

Week 4

Classes of Rings

4.1 Euclidean Domains and Reducibility

1/23:

- Notes to wrap up last time to start.
- Recall the theorem from last time: There is an injective ring homomorphism $\iota : R \rightarrow D^{-1}R$ such that for any $\varphi : R \rightarrow S$ such that $\varphi(D) \subset S^\times$, there exists a unique $\tilde{\varphi} : D^{-1}R \rightarrow S$ such that $\tilde{\varphi} \circ \iota = \varphi$.
 - Callum redraws Figure 3.1.
- Something Callum misstated last time: Diadic refers to 2-adic, not p -adic.
- Corollary: If $f \in R$ is not a zero divisor, then $R_f \cong R[X]/(fX - 1)$.
 - We can prove this using the universal property; it's on the HW.
- **Subfield of F generated by R :** The field defined as follows, where F is a field and $R \subset F$ is an integral domain. Denoted by K . Given by

$$K = \bigcap_{\substack{R \subset F' \subset F \\ F' \text{ a field}}} F'$$

- Alternative definition: The smallest field inside F that contains R .
- Proposition: Let $R \subset F$ be an integral domain, where F is a field. Then

$$K \cong \text{Frac } R$$

Proof. Background: Consider the injection $R \rightarrow F$. It sends every element of $D = R \setminus \{0\}$ to a unit in F . Moreover, this function “factors through the fraction field” via Figure 3.1 as per the theorem. We now begin the argument in earnest.

To prove that $K \cong \text{Frac } R$, we will use a bidirectional inclusion proof. For the forward direction, observe that $R \subset \text{Frac } R \subset F$. Therefore, by the definition of K , $K \subset \text{Frac } R$, as desired. For the backward direction, let $x/y \in \text{Frac } R$ be arbitrary. To confirm that $x/y \in K$, it will suffice to verify that $x/y \in F'$ for all $R \subset F' \subset F$. Let F' subject to said constraint be arbitrary. Since $x/y \in \text{Frac } R$, $x, y \in R$. It follows since $R \subset F'$ that $x, y \in F'$. Thus, since F' is a field and hence closed under multiplicative inverses, $1/y \in F'$. Finally, since F' is closed under multiplication and $x, 1/y \in F'$, we have that $x/y \in F'$, as desired. \square

- Example: Let $R = \mathbb{Z}[\sqrt{2}] = \mathbb{Z}[X]/(X^2 - 2)$. Then

$$\text{Frac } R = \mathbb{Q}[\sqrt{2}] = \frac{\mathbb{Q}[X]}{(X^2 - 2)}$$

- That's it for rings of fractions. We now move onto Euclidean Domains (EDs), Principal Ideal Domains (PIDs), and Unique Factorization Domains (UFDs).
- An ED is a PID, and a PID is a UFD (hence, for example, an ED is both a PID and a UFD).
- **Norm:** A function from an integral domain R to $\mathbb{Z}_{\geq 0}$ that satisfies the following. *Denoted by N .*
Constraints
 - (i) Let $a \in R$. Then $N(a) = 0$ iff $a = 0$.
 - (ii) $h, f \in R$ and $f \neq 0$ implies that there exists $q, r \in R$ such that $h = qf + r$ and $N(r) < N(f)$.
- **Euclidean domain:** An integral domain on which there exists a norm. *Also known as **ED**.*
- **Theorem:** If R is an ED, then R is a PID.

Proof. This proof will use an analogous argument to that used in the proof that $F[X]$ is a PID from the end Lecture 3.1. Let's begin.

To prove that R is a PID, it will suffice show that for every ideal $I \subset R$, $I = (f)$ for some $f \in I$. Let $I \subset R$ be arbitrary. Let

$$d = \min\{N(a) \mid a \in I \setminus \{0\}\}$$

Pick $f \in I \setminus \{0\}$ such that $N(f) = d$. We will now argue that $I = (f)$ via a bidirectional inclusion proof. In one direction, since I is an ideal, $(f) = Rf \subset I$. In the other direction, let $h \in I$ be arbitrary. Then since $f \neq 0$ by assumption, the hypothesis that R is an ED implies that there exist $q, r \in R$ such that $h = qf + r$ and $N(r) < N(f)$. It follows since $h, qf \in I$ that $r = h - qf \in I$. But since $N(r) < N(f) = d$, $r \in I$ implies by the definition of d that necessarily $N(r) = 0$ and hence $r = 0$. Therefore, $h = qf$, as desired. \square

- Note that showing that $r \in I$ this way would not be acceptable in the HW??
- Examples of EDs:
 1. \mathbb{Z} , $N(m) = |m|$.
 - The norm is non-unique.
 2. $F[X]^{[1]}$, $N(f) = 2^{\deg(f)}$.
 - We define the norm in this way because then the degree of the zero polynomial being $-\infty$ makes $N(0) = 2^{-\infty} = 0$.
 - Note that since $\deg(fg) = \deg(f) + \deg(g)$, $N(fg) = N(f)N(g)$ here.
 3. $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ (d is a **square-free integer**), $N(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - b^2d|$ for $a, b \in \mathbb{Q}$.
 - Most famous example: $\mathbb{Z}[\sqrt{-1}]$, which are the **Gaussian integers**.
 - Also interesting are $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] \cong \mathbb{Z}[X]/(X^2 + X + 1)$.
 - In the last example, the complex number in brackets is a cube root of unity equal to $\cos(120) + i\sin(120)$.
 - The reason why we define the norm on $\{a + b\sqrt{d}\}$ for $a, b \in \mathbb{Q}$ instead of $a, b \in \mathbb{Z}$.
 - The number θ in $\mathbb{Z}[\theta]$ may not always be a radical or imaginary; it can be complex, too, as in the case of $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$.
 - Let $\theta = \frac{-1+\sqrt{-3}}{2}$. In this case, we have

$$\left\{ \alpha + \beta \frac{-1 + \sqrt{-3}}{2} \mid \alpha, \beta \in \mathbb{Z} \right\} \cong \left\{ a + b\sqrt{-3} \mid a, b \in \mathbb{Q}, a = \alpha - \frac{1}{2}\beta, b = \frac{1}{2}\beta, \alpha, \beta \in \mathbb{Z} \right\}$$

¹Henceforth, " F " is assumed to denote a field.

- **Square-free integer:** An integer that is not divisible by the square of any integer.
- **Gaussian integers:** The Euclidean domain $\mathbb{Z}[\sqrt{-1}]$.
- **Unit:** An element $u \in R$ for which there exists $v \in R$ such that $uv = vu = 1$.
- R^\times : The set of all units of R .
 - (R^\times, \times) is a group.
- Examples:
 1. $F^\times = F \setminus \{0\}$.
 2. $F[X]^\times = F^\times$, i.e., is the nonzero constant polynomials.
 - This is because any higher degree polynomial cannot be taken back down in degree — multiplying polynomials adds degrees.
 3. $\mathbb{Z}^\times = \{\pm 1\}$.
 4. $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm i\}$.
 5. $R[X]^\times = R^\times$ (R an integral domain).
 6. Suppose R is not an integral domain. Then we get things like $a \neq 0 \in R$ and $a^2 = 0$ (i.e., a is a zero divisor) implies that $(1 - aX)(1 + aX) = 1 - a^2X^2 = 1$.
 - We forbid this! It's nasty. Thus, we assume that rings of polynomials are taken over integral domains.
- **Reducible (element):** A nonzero element $a \in R$ such that $a = bc$ and $b, c \notin R^\times$, where R is an integral domain.
 - Alternative definition: An element that is the product of two things, neither of which is a unit.
- $R \setminus \{0\}$ is a disjoint union of...
 - (i) Units;
 - (ii) Reducible elements;
 - (iii) And irreducible elements.

Proof. Suppose for the sake of contradiction that $a \in R \setminus \{0\}$ is both reducible and a unit. Since a is reducible, $a = bc$ where $b, c \notin R^\times$. Since a is a unit, we may define $d = a^{-1}$. Then

$$1 = ad = bcd = b(cd)$$

so $b \in R^\times$, a contradiction. □

- Reducibility/irreducibility changes based on context.
- Example:
 - Consider $F[[X]]$, where X is taken to be irreducible.
 - Here, all elements are of the form uX^n for some $u \in F$ and $n \in \mathbb{Z}_{\geq 0}$.
 - However, if we define $X = (X^{1/2})^2$, then $F[[X]] \subset F[[X^{1/2}]]$. In this larger context, X is now reducible.
 - We can continue the chain via

$$\bigcup_{n=1}^{\infty} F[[X^{\frac{1}{2^n}}]]$$

- **Factorization** (of $a \in R$): A product of certain elements of R that is equal to a , where R is a ring; in particular, the product must consist of one unit u and r irreducible elements $\pi_1, \dots, \pi_r \in R$. Given by

$$a = u\pi_1\pi_2 \cdots \pi_r$$

- **Unique factorization domain**: A ring R such that for every nonzero element $a \in R$, any two factorizations

$$a = u\pi_1\pi_2 \cdots \pi_r$$

$$a = u'\pi'_1\pi'_2 \cdots \pi'_s$$

of a satisfy the following conditions.

- (i) $r = s$.
- (ii) There exists $\sigma \in S_r$ such that $\pi'_i = \pi_{\sigma(i)}u_i$ for all $1 \leq i \leq r$, u_i being a unit.

Also known as **UFD**.

- Wednesday: Show that a PID is a UFD.

4.2 Unique Factorization Domains

1/25:

- Goal: UFDs.
- We review some definitions from last time to start.
- **Prime** (ideal): An ideal P in a commutative ring R for which R/P is an integral domain.
 - Equivalently, $1 \notin P$ and $a, b \notin P$ imply $ab \notin P$, i.e., $R \setminus P$ is a multiplicative set.
- Observation: Maximal ideals are prime ideals.
- From now on, R denotes an integral domain.
- **Factorization** (of a nonzero element): A product $a = u\pi_1\pi_2 \cdots \pi_r$, where $u \in R^\times$, each π_i is irreducible, and $r = 0$ is allowed.
- **Irreducible** (element): An element...
 - Think of them a bit like primes, though this is very dangerous.
- **Equivalent** (factorizations): Two factorizations $a = u\pi_1\pi_2 \cdots \pi_r$ and $a = u'\pi'_1\pi'_2 \cdots \pi'_s$ for which $r = s$ and there exists $\sigma \in S_r$ and $u_1, \dots, u_r \in R^\times$ such that $\pi'_i = u_i\pi_{\sigma(i)}$ ($i = 1, \dots, r$) where $u\pi_1$ is also irreducible.
- **Unique factorization domain**: An integral domain R for which every nonzero a has a factorization and any factorizations of a are equivalent to each other.
- **Prime** (element): A nonzero $\pi \in R$ for which (π) is a prime ideal.
- Exercise: Prove that if π is prime, then π is irreducible.
 - Note that π irreducible does *not* imply that π is prime in general.
- Lemma*: If every irreducible element of R is prime, then any two factorizations of any nonzero $a \in R$ are equivalent.

Proof. We induct on the length $r \geq 0$ of factorizations.

For the base case $r = 0$, let $a \in R$ be arbitrary. Factor it into

$$a = u \prod_{i=1}^r \pi_i = u \prod_{i=1}^0 \pi_i = u$$

It follows that a is a unit. Therefore, there exists $b \in R$ such that $ab = 1$. Now suppose for the sake of contradiction that we also have

$$a = u' \pi'_1 \cdots \pi'_s$$

It follows that

$$1 = (u' \pi'_1 \cdots \pi'_s) b = \pi'_1 (u' \pi'_2 \cdots \pi'_s b)$$

Thus, π'_1 is a unit, contradicting the hypothesis that π'_1 is irreducible. Therefore, $s = 0$ and $u' = u$, as desired.

Now suppose inductively that we have proven the claim for $r - 1$; we now wish to prove it for r . Let

$$a = u \pi_1 \cdots \pi_r \qquad a = u' \pi'_1 \cdots \pi'_s$$

be two factorizations of an arbitrary $a \in R$. By the definition of a factorization, π_1 is irreducible. Thus, by hypothesis, π_1 is prime and hence (π_1) is a prime ideal. Additionally, we have that

$$a = u \pi_1 \cdots \pi_r = (u \pi_2 \cdots \pi_r) \pi_1 \in R \pi_1 = (\pi_1)$$

Thus, we must have $u' \pi'_1 \cdots \pi'_s \in (\pi_1)$ as well. It follows that one of the elements in the product $u' \pi'_1 \cdots \pi'_s$ is equal to $\pi_1 b$ for some $b \in R$. Suppose for the sake of contradiction that this element is u' . Then $u' = \pi_1 b$. But since u' is a unit, there exists $c \in R$ such that $1 = u' c$. It follows via substitution that

$$1 = u' c = \pi_1 b c = \pi_1 (bc)$$

i.e., that π_1 is a unit, contradicting the hypothesis that it's irreducible. Therefore, $u' \notin (\pi_1)$. It follows that one of the $\pi'_i \in (\pi_1)$. WLOG, let $\pi'_1 \in (\pi_1)$. Then $\pi'_1 = u_1 \pi_1$ for some $u_1 \in R$. In particular, since π'_1 is irreducible, then either $u_1 \in R^\times$ or $\pi_1 \in R^\times$. But we can't have the second case since π_1 is irreducible (and hence not a unit) by assumption. Thus $u_1 \in R^\times$. It follows that

$$\begin{aligned} a &= a \\ u \pi_1 \cdots \pi_r &= u' \pi'_1 \cdots \pi'_s \\ u \pi_1 \cdots \pi_r &= u' u_1 \pi_1 \pi'_2 \cdots \pi'_s \\ u \pi_2 \cdots \pi_r &= u' u_1 \pi'_2 \cdots \pi'_s \end{aligned}$$

where we apply the cancellation lemma in the last step, as permitted by the facts that R is an integral domain and π_1 is irreducible (hence nonzero). Thus, by the induction hypothesis, the factorizations $u \pi_2 \cdots \pi_r$ and $u' u_1 \pi'_2 \cdots \pi'_s$ are equivalent. It follows that $r = s$ and there exists $\sigma \in S_{[2:r]}$ and units $u_2, \dots, u_r \in R^\times$ such that $\pi'_i = u_i \pi_{\sigma(i)}$ ($i = 2, \dots, r$). Extend σ to S_r by defining $\sigma(1) = 1$. Thus, taking $\sigma \in S_r$ and $u_1, \dots, u_r \in R^\times$, we know that $\pi'_i = u_i \pi_i$ ($i = 1, \dots, r$). Therefore, $u \pi_1 \cdots \pi_r$ and $u' \pi'_1 \cdots \pi'_s$ are equivalent factorizations of a , as desired. \square

- To prove that something is a UFD, it is all important to show that irreducible...??
- Notation: $a \mid b$ iff $b \in (a)$.
- **Greatest common divisor:** The number pertaining to $a, b \in R$ both nonzero which satisfies the following two constraints. Denoted by d , $\gcd(a, b)$, **g.c.d.** (a, b) . Constraints
 - (i) $d \mid a$ and $d \mid b$.
 - (ii) $d' \mid a$ and $d' \mid b$ implies $d' \mid d$.

- d is well-defined up to multiplication by $u \in R^\times$.
 - Example: We commonly think of $\gcd(6, 9) = 3$, but in \mathbb{Z} , it could also be $-3 = -1 \cdot 3$ where $-1 \in \mathbb{Z}^\times = \{\pm 1\}$.
- Essay: $d \mid a$ implies $a = bd$ and the factors of d are a subset of the factors of a . Let $a = u\pi_1 \cdots \pi_r \cdot \pi'_1 \pi'_2 \cdots \pi'_h$ and $b = u'\pi_1 \cdots \pi_r \cdot \pi''_1 \pi''_2 \cdots \pi''_g$. For all $i \leq h, j \leq g$: $\pi_i \nmid \pi''_j$.
 - I.e., the factors of a, b that don't multiply out to $\gcd(a, b) = d$ are all relatively prime.
- Let $d = \pi_1 \cdots \pi_r = \gcd(a, b)R$.
- Existence of factorization in a PID.
- Example: $F[X]$.
 - Recall that $F[X]$ is a PID.
 - Let $f \in F[X]$ have $\deg(f) > 0$.
 - Then since PIDs are UFDs, $f = uf_1 \cdots f_r$ where $u \in F[X]^\times = F^\times$ and each f_i is irreducible.
 - We have that $\deg f = \deg f_1 + \cdots + \deg f_r \geq r$.
 - This is the Fundamental Theorem of Algebra!
- We now attempt a rigorous proof of existence in PIDs. Without a good norm (as we have in EDs), we need this proof.
 - Suppose that $a \in R$ nonzero is not a unit.
 - Then $a = bc$ where $b, c \notin R^\times$.
 - If b, c have a factorization, then $a = bc$ has a factorization.
 - WLOG, let b have a factorization.
 - Let $a = b_1 a_2$, where $b_1 \notin R^\times$ and a_2 does not admit a factorization. Therefore, $a_2 = b_2 a_3$, where b_2 is not a unit and a_3 does not admit a factorization.
 - We can go on forever: $a_n = b_n a_{n+1}$ where $b_n \notin R^\times$ and $a_{n+1} \cdots$.
 - It follows that $(a_n) \subset (a_{n+1})$ and $b_n \notin R^\times$ implies $(a_n) \neq (a_{n+1})$.
 - All ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$. Is $\bigcup_{n=1}^\infty I_n$ an ideal? Yes, it is. Let's call it I .
 - R is a PID implies that $I = (\alpha)$.
 - There exists n such that $\alpha \in I_n$, and $(\alpha) \subset I_n \subsetneq I_{n+1} \subset \cdots \subset (\alpha)$.
 - See the proof in the book for clarification: Theorem ?? on Dummit and Foote (2004, pp. 287–89).
- Last theorem to prove.
- Theorem: R is a PID implies R is a UFD.
 - Existence, we've done.
 - Equivalence: By Lemma*, we only need irreducible $\pi \in R$ to be prime.
 - a is reducible. $a = bc$, $b \notin R^\times$ and $c \notin R^\times$ implies $(a) \subsetneq (b) \subsetneq R$.
 - Thus, a is irreducible. It follows that (a) is maximal and hence (a) is prime. All these concepts are equivalent in a PID.
- Examples: \mathbb{Z} , $F[X]$, $F[[X]]$.
- Let $a_n = b_n a_{n+1}$. Then $(a_n) \subset (a_{n+1})$. and $b_n \notin R^\times$.
- If $(a_n) = (a_{n+1})$, then $a_{n+1} = ca_n$, $a_n = b_n \subset a_n$, $1 = b_n c$.

4.3 Office Hours (Callum)

- What kind of stuff from the recent lectures do we need to use in HW3?
 - It is mostly content from before Wednesday of Week 3.
 - The Euclidean algorithm will crop up in a few places, and some more recent/advanced stuff may be needed to solve the last problem.
- Do we need to provide rationale for our answers to Q3.1?
 - Yes.
 - We can just give a general proof once in the first one.
- Is Q3.2 a rote check of the definition? Are there any other factors to worry about?
 - It is straight from the definition.
- Is Q3.3(iii) too difficult?
 - The forward inclusion $I_1 I_2 \subset I_1 \cap I_2$ always holds. The backwards one needs coprime ideals (i.e., the fact that $(m) + (n) = \mathbb{Z}$ if m, n are coprime).
- Q3.5?
 - No complications; just consecutive applications of the universal property of $R[X]$ should yield the desired result.
- Is Q3.6 discussing evaluation functions?
 - Yes, even though they're denoted ϕ there.
 - See the Corollary from Lecture 3.1 for help on this problem.
- Hint for Q3.6(ii)?
 - This is a “you either see it or you don't” problem.
 - It shouldn't take that long to do once you see it, but it could take a long time to see it.
- For Q3.7, do we just have to define an inverse ψ and check $\phi \circ \psi = \psi \circ \phi = \text{id}$, or do we need to conduct a broader set of isomorphism checks, such as bijectivity, ring homomorphism ones, etc.?
 - Cite Q3.5 for proving that the inverse is a ring homomorphism. Other than that, not really — it is mainly about focusing on the inverse condition.
- What is meant by “type” in Q3.8? Does the argument have to be a monomial of the given form, or are higher order polynomials allowed, too? Do you more broadly mean evaluation-based functions?
 - Exactly the same monomial evaluation. The only degrees of freedom are a, b .
- Is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$?
 - Yes.
 - Note: Don't use q as a dummy variable because \mathbb{F}_q is something else.
- In Q3.9(ii), how do I prove that there are always two a 's that go to a^2 ? Can I just show that $a^2 = 1^2 a^2$ or something?
 - Don't use (i) to prove (ii); just use similar reasoning.
 - I've already made the big observation by noting that its $\pm a$ that both square to the same number. Rest should be smooth sailing.

- Thoughts on Q3.10?
 - By far the hardest question.
 - Tips: Show that $X^2 - \theta^2$ is a maximal ideal in the polynomial ring. If f is irreducible, then (f) is maximal. Check that $X^2 - \theta^2$ is irreducible.
 - Like 5 problems in 1 problem. Takes a bunch of techniques. The case where the square is zero is not hard. Write down four distinct rings and then use this to prove that you can't get any other ones. Keep them all in the quotient form? One is a product of two cyclic groups; that's a product of fields. You're allowed to multiply differently when they're rings, not groups. 2 groups, but 4 rings.

4.4 Division and the Chinese Remainder Theorem

1/27:

- This whole lecture is a speech for PIDs over UFDs.
- Proposition: Let R be a PID, and let $\pi \in R$ be nonzero. Then TFAE.
 - (1) π is irreducible.
 - (2) (π) is a maximal ideal.
 - (3) π is prime.

Proof. $(2) \implies (3)$: Since (π) is a maximal ideal, $R/(\pi)$ is a field. Thus, it's an integral domain. Therefore, (π) is a prime ideal.

$(3) \implies (1)$: Holds in any integral domain.

$(1) \implies (2)$: If (π) is not maximal, then there exists an ideal I such that $(\pi) \subsetneq I \subsetneq R$. But $I = (a)$. Then $\pi = ab$. $I \neq R$ implies that $a \notin R^\times$. Additionally, $(\pi) \neq (a)$ implies $b \notin R^\times$. Therefore, π is reducible, a contradiction. \square

- Recall computing greatest common divisors from last lecture.
 - In particular, we know that $R \setminus \{0\}$ (or R^\times) is an integral domain.
 - Thus, if $a, b \in R \setminus \{0\}$, then $a \sim b$ if there exists $u \in R^\times$ such that $a = ub$.
 - Nori confirms that \sim is an equivalence relation.
 - If $a \sim b$, we say that a is an **associate** of b .
 - Notation: $\sim \setminus R - \{0\}$ implies that we're applying the equivalence relation \sim to the set $R \setminus \{0\}$.
 - $\gcd(a, b) \in \sim \setminus R - \{0\}$.
 - This allows us to define a unique gcd; recall that gcd's are only unique up to multiplication by units, so by making all elements multiplied by units part of the same equivalence class, we can define a unique one.
- **Associate** (elements): Two elements $a, b \in R$ such that $a = ub$ where $u \in R^\times$. Denoted by $a \sim b$.
- Lemma: If $a, b \in R$ a PID, then $\gcd(a, b)$ is equal to any generator of the ideal $Ra + Rb$.

Proof. Since R is a PID, there exists $d \in R$ such that $Ra + Rb = Rd$. Any such d is a generator of $Ra + Rb$. To prove that $d = \gcd(a, b)$, it will suffice to show that $d \mid a$, $d \mid b$, and $d' \mid a, b$ implies $d' \mid d$. Let's begin.

Since $Ra, Rb \subset Ra + Rb = Rd$, we know that $a, b \in (d)$. Thus, $d \mid a, b$. Now let $d' \in R$ be an arbitrary element such that $d' \mid a$ and $d' \mid b$. It follows that $a, b \in (d')$. Since $d \in Ra + Rb$, there exist $\alpha, \beta \in R$ such that $\alpha a + \beta b = d$. Thus, $d = \alpha a + \beta b \in (d')$, so $d' \mid d$, as desired. \square

- Look back to $AX + AY$ from Lecture 2.2!
- We will see later (next week) that $F[X, Y]$ is a UFD and that $\gcd(X, Y) = 1$.
 - But $1 \notin (X, Y)$.
- Assume R is a UFD and $a \neq 0$.
 - A (traditional) factorization of $a = u\pi_1^{k_1}\pi_2^{k_2}\cdots\pi_r^{k_r}$. We assume as we have been that each π_i is irreducible and $i \neq j$ implies that $(\pi_i) \neq (\pi_j)$ iff $\pi_i \approx \pi_j$.
 - What is $R/(a)$?
 - Note: If $I \subset J \subset R$, then there exist ring homomorphisms from

$$R \rightarrow R/I \qquad R \rightarrow R/J \qquad R/I \rightarrow R/J$$

- Consider $(a) \subset (\pi_i^{k_i})$. Then $R/(a) \rightarrow R/(\pi_i^{k_i})$. Moreover, we get a ring homomorphism

$$R/(a) \hookrightarrow \prod_{i=1}^r R/(\pi_i^{k_i})$$

- For the integers, this is an isomorphism.
 - See the Chinese remainder theorem.
- As per before, there exists $\varphi : R \rightarrow \prod_{i=1}^r R/(\pi_i^{k_i})$.
- What is $\ker(\varphi)$?
- We have that $\varphi(h) = 0$ iff $\pi_i^{k_i} \mid h$ for all $i = 1, 2, \dots, r$ iff $\prod_{i=1}^r \pi_i^{k_i} \mid h$ iff $a = u \prod_{i=1}^r \pi_i^{k_i} \mid h$ iff $h \in (a)$.
 - Nori pauses to explain why the factors of a dividing h implies that the product of the factors does as well.
- $\ker(\varphi) = (a)$. Product of commutative diagrams?? See lower right of board 2
- Let $I \subset J_1 \subset R$ and $I \subset J_2 \subset R$.

- Aside.
 - Let $R = F[X, Y]$.
 - Then $R/(XY) \rightarrow (R/(X)) \times (R/(Y))$ is not onto.
 - Note that $R/(X) = F[X, Y]/(X) \cong F[Y]$ and likewise for $R/(Y)$.
 - There is a function $R \rightarrow R/(XY)$.
 - $f(X, Y) \in R$ maps to $f(0, Y)$ and $f(X, 0)$. There must be a condition: $g(0) = h(0)$.
- Let $\pi_1^{k_1} = b$ and $\pi_2^{k_2} \cdots \pi_r^{k_r} = c$. Then $\gcd(b, c) = 1$. If R is a PID, then $Rb + Rc$ is the ideal generated by $\gcd(b, c)$, and hence is R .

- It follows that there exists $\beta, \gamma \in R$ such that $\beta\pi_1^{k_1} + \gamma c = 1$.
- This is the Chinese Remainder Theorem.
- Consider $R \rightarrow R/(\pi_1^{k_1}) \times (R/(\pi_2^{k_2}) \times \cdots \times R/(\pi_r^{k_r}))$ sending

$$\gamma c \mapsto (1, 0, \dots, 0)$$

- Multiply by an arbitrary $h \in R$. Then $h\gamma c \mapsto (h, 0, \dots, 0)$.
- The image contains $R/(\pi_1^{k_1}) \times 0 \times \cdots \times 0$ which contains $0 \times R/(\pi_2^{k_2}) \times 0 \times \cdots \times 0$. This is because if we have $(\alpha_1, \dots, \alpha_r)$, then we can always write it as

$$(\alpha_1, \dots, \alpha_r) = (\alpha, 0, 0, \dots, 0) + (0, \alpha_2, 0, \dots, 0) + \cdots + (0, 0, 0, \dots, \alpha_r)$$

- **Chinese Remainder Theorem:** Let R be a PID, and let a factor as we've discussed. Then the natural arrow $R/(a) \rightarrow \prod_{i=1}^r R/(\pi_i^{k_i})$ is an isomorphism of rings.
- Examples:
 - $F[X]$: $X - a$ is irreducible for all $a \in F$.
 - $\mathbb{C}[X]$: These are the only irreducibles (fundamental theorem of algebra).
 - $\mathbb{R}[X]$: $X - a$ for $a \in \mathbb{R}$ and $(X - z)(x - \bar{z})$ for $z \in \mathbb{C} - \mathbb{R}$ are all irreducible.
- Corollary of the earlier lemma: If $R_1 \subset R_2$ are both PIDs and $(a, b) \in R_1$, then " $\gcd_{R_1}(a, b) = \gcd_{R_2}(a, b)$."

Proof. Let $R_1 a + R_1 b = R_1 d$, $d \in R_1$. Then $R_2 a + R_2 b = R_2 d$. □

- Explanation of what's in quotes: We're taking gcd's in different rings. See the commutative diagram below.

$$\begin{array}{ccc}
 R_1 - \{0\} & \hookrightarrow & R_2 - \{0\} \\
 \downarrow & & \uparrow \\
 \sim \setminus R_1 - \{0\} & \longrightarrow & \sim \setminus R_2 - \{0\}
 \end{array}$$

Figure 4.1: Greatest common divisor in different rings.

- We should check this.
- How do we put $F[X, Y] \subset F[X, Z]$? Put $Y = XZ$. Then $\gcd(X, Y) = 1$.
- Midterm on Monday of sixth week; HW pushed to Friday that week.

4.5 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.6: The Chinese Remainder Theorem

2/1:

- Assume commutative rings with identity.
- **Ring direct product:** The direct product of an arbitrary collection of rings as (abelian) groups, which is made into a ring by defining multiplication componentwise. Denoted by $\mathbf{R}_1 \times \mathbf{R}_2$.
- $\varphi : R \rightarrow R \times \cdots$ is a ring homomorphism iff the induced maps to each component are all homomorphisms.
- The units of a ring direct product are the n -tuples that have units in every entry.
- **Comaximal** (ideals): Two ideals $A, B \subset R$ such that $A + B = R$.
 - Motivation: Two numbers $n, m \in \mathbb{Z}$ being relatively prime is equivalent to $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$, where we may recall that $n\mathbb{Z}, m\mathbb{Z}$ are ideals.
- Generalizing a result about integer division to rings.

Theorem 17 (Chinese Remainder Theorem). Let A_1, \dots, A_k be ideals in R . The map from $R \rightarrow R/A_1 \times \dots \times R/A_k$ defined by

$$r \mapsto (r + A_1, \dots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap \dots \cap A_k$. If for each $i, j \in \{1, \dots, k\}$ with $i \neq j$, the ideals A_i, A_j are comaximal, then this map is surjective and $A_1 \cap \dots \cap A_k = A_1 \cdots A_k$, so

$$R/(A_1 \cdots A_k) = R/(A_1 \cap \dots \cap A_k) \cong R/A_1 \times \dots \times R/A_k$$

Proof. Given. See HW3 Q3.3. □

- History of the Chinese Remainder Theorem.

- Derives its name from the special case that when n, m are relatively prime integers,

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

- In number theoretic terms: This “relates to simultaneously solving two congruences modulo relatively prime integers (and states that such congruences can always be solved, and uniquely)” (Dummit & Foote, 2004, p. 266).
- Such problems were originally considered by the ancient Chinese.

- Using the Chinese Remainder Theorem to prove the Euler φ -function.

Corollary 18. Let n be a positive integer and let $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

as rings, so in particular, we have the following isomorphism of multiplicative groups.

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

Thus,

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

Proof. Since the rings above are isomorphic as rings, their groups of units must be isomorphic as well. Comparing orders on the two sides of the latter isomorphism gives the final result. □

4.6 Chapter 8: Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

From Dummit and Foote (2004).

Goals for the Chapter

1/30:

- Focus: Study classes of rings with more algebraic structure than generic rings.
- **Euclidean Domain:** A ring with a division algorithm. *Also known as ED.*
- **Principal Ideal Domain:** A ring in which every ideal is principal. *Also known as PID.*
- **Unique Factorization Domain:** A ring in which all elements have factorizations into primes. *Also known as UFD.*
- Examples: \mathbb{Z} and $F[X]$ (F a field).
- This chapter: Recover all theorems concerning the integers \mathbb{Z} stated in Chapter 0 as special cases of results valid for more general rings.
- Next chapter: Apply these results to the special case where $R = F[X]$.
- Assumption for this chapter: All rings R are commutative.

Section 8.1: Euclidean Domains

- Definitions of a **norm** and **Euclidean Domain**.
 - Notes on norms.
 - Essentially a measure of “size” in R .
 - The defined notion is fairly weak, and an integral domain R may possess several different norms.
 - **Positive norm**: A norm N such that $N(a) > 0$ for all $a \neq 0$.
 - EDs are said to possess a **Division Algorithm**.
 - **Quotient**: The element q in the definition of a norm/ED. *Denoted by q .*
 - **Remainder**: The element r in the definition of a norm/ED. *Denoted by r .*
- 2/1:
- Division Algorithms allow a **Euclidean Algorithm** for two elements $a, b \in R$ to find the greatest common divisor.
 - Note that these “divisions” are actually divisions in $\text{Frac } R$, for example.
 - Also, note that the Euclidean algorithm terminates since $N(b) > N(r_0) > \cdots > N(r_n)$ is a decreasing sequence of nonnegative integers and thus cannot continue indefinitely.
 - We have no guarantee (yet) that the quotient and remainder are unique.
 - Examples.
 1. Fields.
 - Any norm satisfies the defining condition of the Division Algorithm because we always have $a = qb + 0$ for any $a, b \in F$.
 2. Integers \mathbb{Z} , $N(m) = |m|$.
 - From class.
 - Dummit and Foote (2004) proves rigorously, from a ring theory perspective, that long division is a thing.
 - The quotient and remainder are not unique (unless we require the remainder to be nonnegative).
 - Example: $5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$.
 3. $F[X]$ with $N(f) = \deg(f)$.
 - That long division is a thing is proved similarly to for \mathbb{Z} (see Chapter 9).
 - For polynomials, the quotient and remainder are unique.
 - We will prove later that $R[X]$ is an ED iff R is a field. Essentially, this is because we must be able to divide arbitrary nonzero coefficients.
 4. Quadratic integer rings.
 - Gaussian integers are a subset.
 5. **Discrete valuation rings**.
 - Take $N = \nu$ and $N(0) = 0$.
 - **Discrete valuation** (on K): A function from $K^\times \rightarrow \mathbb{Z}$, where K is a field, satisfying the following constraints. *Denoted by ν . Constraints*
 - (i) $\nu(ab) = \nu(a) + \nu(b)$, i.e., $\nu : (K^\times, \cdot) \rightarrow (\mathbb{Z}, +)$ is a group homomorphism.
 - (ii) ν is surjective.
 - (iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

- **Valuation ring** (of ν): The subring of K defined as follows. *Given by*

$$\{x \in K^\times \mid \nu(x) \geq 0\} \cup \{0\}$$

- **Discrete valuation ring**: An integral domain R for which there exists a valuation ν on $\text{Frac } R$ such that R is the valuation ring of ν .
- Example: The ring R containing all rationals whose denominators are relatively prime to some fixed $p \in \mathbb{Z}$ is a discrete valuation ring of \mathbb{Q} .
- A Division Algorithm makes every ideal of an ED principal.

Proposition 1. Every ideal in an ED is principal. More precisely, if I is any nonzero ideal in the ED R , then $I = (d)$, where d is any nonzero element of I of minimum norm.

Proof. Given. See Lecture 4.1. □

- Since \mathbb{Z} is an ED, Proposition 1 implies that every ideal of \mathbb{Z} is principal.
 - Recall that we have previously proven this in Section 7.3 and 2.3.

- Examples.

1. Consider $\mathbb{Z}[X]$.
 - Since $(2, X)$ is not principal (see Section 7.4), $\mathbb{Z}[X]$ is not an ED.
2. Quadratic integer rings; specifically, $\mathbb{Z}[\sqrt{-5}]$.

- Euclidean Algorithms guarantee a greatest common divisor in any ED.
- **Multiple** (of b): An element $a \in R$ such that $a = bx$ for some $x \in R$.
- **Divisor** (of a): An element $b \in R$ such that $a = bx$ for some $x \in R$. *Also known as **b divides a**.*
- Definition of the **greatest common divisor** of a, b .
- Note:

$$b \mid a \iff a \in (b) \iff (a) \subset (b)$$

- More on discussing gcd's in terms of ideals (repeat from class).

- A *sufficient* condition for the existence of a gcd.

Proposition 2. If a, b are nonzero elements in the commutative ring R such that the ideal generated by a, b is a principal ideal (d) , then d is the greatest common divisor of a, b .

- Note that the condition is not *necessary*: For example, in $\mathbb{Z}[X]$, $(2, x)$ is nonprincipal even though 1 is a valid gcd.
- **Bezout Domain**: An integral domain in which every ideal generated by two elements is principal.
 - Per the exercises, there are Bezout Domains that contain nonprincipal (necessarily infinitely generated) ideals.
- gcd uniqueness.

Proposition 3. Let R be an integral domain. If two elements d, d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, if d, d' are both greatest common divisors of a, b , then $d' = ud$ for some unit u .

Proof. Given. Very slick. □

- Very important property of EDs: gcd's always exist and can be computed algorithmically.

Theorem 4. Let R be an ED, and let $a, b \in R$ be nonzero. Let $d = r_n$ be the last nonzero remainder in the Euclidean algorithm for a, b . Then

1. $d = \gcd(a, b)$.
2. The principal ideal $(d) = (a, b)$. In particular, d can be written as an R -linear combination of a, b , i.e., there exist $x, y \in R$ such that

$$d = ax + by$$

Proof. Given. See the Lemma from Lecture 4.3. □

- The Euclidean Algorithm is **logarithmic** in the size of the integers.
 - It can be proven that “the number of steps required to determine the greatest common divisor of two integers a and b is at worst 5 times the number of digits of the smaller of the two numbers” (Dummit & Foote, 2004, p. 276).

- Some more stuff on uniqueness and Diophantine equations.

- \tilde{R} : The collection of units of R together with 0. *Given by*

$$\tilde{R} = R^\times \cup \{0\}$$

- **Universal side divisor:** An element $u \in R - \tilde{R}$ such that for every $x \in R$, there is some $z \in \tilde{R}$ such that u divides $x - z$ in R .

- Implication: There is a type of division algorithm for every $x \in R$ by u ; indeed, if $u \mid (x - z)$, then there exists $q \in R$ such that $x - z = qu$ or

$$x = qu + z$$

- The existence of universal side divisors is a weakening of the Euclidean condition (i.e. here, we only postulate that we can divide by *some* elements, not *all* elements).

Proposition 5. Let R be an integral domain that is not a field. If R is a Euclidean Domain, then there are universal side divisors in R .

Proof. Given. □

- Example: Proving $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not an ED using Proposition 5.