

# MATH 603 Notes

David Zhu

March 13, 2024

## 1 More on Commutative Rings

Let  $a, b \in R$ . Then  $a|b \iff \exists a' \in R, b = aa'$ ; A semi ring on  $R, \leq$  defined by  $a \leq b \iff a|b$ . Note that  $\leq$  is usually not an ordering: let  $b \in R^\times$ , then  $a \leq ab \leq a$ , but  $a \neq ab$ .

**Proposition 1.1.**  $a \equiv b$  iff  $a \leq b$  and  $b \leq a$  iff  $(a) = (b)$  is an equivalence relation.

For  $R$  a domain, the induced relation gives a well-defined definition of greatest common divisor.

**Definition 1.1.** The gcd of  $a, b$ , denoted by  $\gcd(a, b)$ , if exists, is any  $d \in R$  such that  $d|a, b$  and for any other  $d'$  satisfying the condition,  $d'|d$ .

**Definition 1.2.** The lcm of  $a, b$ , denoted by  $\text{lcm}(a, b)$ , if exists, is any  $d \in R$  such that  $a, b|d$  and for any other  $d'$  satisfying the condition,  $d'|d$ .

Note that either may not exist, for example take  $R = \mathbb{Z}[\sqrt{6}]$ , then  $\gcd(2, \sqrt{6})$  does not exist.

**Proposition 1.2.** If  $\gcd(a, b)$  exists, then  $\gcd(a, b) = \sup\{d : d \leq a, b\}$ .

The dual notion for lcm also holds. Note that maximal/minimal elements always exist by Zorn's lemma. However, the unique supremum/infimum may not exist.

**Proposition 1.3.** Let  $a, b \in R$  be given. Then the following hold:  $\gcd(a, b) = d$  exists iff  $(d)$  is the unique maximal principal ideal such that  $(a) + (b) \subset (d)$ . Dually,  $\text{lcm}(a, b) = c$  exists iff  $(c) = (a) \cap (b)$ . If both hold, then  $a \cdot b = \text{lcm}(a, b) \cdot \gcd(a, b)$ .

*Proof.* Easy exercise for gcd. Note that the inclusion can be proper, for example, take  $R = k[x, y]$  and ideals  $(x), (y)$ . Then  $(1)$  is the gcd, but the containment is proper.  $\square$

Recall that  $\text{Id}(R)$  is partially ordered by inclusion.

**Definition 1.3.**  $\text{Id}(R), +, \cap, \cdot, \leq$  is the lattice of ideals of  $R$ .

Note that  $+, \cap$  are simply the sums and intersection, but  $\cdot$  is the ideal generated by the products.

**Theorem 1.1.** TFAE for non-finitely generated ideals of  $R$ , which we denote  $\text{Id}^\infty(R)$ : 1.  $\text{Id}^\infty(R)$  is non-empty; 2. there exists infinite non-stationary chains  $(\sigma_i)$ , where  $\sigma_i \in \text{Id}(R)$ ;

*Proof.* Easy exercise.  $\square$

**Theorem 1.2.** Cohen's lemma: Let  $\text{Id}^\infty(R) \neq \emptyset$ . Then, it has a maximal element and any such maximal element is prime.

*Proof.* Zorn's lemma implies  $Id^\infty(R)$  has maximal elements. Let  $a$  be maximal, and  $xy \in a$ . Suppose by contradiction that  $x, y \notin a$ , then  $I_1 = a \subset (x) + a$  and  $I_2 = a \subset (y) + a$ , which contradicts maximality by proving one of them must be infinitely generated. Consider  $(a : x) = \{\gamma \in R : \gamma \cdot x \in a\}$ . Note  $a, y \in (a : x)$ , and  $x \cdot (a : x) \subseteq a$ . Hence  $(a : x) \notin Id^\infty(R)$  and  $(a : x)$  is finitely generated. Thus,  $a = I_0 + (a : x)$  must be finitely generated.  $\square$

## 2 Euclidean Rings

**Definition 2.1.** A Principal Ideal Ring is any ring  $R$  such that  $Id(R) = Id^p(R)$ . If  $R$  is a domain, then  $R$  is called a PID.

**Definition 2.2.** A Factorial Ring is any ring  $R$  in which all units can be written as a finite product of irreducible elements. If  $R$  is domain, then it is called a UFD. (Note that if it is not a domain, weird things can happen)

**Definition 2.3.** A Noetherian Ring is any ring  $R$  such that any ideal is finitely generated.

**Definition 2.4.** Let  $R$  be a domain. A Euclidean norm on  $R$  is any map  $\phi : R \rightarrow \mathbb{N}$  satisfying  $\phi(x) = 0$  iff  $x = 0$  and for every  $a, b \in R$  with  $b \neq 0$ , then there exists  $q, r \in R$  such that  $a = bq + r$  with  $\phi(r) < \phi(b)$ . A Euclidean domain is any domain equipped with a Euclidean norm.

Example of Euclidean domains include  $\mathbb{Z}, \mathbb{Z}[i]$ . A non-trivial example  $R = F[t]$ , with  $\phi(p(t)) = 2^{\deg(p(t))}$ . A non-example is  $\mathbb{Z}[\sqrt{6}]$  for it is not a PID.

**Theorem 2.1.** Euclidean Domains are PIDs; The Euclidean Algorithm:  $a, b \in R, b \neq 0$  and set  $r_0 = a, r_1 = b$ , and continue inductively  $r_{i-1} = r_i \cdot q_i + r_{i+1}$ . Then,  $r_i = 0$  for  $i > \phi(b)$  and if  $r_{i_0} \geq 1$  maximal with  $r_{i_0} \neq 0$ , then  $r_{i_0} = \gcd(a, b)$ .

*Proof.* Easy exercise.  $\square$

## 3 Principal Ideal Domains

**Theorem 3.1.** (Charaterization) For A domain  $R$  TFAE: 1.  $R$  is a PID; 2. every  $a \in R^\times, a \neq 0$  is a product of finitely many prime elements up unique up to permutation. 3. every  $p \in \text{Spec}(R)$  is principal.

*Proof.* Let  $a \in R$  such that  $a$  is non-zero and not a unit. Then, there exists  $p \in \text{Spec}(R)$  such that  $(a) \subseteq p$ . Hence  $R$  being a PID implies  $\exists \pi \in R$  such that  $p = (\pi)$ . Hence,  $\pi$  must be prime and  $\pi | a$ . Set  $a_1 = a$ ,  $\pi_1 = \pi$ , and let  $a_2$  be the element such that  $\pi_1 a_2 = a_1$ . Continue inductively such that if  $a_n$  is a unit, stop; otherwise repeat. Suppose by contradiction that the process does not stablize.

Assuming that every prime is principal, Cohen's Lemma implies  $Id^\infty(R) \neq \emptyset$ ; therefore, every ideal is finitely generated. We therefore can choose a minimal prime over a given finitely generated ideal and build a chain of ideals whose union is prime and contradiction.  $\square$

**Corollary 3.1.1.** Let  $R$  be a PID; let  $P \subset R$  be a set of representatives for the prime elements up to association. For every  $a \in R, \exists \epsilon \in R^\times$  and  $e_\pi \in \mathbb{N}$  such that almost all  $e_\pi = 0$ . Then, every  $a \in R$  can be written as  $a = \epsilon \prod_{\pi \in P} \pi^{e_\pi}$ . We proceed to recover gcd and lcm, up to associates.

Note that the above corollary generalizes to the quotient field by replacing  $\mathbb{N}$  with  $\mathbb{Z}$ .

## 4 Unique Factorization Domains

**Definition 4.1.** A Unique Factorization Domain is a domain in which every non-zero, non-units is a product of prime elements.

**Proposition 4.1.** TFAE: (1.)  $R$  is a UFD; (2). every minimal prime ideal is principal and every non-zero, non-invertible elements in contained in finitely many primes.

*Proof.* Exercise. □

Remark: we recover the  $\gcd$  and  $\text{lcm}$  definition using the same factorization as Corollary 3.1.1.

**Theorem 4.1.** (Gauss Lemma) Let  $R$  be a UFD; then  $R[t]$  is a UFD.

*Proof.* Let  $f(t) = a_0 + \dots + a_n t^n$  be given. Then, the content of  $f$ , denoted  $C(f)$ , is the GCD of all coefficients. In particular,  $C(f) | a_i$  for all  $i$ , and  $f_0 := f/(C(f))$  has content 1.

**Lemma 4.2.** Let  $R$  be a UFD, then the following hold: (1).  $C(f) : R[t] \rightarrow R$  given by  $f \mapsto C(f)$  is multiplicative; in particular, if  $C(f) = C(g) = 1$ , then  $C(fg) = 1$ .

proof of the lemma: given  $f(t) = a_0 + \dots + a_n t^n$  and  $g(t) = b_0 + \dots + b_m t^m$ . If one of  $f, g$  is constant, then it is easy exercise; suppose neither is constant, then set  $f = f_0 \cdot C(f)$  and  $g = g_0 \cdot C(g)$ . Clearly we have  $C(f) \cdot C(g) | C(fg)$ . Hence it suffices to prove that  $C(f_0 g_0) = 1$ . Equivalently, let  $\pi \in R$  be a prime element, then there exists a coefficient  $c_k \in f_0 g_0$  such that  $\pi$  does not divide  $c_k$ . Suppose  $\pi | C_k = \sum_{i+j=k} a_i b_j$  for all  $k$ . Then,  $\pi | a_0 b_0$  and WLOG,  $\pi | a_0$ . Because  $C(f_0) = C(g_0) = 1$ , then there exists minimal  $a_i, b_j$  such that  $\pi$  does not divide  $a_{i_0}, b_{j_0}$ . Then,  $\pi$  does not divide  $C_{i_0+j_0}$ . □

The proof goes similarly for quotient fields.

**Theorem 4.3.** For  $f(t) \in R[t]$ , TFAE 1.  $f(t)$  is prime 2.  $f$  is irreducible 3. If  $f = a_0 \in R$  and  $a_0$  is prime or  $C(f) = 1$  and  $f$  is irreducible.