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 $\iota : R \to D^{-1}R$ 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: Dyadic 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 $D = R - \{0\}$ 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**.
- **Strongly Euclidean domain**: An ED for which the norm N satisfies the additional constraint (iii) below. *Also known as* **SED**. *Constraint*

  (iii) $N(ab) = N(a)N(b)$ for all $a, b \in R$.
- 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

  $$d = \min\{N(a) : a \in I - \{0\}\}$$

  Pick $f \in I - \{0\}$ 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. □

- 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. $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ (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 $a, b \in \mathbb{Q}$.
     - Observations (in the context of $\mathbb{Q}[\sqrt{d}]$, not $\mathbb{Z}[\sqrt{d}]$):
       - $N(a + b\sqrt{d}) = 0$ iff $(a, b) = (0, 0)$.
       - $\mathbb{Q}[\sqrt{d}]$ is SE (strongly Euclidean) since $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$.
       - $N(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathbb{Z}[\sqrt{d}]$. This is why only $\mathbb{Z}[\sqrt{d}]$ is an ED.
     - 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 $\cos(120) + i\sin(120)$.

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

    - 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

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

- **Square-free integer**: An integer that is not divisible by the square of any integer.
- **Gaussian integers**: The Euclidean domain $\mathbb{Z}[\sqrt{-1}]$.
- Exercise: Prove that $\mathbb{Z}[\sqrt{d}]$ is SE (i.e., is an SED) for $d=-1,-2,2,3$.
    - Hint: Given $h,f\in\mathbb{Z}[\sqrt{d}]$, we have $h/f\in\mathbb{Q}[\sqrt{d}]$. Choose $q\in\mathbb{Z}[\sqrt{d}]$ as close as possible to h/f. For a given d, you will find $N(q-h/f)<1$.
    - The same procedure will show that $\mathbb{Z}[(-1+\sqrt{d})/2]$ is SE for $d=-3,5$.
- **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. $F^\times=F-\{0\}$.
    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. $\mathbb{Z}^\times=\{\pm1\}$.
    4. $\mathbb{Z}[\sqrt{-1}]^\times=\{\pm1,\pm i\}$.
    5. $R[X]^\times=R^\times$ (R an integral domain).
    6. Suppose R is not an integral domain. Then we get things like $a\neq0\in R$ 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.
- $R-\{0\}$ is a disjoint union of...
    (i) Units;
    (ii) Reducible elements;
    (iii) And irreducible elements.

Proof. Suppose for the sake of contradiction that $a\in R-\{0\}$ 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. □

- Corollary: If $a_1 \cdots a_r \in R^\times$, then $a_i \in R^\times$ $(i = 1, \dots, r)$.

  Proof. Same strategy as above, i.e., definition of a unit followed by associativity. □

- 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**: An integral domain R such that for every nonzero element $a \in R$ which is not a unit, any two factorizations
  $$a = u\pi_1\pi_2 \cdots \pi_r \qquad a = u'\pi_1'\pi_2' \cdots \pi_s'$$
  of a satisfy the following conditions.
  (i) *Same length*: $r = s$.
  (ii) *Uniqueness up to* ***associates***: 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., $R - P$ is a multiplicative set.
  - Equivalently (contrapositive): $ab \in P$ implies $a \in P$ or $b \in P$.
- 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): A nonzero element that is neither a unit nor reducible.
  - Think of them a bit like primes, though this is very dangerous. See Dummit and Foote (2004).

- **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 $-1\in\mathbb{Z}^\times=\{\pm1\}$.
- 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 the existence of prime factorizations in PIDs. Without a convenient norm from which to derive a prime factorization (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 or c has a factorization, then $a=bc$ factors further.
  - WLOG, let c have a factorization.
  - Let $c=b_1a_2$, where $b_1,a_2\notin R^\times$. Suppose a_2 admits a factorization. Then $a_2=b_2a_3$, where $b_2,a_3\notin R^\times$.
  - We can go on forever: $a_n=b_na_{n+1}$ where $b_n\notin R^\times$ and a_{n+1} factors further.
  - By their definitions, $\cdots(a_n)\subset(a_{n+1})\cdots$. Additionally, $b_n\notin R^\times$ implies $(a_n)\neq(a_{n+1})$.
  - Now consider a chain of 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 $I=(\alpha)$.
  - Definition of an infinite union: There exists n such that $\alpha\in I_n$. Therefore, $(\alpha)\subset I_n\subsetneq I_{n+1}\subset\cdots\subset(\alpha)$. It follows that the factorization is finite.
  - See the proof in the book for clarification: Theorem 8.14 of Dummit and Foote (2004).

- Last theorem to prove.
- Theorem: R is a PID implies R is a UFD.
  - Existence, we've done directly above.
  - Equivalence: By Lemma*, we only need irreducible $\pi \in R$ to be prime.
  - a is reducible.
  - Gist: $a = bc$, $b \notin R^\times$ 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 $a_{n+1} = ca_n$, $a_n = b_n \subset a_n$, $1 = b_n c$.
- Lastly, we have a theorem summarizing some of today's results.
- Theorem: Let R be an integral domain such that every nonzero $a \in R$ admits a factorization. Then TFAE.
  1. R is a UFD.
  2. Every irreducible element of R is prime.
  3. Every pair of elements of R has a gcd.

  Proof. Partially given above. □

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 $a^2 = 1^2a^2$ 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. $\underline{(2) \implies (3)}$: Since (π) is a maximal ideal, $R/(\pi)$ is a field. Thus, it's an integral domain. Therefore, (π) is a prime ideal.

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

  $\underline{(1) \implies (2)}$: 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. □

- Recall computing greatest common divisors from last lecture.
  - In particular, we know that $R - \{0\}$ (or R??) is an integral domain.
  - Thus, if $a, b \in R - \{0\}$, 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: $\sim \backslash R - \{0\}$ implies that we're applying the equivalence relation $\sim$ to the set $R - \{0\}$.
  - $\gcd(a, b) \in \sim \backslash R - \{0\}$.
    - This allows us to define a unique gcd; recall that gcd's are only unique up to multiplication by units, so by making all **associates** 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* $\boldsymbol{a \sim b}$.
- 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. □

- 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 $\pi_i \nsim \pi_j$.
  - What is $R/(a)$?
  - Note: If $I \subset J \subset R$, then there exist ring homomorphisms from

    $$R \to R/I \qquad\qquad R \to R/J \qquad\qquad R/I \to R/J$$

  - Consider $(a) \subset (\pi_i^{k_i})$. Then $R/(a) \to R/(\pi_i^{k_i})$. 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 $\varphi : R \to \prod_{i=1}^{r} R/(\pi_i^{k_i})$.
  - What is $\ker(\varphi)$?
  - We have that $\varphi(h) = 0$ iff $\pi_i^{k_i} \mid h$ for all $i = 1, 2, \ldots, r$ 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 motivate why the factors of a dividing h implies that 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 $R/(XY) \to (R/(X)) \times (R/(Y))$ is not onto.
    - Note that $R/(X) = F[X, Y]/(X) \cong F[Y]$ and likewise for $R/(Y)$.
    - There is a function $R \to R/(XY)$.
    - $f(X, Y) \in R$ 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 $R \to R/(\pi_1^{k_1}) \times (R/(\pi_2^{k_2}) \times \cdots \times R/(\pi_r^{k_r}))$ 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 $R/(a) \to \prod_{i=1}^r R/(\pi_i^{k_i})$ 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 $(X - z)(x - z)$ 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.

$$\begin{tikzcd}
R_1 - \{0\} \arrow[r, hook] \arrow[d] & R_2 - \{0\} \\
\sim \backslash R_1 - \{0\} \arrow[r] & \sim \backslash R_2 - \{0\} \arrow[u]
\end{tikzcd}$$

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.
- Problem: Let F be a subfield of the field E. Assume $\gcd(f, g) = 1$ where $f, g \in F[X]$. Show that there does not exist $a \in E$ such that $f(a) = g(a) = 0$.
- Problem: Let $f \in \mathbb{Q}[X]$. Assume that $\gcd(f, f') = 1$ where f' denotes the derivative of f. Prove that if $f(a) = 0$ for some $a \in \mathbb{R}$, then f is not divisible by $(X - a)^2$ in $\mathbb{R}[X]$.

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* $\boldsymbol{R_1 \times R_2}$.
- $\varphi : R \to R \times \cdots$ 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 7.17 (Chinese Remainder Theorem)**.** Let $A_1, \dots, A_k$ be ideals in R. The map from $R \to R/A_1 \times \cdots \times R/A_k$ defined by
  $$r \mapsto (r + A_1, \dots, r + A_k)$$
  is a ring homomorphism with kernel $A_1 \cap \cdots \cap A_k$. 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 $A_1 \cap \cdots \cap A_k = A_1 \cdots A_k$, so
  $$R/(A_1 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k$$

  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 7.18. 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
  $$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$
  as rings, so in particular, we have the following isomorphism of multiplicative groups.
  $$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$
  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 week, 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**.
- Converting between the book's definition of an ED and the in-class one.
  - Take the N of the book, define $N'(x) = N(x) + 1$ for all nonzero $x \in R$ and $N'(0) = 0$. Then N' satisfies the in-class requirements.
- **Quotient**: The element q in the definition of a norm/ED. *Denoted by* $\boldsymbol{q}$.
- **Remainder**: The element r in the definition of a norm/ED. *Denoted by* $\boldsymbol{r}$.

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 $\operatorname{Frac} R$, 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 is 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 are not EDs in general.
   - Take the absolute value of the field norm to get a potential norm, but these rarely work.
   - Gaussian integers do work, though, under this absolute value field norm.
   - The rest of the proof that $\mathbb{Z}[i]$ is an ED goes beyond the scope of class.
5. **Discrete valuation rings**.
   - Take $N = \nu$ and $N(0) = 0$.

- **Discrete valuation** (on K): A function from $K^\times \to \mathbb{Z}$, where K is a field, satisfying the following constraints. *Denoted by* $\boldsymbol{\nu}$. *Constraints*

  (i) $\nu(ab) = \nu(a) + \nu(b)$, i.e., $\nu : (K^\times, \cdot) \to (\mathbb{Z}, +)$ 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*

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

- **Discrete valuation ring**: An integral domain R for which there exists a valuation ν on $\operatorname{Frac} R$ 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 8.1. 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 8.1 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. The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID.
     - Consider the ideal $I = (3, 2 + \sqrt{-5})$. Suppose it equals $(a + b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$ and then arrive at contradictions in every case you consider.

- 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 8.2. 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 8.3. 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. Not very important since its only relation to class content is via the lemma from Lecture 4.3 that $Ra + Rb = (\gcd(a, b))$. However, included because it's very slick. We prove each statement separately.

  Suppose $(d) = (d')$. We divide into two cases (d or d' is 0, and neither is zero). Suppose first that d or d' is 0. WLOG, let $d = 0$. Then $d' \in (0) = \{0\}$, so $d' = 0$. Therefore, since $0 = 1 \cdot 0$, $d' = ud$ for a unit (specifically the identity, for example) in R. Now suppose that $d, d' \neq 0$. Since $d \in (d')$, $d = xd'$ for some $x \in R$. Similarly, $d' = yd$ for some $y \in R$. It follows that

$$\begin{aligned} d &= xyd \\ d(1 - xy) &= 0 \end{aligned}$$

  Since R is an integral domain, $d = 0$ or $1 - xy = 0$. But $d \neq 0$ by hypothesis, so

$$\begin{aligned} 1 - xy &= 0 \\ 1 &= xy \end{aligned}$$

  Therefore, x, y are both units and we have the desired result.

  If d, d' are both gcd's of a, b, then $(d) = (d')$. Thus, apply the first statement to obtain the desired result. □

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

  Theorem 8.4. 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.
- $\widetilde{\boldsymbol{R}}$: The collection of units of R together with 0. *Given by*
$$\widetilde{R} = R^\times \cup \{0\}$$
- **Universal side divisor**: An element $u \in R - \widetilde{R}$ such that for every $x \in R$, there is some $z \in \widetilde{R}$ 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 8.5. 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 8.5.

Section 8.2: Principal Ideal Domains

2/3:

- Definition of a **PID**.
- Since EDs are PIDs, all results proved herein hold for EDs, too.
- Examples.
  1. $\mathbb{Z}$ is a PID; $\mathbb{Z}[X]$ is not (think $(2, X)$).
  2. Quadratic integer rings.
- Not every PID is an ED.
- Dummit and Foote (2004) believes that PIDs are a natural class of rings in which to study ideals.
- Both EDs and PIDs have gcd's; only EDs have an algorithm for computing them, though.
  - Thus, gcd-adjacent results are often proven in PIDs, but specific examples are typically computed using a Euclidean Algorithm if available.
- Facts about gcd's.

Proposition 8.6. Let R be a PID and let a, b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then...

1. d is a greatest common divisor of a and b;
2. d can be written as an ***R*-linear combination** of a and b.
3. d is unique up to multiplication by a unit of R.

Proof. See Propositions 8.2-8.3, which this proposition just rehashes. □

- Per Corollary 7.14, every maximal ideal is a prime ideal. The converse also holds in PIDs.

  Proposition 8.7. Every nonzero prime ideal in a PID is a maximal ideal.

  Proof. See Lecture 4.3. □

- Recall that F a field implies that $F[X]$ is an ED. The converse also holds in PIDs.

  Corollary 8.8. If R is any commutative ring such that the polynomial ring $R[X]$ is a PID (or an ED), then R is necessarily a field.

  Proof. Given. □

- We wrap up by proving that not every PID is an ED. We also relate the principal ideal property to another weakening of the Euclidean condition.
- **Dedekind-Hasse norm**: A positive norm N such that for every nonzero $a, b \in R$, either $a \in (b)$ or there exists a nonzero element $x \in (a, b)$ such that $N(x) < N(b)$.
  - Alternate definition: Either $b \mid a \in R$ or there exist $s, t \in R$ such that $0 < N(sa - tb) < N(b)$.
  - Dedekind-Hasse norms and all related content will be omitted from this course.
- R is Euclidean with respect to N if it is always possible to satisfy the Dedekind-Hasse condition with $s = 1$..
  - This means that other values of s represent a related but weaker condition than the Euclidean one; this is the weakening alluded to above.
- PIDs and Dedekind-Hasse normed spaces are equivalent.

  Proposition 8.9. The integral domain R is a PID iff R has a Dedekind-Hasse norm.

  Proof. Given. □

- Note: That a ring satisfying the Dedekind-Hasse condition is a PID has been known since 1928. That a PID necessarily satisfies the Dedekind-Hasse condition was not discovered until 1997.
- Example: Proof that $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a PID but not an ED.

Section 8.3: Unique Factorization Domains

2/5:

- In addition to the Euclidean Algorithm, gcd's can be computed via factorization into primes and a simple comparison.
- The notion of factorization can be extended to a larger class of rings called UFDs.
- Goal of this section: Prove that every PID is a UFD; thus, all results in this section will hold for EDs and PIDs, too.
- **Irreducible** (element): A nonzero element $r \in R$ that is not a unit and such that whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R.
- **Reducible** (element): An element that is not reducible.
  - Recall from class that even though it's not explicitly stated in the definition, we can prove that reducible elements are not units.
- **Prime** (element): A nonzero element $p \in R$ that is not a unit and such that whenever $p \mid ab$ for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.
  - The definition from class is also given.
- Definition of **associate** elements.
- Prime implies irreducible.

  Proposition 8.10. In an integral domain, a prime element is always irreducible.

  Proof. Let (p) be an arbitrary prime ideal in R an integral domain. Suppose $p = ab$. Then $ab \in (p)$, so WLOG $a \in (p)$. It follows that $a = pr$ for some $r \in R$. Thus, $p = ab = prb$, so by the cancellation lemma (which applies under the given hypotheses), $rb = 1$. Therefore, b is a unit, so p is irreducible, as desired. □

- Irreducible $\not\Rightarrow$ prime in general.
  - Example using quadratic integer rings given.
- Prime $\iff$ irreducible in a PID.

  Proposition 8.11. In a PID, a nonzero element is prime iff it is irreducible.

  Proof. Given (see Lecture 4.3). □

- Example.
  1. Quadratic integer rings.
- Example:
  - The irreducible of $\mathbb{Z}$ are the prime numbers (and their negatives).
  - Two integers $a, b \in \mathbb{Z}$ are associates iff $a = \pm b$.
- Dummit and Foote (2004) discusses factorization in $\mathbb{Z}$ in the language of rings (e.g., "units," "irreducible," "unique," etc.) to motivate UFDs.
  - Very insightful.
- **Prime factorization**: The expression of an element in $\mathbb{N}$ as a product of other elements in $\mathbb{Z}$, all of which are positive and prime.

- Definition of a **UFD**.
- Examples.
    1. All fields F are trivially UFDs.
        - All elements are units, so there exist no elements for which we can verify the constraints, so the condition is vacuously true.
    2. PIDs are UFDs.
        - E.g., $\mathbb{Z}$, $F[X]$ are UFDs.
    3. $R[X]$, where R is a UFD.
        - See Theorem 9.7.
        - This contrasts with EDs and PIDs, where R being an ED (resp. PID) does not make $R[X]$ an ED (resp. PID).
        - It follows that $\mathbb{Z}[X]$ is a UFD.
    4. $\mathbb{Z}[2i]$: Integral domain that is not a UFD.
        - See Exercise 7.1.23.
        - Argument included.
    5. $\mathbb{Z}[\sqrt{-5}]$: Another integral domain that is not a UFD.
        - Argument included.
- Proposition 8.11 for UFDs.

  Proposition 8.12. In a UFD, a nonzero element is prime iff it is irreducible.

  Proof. Given (not covered in class).

  Note that this proposition plus the previously alluded to result that PID $\Longrightarrow$ UFD do *not* suffice to prove Proposition 8.11. This is because we will need Proposition 8.11 to prove that PID $\Longrightarrow$ UFD, and we must avoid circular reasoning. □

- Greatest common divisors exist in UFDs.

  Proposition 8.13. Let a, b be two nonzero elements of a UFD R and suppose that

  $$a = up_1^{e_1} \cdots p_n^{e_n} \qquad\qquad b = vp_1^{f_1} \cdots p_n^{f_n}$$

  are prime factorizations for a and b, where u, v are units, the primes $p_1, \dots, p_n$ are *distinct*, and the exponents $e_i, f_i \geq 0$ $(i = 1, \dots, n)$. Then the element

  $$d = p_1^{\min(e_1,f_1)} \cdots p_n^{\min(e_n,f_n)}$$

  (where $d = 1$ if all the exponents are 0) is a gcd of a, b.

  Proof. Given (not directly covered in class; related to Statement (*) from Lecture 5.1). According to the Week 4 summary, it is important. The proof in the book is a bit hand-wavey, though.

  We first must prove that $d \mid a, b$. This follows immediately from the fact the the exponents of each prime in d are no larger than the corresponding ones in a, b.

  We now must prove that if $c \mid a, b$, then $c \mid d$. Since R is a UFD, factor c into $q_1^{g_1} \cdots q_m^{g_m}$. Consider an arbitrary q_i. Since it divides c, it must divide a, b. In particular, since it and all of the p_j are irreducible by Proposition 8.12, it must divide some p_j to yield a unit. Thus, q_i and p_j are the same up to associates. Consequently, all q's are equal to p's up to associates. We get a similar condition on the exponents to that in d, implying that $c \mid d$, as desired. □

- Example.

  1. An application of Proposition 8.13.

- We now prove the main result.

  Theorem 8.14. Every PID is a UFD. In particular, every ED is a UFD.

  Proof. Let R be a PID, and let r be an arbitrary nonzero element of R which is not a unit. To prove that R is a UFD, it will suffice to show that r can be written as a finite product of irreducible elements of R and that this decomposition is unique up to associates.

  Existence: We proceed analogously to the prime factorization algorithm for integers, meaning that we will divide into cases, subcases, subsubcases, etc. as needed depending on whether or not all factors are irreducible at each step and then use the "finiteness" of r to prove that the decomposition can only go on for so long. To see what this means, let's begin. If r is irreducible, then we are done. Otherwise, r is reducible, and hence $r = r_1r_2$ where $r_1, r_2 \notin R^\times$. If r_1, r_2 are both irreducible, then (again) we are done. Otherwise, at least one of the two elements (say r_1) is reducible and hence can be written $r_1 = r_{11}r_{12}$ for nonunit elements r_{11}, r_{12}. We can continue on in this manner.

  We now verify that this process terminates. Precisely, we verify that we necessarily reach a point where all of the elements obtained as factors of r are irreducible. Let's begin. Suppose for the sake of contradiction that the process never terminates. Then we obtain a *proper* inclusion of ideals

  $$(r) \subsetneq (r_1) \subsetneq (r_{11}) \subsetneq \cdots \subsetneq R$$

  where the labeling is justified WLOG[2] Note that the above can also be called an infinite ascending chain of ideals. Also note that the first inclusion is proper because r_2 is not a unit, the second is proper because r_{12} is not a unit, on and on until the last inclusion is proper because $r_{1\cdots 1}$ is not a unit. Lastly, note that we need the Axiom of Choice (why??) to justify the existence of such an infinite chain.

  To verify that the proper inclusion terminates, it will suffice to demonstrate that any ascending chain $I_1 \subsetneq \cdots \subsetneq R$ of ideals *in a PID* eventually becomes stationary. Precisely, we wish to find a positive integer n such that $I_k = I_n$ for all $k \geq n$. Let's begin. Let

  $$I = \bigcup_{i=1}^{\infty} I_i$$

  We can prove (easily from the definition) that I is an ideal. Thus, since R is a PID, we may write $I = (a)$ for some $a \in R$. It follows by the definition of I that $a \in I_n$ for some $n \geq 1$. By definition, $I_n \subset I$; additionally, $I = (a) \subset I_n$ since I_n is an ideal. Consequently, $I = I_n$ and the chain becomes stationary at I_n.

  Returning to the original case, the above result implies a contradiction. Thus, the original chain of ideals terminates. Therefore, a factorization of r into irreducibles is finite and, importantly, *exists.*

  Uniqueness: Since R is a PID, Proposition 8.11 implies that all irreducible elements are prime. Therefore, by Lemma* from Lecture 4.2, any two factorizations of r are equivalent, as desired. Note that Dummit and Foote (2004) proves their own version of Lemma* as part of the argument.

  The second statement follows from the first and Proposition 8.1. □

- In the proof of Theorem 8.14, we showed that any ascending chain of ideals in a PID eventually becomes stationary.

  - In Chapter 12, we will prove a more general result: An ascending chain of ideals becomes stationary in any commutative ring where all the ideals are *finitely generated.*

[2] If r_1 is irreducible and r_2 is reducible, flip the names.

- Theorem 8.14 implies another, very important result.

  Corollary 8.15 (Fundamental Theorem of Arithmetic)**.** The integers $\mathbb{Z}$ are a UFD.

  Proof. They're an ED, and hence a UFD by Theorem 8.14. □

- Relation to Dedekind-Hasse norms.

  Corollary 8.16. Let R be a PID. Then there exists a multiplicative Dedekind-Hasse norm on R.

  Proof. Given. □

- We now switch to the specific example of factorization in the Gaussian integers.
  - This will be covered in the class at a later date.
- Dummit and Foote (2004) proves a number of interesting theorems not covered in any depth in class.
- Dummit and Foote (2004) concludes the chapter with a short summary.
  - Restatement of the central result:

    $$\text{fields} \subsetneq \text{EDs} \subsetneq \text{PIDs} \subsetneq \text{UFDs} \subsetneq \text{integral domains}$$

  - Review of examples that prove *proper* inclusion:
    - $\mathbb{Z}$ is an ED, not a field.
    - $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID, not an ED.
    - $\mathbb{Z}[X]$ is a UFD (see Theorem 9.7), not a PID.
    - $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, not a UFD.