Week 4

???

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 $\iota : R \to D^{-1}R$ such that for any $\varphi : R \to S$ such that $\varphi(D) \subset S^\times$, there exists a unique $\tilde{\varphi} : D^{-1}R \to S$ 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 $\boldsymbol{F}$ generated by $\boldsymbol{R}$**: The field defined as follows, where F is a field and $R \subset F$ is an integral domain. *Denoted by* $\boldsymbol{K}$. *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

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

Proof. Background: Consider the injection $R \to F$. 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 $K \cong \operatorname{Frac} R$, we will use a bidirectional inclusion proof. For the forward direction, observe that $R \subset \operatorname{Frac} R \subset F$. Therefore, by the definition of K, $K \subset \operatorname{Frac} R$, as desired. For the backward direction, let $x/y \in \operatorname{Frac} R$ 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 $x/y \in \operatorname{Frac} R$, $x, y \in R$. 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. ◻

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

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

- 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* $\boldsymbol{N}$. *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**), $N(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - b^2 d|$ 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
         $$\left\{\alpha + \beta\frac{-1 + \sqrt{-3}}{2} \mid \alpha, \beta \in \mathbb{Z}\right\} \cong \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Q},\ a = \alpha - \frac{1}{2}\beta,\ b = \frac{1}{2}\beta,\ \alpha, \beta \in \mathbb{Z}\right\}$$

[1] Henceforth, "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 $uv = vu = 1$.
- $\boldsymbol{R^\times}$: 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. $\square$

- 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

$$a = u\pi_1\pi_2 \cdots \pi_r \qquad\qquad a = u'\pi_1'\pi_2' \cdots \pi_s'$$

  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

$$a = u\pi_1 \cdots \pi_r \qquad\qquad a = u'\pi_1' \cdots \pi_s'$$

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

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

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. □

- 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* $\boldsymbol{d}$, $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b})$, $\mathbf{g.c.d.}\,(\boldsymbol{a}, \boldsymbol{b})$. *Constraints*
  (i) $d \mid a$ and $d \mid b$.
  (ii) $d' \mid a$ and $d' \mid b$ implies $d' | d$.

- 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 $a_{n+1} = ca_n$, $a_n = b_n \subset a_n$, $1 = b_n c$.