NOVEMBER 16 NOTES

We discuss Chapter 8 of the textbook (all at once, instead of in individual sections).

1. Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

Let R be an integral domain. Today, we will define three different types of domain and see how they are related.

Definition 1.1. A function $N : R \to \mathbb{Z}^{\geq 0}$ such that $N(0) = 0$ is called a **norm** on R. If $N(a) > 0$ for all $a \neq 0$, then N is a **positive norm.**

Definition 1.2. An integral domain R is a **Euclidean Domain** if there exists a norm on R such that R has a division algorithm: for any $a, b \in R$, there exists $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $N(r) < N(b)$.

Example 1.3.
(1) Fields are Euclidean domains with any norm, because for any $a, b \in F$, $a = qb + 0$ where $q = ab^{-1}$.
(2) $\mathbb{Z}$ is a Euclidean domain with norm $N(a) = |a|$.
(3) If F is a field, $F[x]$ is a Euclidean domain with norm $N(p(x)) = \deg p(x)$. (We can do long division of polynomials.)
(4) The quadratic integer rings $\mathcal{O}$ are typically not Euclidean domains, but $\mathbb{Z}[i]$ is. Let $N(a + bi) = a^2 + b^2$. Let $\alpha = a + bi$ and $\beta = c + di$ be elements of $\mathbb{Z}[i]$. In $\mathbb{Q}(i)$, we can write $\alpha/\beta = r + si$ for rational numbers r, s. Let p be the integer closest to r and q the integer closest to s (note that this implies that $|r - p| \leq 1/2$ and $|s - q| \leq 1/2$).

Then, in $\mathbb{Z}[i]$, we can write $\alpha = (p + qi)\beta + (\alpha - (p + qi)\beta)$. Because

$$\alpha - (p + qi)\beta = \beta(\alpha/\beta - (p + qi)) = \beta((r - p) + (s - q)i),$$

we have

$$N(\alpha-(p+qi)\beta) = N(\beta((r-p)+(s-q)i)) = N(\beta)N((r-p)+(s-q)i) = N(\beta)((r-p)^2+(s-q)^2) \leq \frac{1}{2}N(\beta)$$

so $N(\alpha - (p + qi)\beta) < N(\beta)$, and hence $\mathbb{Z}[i]$ is a Euclidean domain.

Definition 1.4. An integral domain in which every ideal is principal is called a **principal ideal domain** (PID).

Example 1.5. Fields are PIDs because the only ideals are (0) and (1). The integers $\mathbb{Z}$ are a PID because the only ideals are (n) for some $n \in \mathbb{Z}$.

Example 1.6. $\mathbb{Z}[x]$ is not a principal ideal domain. The ideal $(2, x) = \{2p(x) + xq(x) \mid p, q \in \mathbb{Z}[x]\}$ is not principal. If it were, then $(2, x) = (a(x))$ for $a(x) \in \mathbb{Z}[x]$. Then, $2 \in (a(x))$ so $2 = p(x)a(x)$ for some $p(x) \in \mathbb{Z}[x]$. Since degree is additive, this implies that $\deg p(x) = \deg a(x) = 0$, so $p(x)$ and $a(x)$ are integers. But, the only factors of 2 are $\pm 1, \pm 2$, so either $a(x) = \pm 1$ or $a(x) = \pm 2$. If $a(x) = \pm 1$, it is a unit, so $(a(x)) = \mathbb{Z}[x]$, which is a contradiction because $1 \notin (2, x)$. If $a(x) = \pm 2$, then $x \in (a(x))$ implies that $x = 2q(x)$ for some $q \in \mathbb{Z}[x]$, which is impossible. Therefore, $(2, x)$ is not principal.

Proposition 1.7. *If R is a Euclidean domain, then R is a principal ideal domain.*

Proof. Suppose $I \subset R$ is an ideal. If $I = (0)$, then I is principal. Suppose $I \neq (0)$ and let $d \in I$ be any element with minimum norm. Then, $d \in I$ implies $(d) \subset I$, and if $a \in I$ is any element, then because R is a Euclidean domain, $a = qd + r$ where either $r = 0$ or $N(r) < N(d)$. However,

$r = a - qd \in I$, so we cannot have $N(r) < N(d)$, so we must have $r = 0$ and $a = qd$ so $a \in (d)$. Therefore, $I = (d)$. $\square$

Example 1.8. If $R = \mathbb{Z}[\sqrt{-5}]$, then R is not a PID so not a Euclidean domain. In particular, not all quadratic integer rings are Euclidean domains.

Let $I = (3, 2 + \sqrt{-5})$. We will show that I is not principal. Let N be $N(a + b\sqrt{-5}) = a^2 + 5b^2$. If $I = (a + b\sqrt{-5})$ were principal, then $3 = \alpha(a + b\sqrt{-5})$ and $2 + \sqrt{-5} = \beta(a + b\sqrt{-5})$ for some $\alpha, \beta \in R$. Taking norm of the first equation, we get $9 = N(\alpha)(a^2 + 5b^2)$, but norms are integers, so this implies $a^2 + 5b^2 = 1, 3, 9$. It cannot be 3 (there are just no solutions to this equation) and it cannot be 1 because this implies that $a^2 = 1$ and $b = 0$, so $I = (\pm 1)$ so $I = R$, which is a contradiction (exercise: show this!). Finally, it cannot be 9 because that implies that $N(\alpha) = 1$, so we must have $\alpha = \pm 1$, but then $a + b\sqrt{-5} = \pm 3$, so $2 + \sqrt{-5} = \pm 3\beta$, a contradiction. Therefore, this is not principal.

Proposition 1.9. *Suppose R is a PID. Then, every nonzero prime ideal in R is maximal.*

Proof. Let (p) be a nonzero prime ideal and let $I = (m)$ be an ideal containing (p). Then, $p \in (m)$, so $p = rm$ for some $r \in R$, but (p) is prime, so this means $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(m) \subset (p)$ so $(m) = (p)$. If $r \in (p)$, then $r = ps$ for some $s \in R$ so $p = rm = psm$ so $sm = 1$ and hence m is a unit and $(m) = R$. Therefore, the only ideals that contain (p) are (p) and R, so (p) is maximal. $\square$

Corollary 1.10. If R is commutative such that $R[x]$ is a PID, then R is a field.

Proof. Because $R \subset R[x]$ which is an integral domain, R is an integral domain. Note that (x) is a nonzero prime ideal because $R[x]/(x) \cong R$ is an integral domain, but the previous proposition implies that (x) is maximal, so in fact $R[x]/(x) \cong R$ is a field. $\square$

Euclidean domains and PIDs enjoy many of the same properties as the integers. We won't prove all of these because their proofs are *the same* as the proofs when $R = \mathbb{Z}$.

Suppose R is an integral domain.

Definition 1.11. If $a, b \in R$, $b \neq 0$, then we say b divides a if $a = bx$ for some $x \in R$. The greatest common divisor of a and b is $d = \gcd(a, b)$ such that $d \mid a$, $d \mid b$, and for any d' such that $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Proposition 1.12. *If the ideal $(a, b) = (d)$, then d is the greatest common divisor of a and b.*

Proposition 1.13. *If R is a PID and $a, b \in R$ are nonzero elements, then $(a, b) = (d)$ where $d = \gcd(a, b)$.*

Remark 1.14. Not every PID is a Euclidean domain. See the book for the proof that certain quadratic integer rings are PIDs but not Euclidean domains.

Finally, we define UFDs.

Definition 1.15. Let R be an integral domain.

(1) A nonzero, nonunit element $r \in R$ is **irreducible** if whenever $r = ab$ for $a, b \in R$, either a or b is a unit. If r is not irreducible, it is **reducible**.
(2) If $p \in R$ is a nonzero, nonunit, it is **prime** if (p) is a prime ideal. (Equivalently, if $p \mid ab$, then $p \mid a$ or $p \mid b$.)
(3) If $a = ub$ for a unit $u \in R$, then a and b are **associate**.

Proposition 1.16. *If R is an integral domain, a prime element is irreducible.*

Proof. Suppose p is prime and $p = ab$. Because p is prime, $a = pr$ or $b = pr$ for some $r \in R$. Without loss of generality, suppose $a = pr$. Then, $p = ab = prb$ so $rb = 1$ so b is a unit, so p is irreducible. $\square$

So, prime always implies irreducible. The converse holds in PIDs.

Proposition 1.17. *If R is a PID, an element is prime if and only if it is irreducible.*

Proof. We must show an irreducible element is prime. Suppose p is irreducible and let $M = (m)$ be any ideal containing (p) (which is principal by assumption). Then, $p \in (m)$, so $p = rm$, but p is irreducible, so either r or m is a unit. If r is a unit, then $(p) = (m)$, and if m is a unit, then $(m) = R$, so the only ideals containing (p) are itself or R, so (p) is maximal and hence prime. □

Definition 1.18. A **unique factorization domain** (UFD) is an integral domain R in which every nonzero nonunit element $r \in R$ satisfies:

(1) $r = p_1 \dots p_n$ for irreducible elements $p_i \in R$, and
(2) this decomposition is unique up to associates (if $r = q_1 \dots q_m$, then $n = m$ and up to rearranging, $p_i = u_i q_i$ for some unit u_i).

Example 1.19. $\mathbb{Z}$ is a UFD because every element has a prime factorization.

Example 1.20. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD: we can write $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Exercise: these are two non-associate factorizations into irreducible elements.

Proposition 1.21. *If R is a UFD, an element is prime if and only if it is irreducible.*

Proof. We must show an irreducible element is prime. Suppose p is irreducible and assume $p \mid ab$, so $pc = ab$ for some $c \in R$. Writing a, b, c as products of irreducible elements and using associateness of the factorization, because p is irreducible, it must be associate to one of the elements in the factorization of a or b (without loss of generality, assume a). Then, $a = (up)p_2 \dots p_n$, so $p \mid a$ and hence p is prime. □

Theorem 1.22. *Every PID is a UFD.*

Proof. Let R be a PID and $r \in R$ is a nonzero element. We must show that R has a unique factorization into irreducible elements. *This proof follows the same structure as the proof that we can factor integers!*

If r is irreducible, then we are done. If r is not irreducible, then $r = r_1 r_2$ where neither r_1, r_2 is a unit. If these are irreducible, we are not. If not, write $r_1 = r_{11} r_{12}$ and $r_2 = r_{21} r_{22}$. We will just repeat this process until we obtain the factorization of r, so it just suffices to show that this terminates.

Suppose that this never ended. Then, $(r) \subset (r_1) \subset (r_{11}) \subset (r_{111}) \subset \cdots \subset R$. Because these elements do not differ by a unit, all of these containments are proper, so we have an infinite ascending chain of ideals. However, this is a contradiction: let $I_0 = (r)$, $I_1 = (r_1)$, etc, and let $I = \cup_{k \geq 0} I_k$. Because I is an ideal and R is a PID, I is principal, so $I = (a)$ for some $a \in R$, but by definition of union, we must have $a \in I_k$ for some k so $I \subset I_k$ and hence $I_n = I_k$ for all $n \geq k$. Therefore, this chain of ideals must terminate, so we have a contradiction.

One can show uniqueness by induction, which we leave to the reader. □

So, we have shown:
Fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ integral domains.