z}$ such that*

$$a = bq + r$$

with $0 \leq r < b$. (Think q is the quotient and r is the remainder.)

Proof. Consider the set $S = \{a - xb \mid x \in Z\}$.
Note that S contains positive elements. Let $r = a - qb$ be the least nonnegative element of S. We need to show that $0 \leq r < b$.
Well, suppose it's not, so $r \geq b$. Then $r = a - qb \geq b$, which gives $a - (q+1)b \geq 0$. But, $0 \leq a - (q+1)b < a - qb$. This contradicts that $r = a - qb$ is the least nonnegative element of S! □

Corollary 1. *$\mathbb{Z}$ is a Euclidean domain, with a Euclidean function given by $\lambda x = |x|$.*

Let R be an integral domain. R is said to be a **Euclidean domain** if there exists a function $\lambda : R \setminus \{0\} \to \mathbb{N}$ such that if $a, b \in R$, $b \neq 0$, then there exist $c, d \in R$ such that $a = cb + d$, with $d = 0$ or $\lambda(d) < \lambda(b)$.
Examples:

- Z is a Euclidean domain with $\lambda =$ the absolute value
- k[x], where k is a field, with $\lambda = deg$
- Z[i], with $\lambda(a + bi) = a^2 + b^2$

Proposition 1. *If R is a Euclidean domain, then R is a principal ideal domain (PID). (i.e. if $I \subseteq R$ is an ideal, then $a \in R$ implies $I = Ra = \{ra \mid r \in R\}$)*

Proof. Assume without loss of generality that $I \neq (0)$. Let $0 \neq a \in I$ be such that $\lambda(a) \leq \lambda(b)$ for all $b \in I, b \neq 0$. We need to show that $I = (a) = Ra$. Well, $Ra \subseteq I$ since I is an ideal. Let $b \in I$. Then for all $c, d \in R$ such that $b = ca + d$, where $d = 0$ or $\lambda(d) < \lambda(a)$. Now we have that $d = b - ca \in I$, so we can't have $\lambda(d) < \lambda(a)$. Thus $d = 0$, so $b = ca \in Ra$. Hence $I \subseteq Ra$. □

If $I = (a)$ for some $a \in I$, I is said to be a principal ideal. R is a principal ideal domain if every ideal of R is principal.

Important Things about PIDs

- Nonunit irreducible elements are exactly the prime elements. (Recall: $p \in R$ is **irreducible** if
  - $a|p \Rightarrow a$ is either a unit or an associate of p.
  - $p \in R$ is **prime** if $p|ab \Rightarrow p|a$ or $a|b$ and p is a nonzero nonunit of R.)
- GCDs always exist in PIDs.

Lemma 3. *Suppose p is a prime and $a, b \in \mathbb{Z}$. Then $ord_p(ab) = ord_p a + ord_p b$.*

Proof. WLOG, assume $a, b \neq 0$. Let $\alpha = ord_p a$ and $\beta = ord_p b$. Then $a = p^\alpha \cdot c$ where $p \nmid c$, and $b = p^\beta \cdot d$ where $p \nmid d$. Thus, $ab = p^{\alpha+\beta} \cdot cd$. We have that $p \nmid cd$, since $p \nmid c$ and $p \nmid d$. (Note that irreducible elements are prime.) Hence, $ord_p ab = \alpha + \beta$. □

We now have the tools to prove unique factorization.

Proof of Unique Factorization. Recall that for a nonzero $n \in \mathbb{Z}$, we can write

$$n = (-1)^\varepsilon \cdot \prod_{\substack{p \\ \text{positive prime}}} p^{a(p)}$$

where $\varepsilon = 0$ or 1 and $a(p) \geq 0$. Given a positive prime q, we can take ord_q of both sides. By the previous lemma, this yields

$$ord_q n = \varepsilon ord_q(-1) + \sum_p a(p) ord_q(p). \tag{1}$$

We have $ord_q(-1) = 0$ and $ord_q(p) = 0$ for all $p \neq q$ (coprimality). Thus (1) tells us that $ord_q n = a(q)$. In other words, $a(q)$ is uniquely determined for all primes q. □

2 Greatest Common Divisors

Let R be an integral domain. Then $d \in R$ is said to be a GCD of two elements $a, b \in R$ if

1. $d|a$ and $d|b$
2. $d'|a$ and $d'|b \Rightarrow d'|d$.

Aside: GCD domains are a class of rings more general the UFDs or PIDs.

We will denote GCDs as (a, b) being the GCD of a and b.
Caution: GCDs are only unique up to units; e.g. -5 and 5 are both $(-5, 10)$. By convention, we say that GCDs are always positive, so $(-5, 10) = 5$.