II. PIDs, UFDs & Euclidean Domains

Definition 1. An ideal $I$ of a ring $R$ is a principal ideal provided $I = (x) = xR = Rx$ for some element $x \in R$. An integral domain $R$ is a principal ideal domain, or PID, if every ideal of $R$ is principal.

Example 2.
1. The ring of integer $\mathbb{Z}$ is a PID.
2. The ring $\mathbb{Z}[x]$ is not a PID.

Definition 3. Let $R$ be an integral domain. An element $a$ divides an element $b$, written $a \mid b$, provided there exists $q \in R$ such that $b = aq$. The element $a$ is a proper divisor of $b$ if neither $a$ nor $q$ is a unit. A nonzero nonunit element $x \in R$ is irreducible if $x$ has no proper divisors. Two elements $a$ and $b$ of $R$ are associates if $a = ub$ for some unit $u$ of $R$. A nonzero nonunit $p$ is prime in $R$ provided the ideal $(p)$ is a prime ideal in $R$.

Example 4.
1. The prime elements and the irreducible elements of $\mathbb{Z}$ are precisely the prime numbers and their additive inverses. The units of $\mathbb{Z}$ are $\pm 1$ and thus $a$ and $b$ are associates if and only if $a = \pm b$.
2. The prime elements and the irreducible elements of $\mathbb{Q}[x]$ are the polynomials which cannot be written as the product of two nonconstant polynomials. Two polynomials $f$ and $g$ in $\mathbb{Q}[x]$ are associate if and only if $f = rg$ for some $0 \neq r \in \mathbb{Q}$.

Proposition 5. Let $R$ be an integral domain. Then every prime element is irreducible.

Proposition 6. Let $R$ be an integral domain. The following statements are equivalent.

1. For each nonzero nonunit $x \in R$, the process of factoring $x$ into a product of irreducible elements terminates after finitely many steps.

2. The ring $R$ does not contain an infinite chain of principal ideals

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots .$$

Definition 7. Existence of factorization holds in $R$ when property 1 of Proposition 6 is satisfied. An integral domain $R$ satisfies the ascending chain condition on principal ideals or ACCP if property 2 of Proposition 6 is satisfied.
Example 8.
1. The ring \( \mathbb{Z} \) satisfies ACCP.
2. The ring \( \mathbb{C}[x_1, x_2, x_3, x_4, \ldots] \), where \( x_2^2 = x_1, x_3^2 = x_2 \), etc. does not satisfy ACCP.

Definition 9. An integral domain \( R \) is a unique factorization domain or UFD provided each nonzero nonunit element in \( R \) can be factored as a product of finitely many irreducible elements and whenever \( a_1a_2a_3 \cdots a_s = b_1b_2 \cdots b_t \) with each \( a_i \) and \( b_j \) irreducible,

1. \( s = t \) and
2. after a suitable reordering, \( a_i = u_ib_i \), where each \( u_i \) is a unit.

Example 10.
1. The rings \( \mathbb{Z}, \mathbb{C}[x] \) and \( \mathbb{Z}[i] \) are UFDs.
2. The rings \( \mathbb{Z}[\sqrt{-5}] \) and \( \mathbb{Z}[2i] \) are not UFDs.

Proposition 11. Let \( R \) be an integral domain which satisfies ACCP. Then \( R \) is a UFD if and only if the set of irreducible elements coincides with the set of prime elements.

Definition 12. An integral domain \( R \) is a Euclidean domain if there exists a function \( N : R - \{0\} \to \mathbb{N} \), called a norm on \( R \) such that whenever \( a, b \in R \) with \( b \neq 0 \), there exist elements \( q \) and \( r \) in \( R \) such that \( a = bq + r \) with either \( r = 0 \) or \( N(r) < N(b) \).

Example 13.
1. The ring \( \mathbb{Z} \) is a Euclidean domain.
2. If \( F \) is a field, the ring \( F[x] \) is a Euclidean domain.

Theorem 14. Let \( R \) be an integral domain.
1. If \( R \) is a PID, then \( R \) is a UFD.
2. If \( R \) is a Euclidean domain, then \( R \) is a PID.

Example 15.
1. The ring \( \mathbb{Z} \) is a UFD.
2. If \( F \) is a field, the ring \( F[x] \) is a UFD.
Definition 16. A polynomial \( f(x) \in \mathbb{Z}[x] \) is \textbf{primitive} if the coefficients of \( f \) have no nonunit common factors.

Lemma 17. If \( 0 \neq f \in \mathbb{Q}[x] \), then there is a unique positive \( c \in \mathbb{Q} \) and a unique primitive \( f_0(x) \in \mathbb{Z}[x] \) such that \( f(x) = cf_0(x) \).

Definition 18. The rational number \( c \) in Lemma 17 is called the \textbf{content} of \( f \).

Theorem 19. (Gauss’s Lemma) The product of a finite number of primitive polynomials in \( \mathbb{Z}[x] \) is again primitive.

Proposition 20.

1. Any nonconstant polynomial \( f \in \mathbb{Z}[x] \) that is irreducible in \( \mathbb{Z}[x] \) is also irreducible in \( \mathbb{Q}[x] \).

2. Let \( f \) be a polynomial in \( \mathbb{Z}[x] \) with positive leading coefficient. Then \( f \) is irreducible in \( \mathbb{Z}[x] \) if and only if either

   (a) \( f \) is a prime integer, or

   (b) \( f \) is primitive and irreducible in \( \mathbb{Q}[x] \).

Proposition 21. Every irreducible element of \( \mathbb{Z}[x] \) is prime.

Theorem 22. The ring \( \mathbb{Z}[x] \) is a \textbf{UFD}.

Example 23. The ring \( \mathbb{Z}[x] \) is a \textbf{UFD}, but is not a \textbf{PID}.

Theorem 24. Let \( D \) be a \textbf{UFD}. Then \( D[x] \) is \textbf{UFD}.
Homework II:

1. ✷ Let $R$ be a commutative ring with unity. Prove the following statements.
   
   (a) An element $u \in R$ is a unit if and only if $(u) = R$.
   
   (b) Further assume that $R$ is an integral domain. Prove that elements $a$ and $b$ are associates if and only if $(a) = (b)$.
   
   (c) If $a$ and $b$ are elements of $R$, then $a | b$ if and only if $(a) \supseteq (b)$ with strict containment if and only if $a$ properly divides $b$.

2. ✷ Let $r$ be an element of a PID $R$. Prove that $r$ is irreducible if and only if $r$ is prime.

3. Prove that if $R$ is a PID with nonzero element $p$, then $R/(p)$ is a field if and only if $p$ is irreducible in $R$.

4. ✷ Let $F$ be a field, $a \in F$, and $f(x) \in F[x]$. Prove that $a$ is a root of $f(x)$ if and only if $x - a$ is a factor of $f(x)$. (Hint: Use Euclidian Division Algorithm.)

5. Prove that the following rings are not unique factorization domains. In each case, give at least two distinct factorizations of some nonzero nonunit.
   
   (a) $\mathbb{Q}[x^2, x^3]$
   
   (b) $\mathbb{Z}[\sqrt{-n}]$ where $n$ is a squarefree integer greater than 3.
      (Hint: First show that $2$, $\sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducible in $R$.)

6. ✷ Prove that the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, of Gaussian integers is a Euclidian domain and hence a UFD. Explain why the identities $5 = (2 + i)(2 - i)$ and $2 \cdot 3 = 6 = (1 + i)(1 - i) \cdot 3$ do not violate unique factorization. (Hint: Consider the ‘usual’ complex norm $N(a + bi) = a^2 + b^2$ on $\mathbb{Z}[i]$ and the fact that it is multiplicative; i.e., $N(\alpha \beta) = N(\alpha)N(\beta)$. Given $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, write $\frac{\alpha}{\beta} = r + si$ in $\mathbb{Q}(i)$ (the quotient field of $\mathbb{Z}[i]$, cf. 9) and find integers $p$ and $q$ sufficiently close to $r$ and $s$ respectively so that you can apply the division algorithm in $\mathbb{Z}$.)

7. Generalize the statements and proofs of Lemma 17 through Theorem 22 to $D$ a UFD and $F$ its quotient field. Prove Theorem 24.

8. (Mod $p$ Irreducibility Test) Let $f \in \mathbb{Z}[x]$ such that a prime $p$ does not divide the leading coefficient of $f$. Prove that if $\overline{f}$, the polynomial $f$ with coefficients reduced modulo $p$, is irreducible in $\mathbb{Z}_p[x]$, then $f$ is irreducible in $\mathbb{Q}[x]$. (Hint: reduce to primitive polynomials.) Use this fact to prove that $x^4 - 6x^3 + 12x^2 - 3x + 9$ is irreducible in $\mathbb{Q}[x]$. 


9. ★ In this sequence of exercises, you will develop the quotient field of an integral domain, analogous to the field of rational numbers which contains the ring of integers.

(a) Let $R$ be an integral domain and define a fraction to be a symbol $a/b$ with $a, b \in R$ and $b \neq 0$. Let $S$ denote the set of all fractions of elements in $R$. We define a relation $\approx$ on the set $S$ of symbols as follows: $a/b \approx c/d$ if and only if $ad = bc$ in $R$. Prove that $\approx$ is an equivalence relation on $S$.

(b) Define $F = S/\approx$ to be the set of equivalence classes of fractions. That is, we consider two fractions to be equal in $F$ if they are equivalent in $S$. Define multiplication and addition of fractions in the obvious ways: $(a/b)(c/d) = (ac)/(bd)$, $a/b + c/d = (ad + bc)/(bd)$. Prove that these are well-defined operations on $F$; i.e., verify that these rules lead to equivalent answers if the fractions $a/b$ and $c/d$ are each replaced by equivalent fractions.

(c) Prove that $F$ is a field (that contains $R$) by proving the following items.

- Prove that $F$ is an abelian group with respect to addition.
- Prove that multiplication in $F$ is commutative and associative and that it distributes across addition.
- Prove that $F$ has a multiplicative identity and that every nonzero element has a multiplicative inverse.

(d) Finally, prove that $F$ is unique up to isomorphism. In other words, prove that any field containing an isomorphic copy of $R$ must also contain an isomorphic copy of $F$.

10. ★ Let $D$ be an integral domain with quotient field $K$. Let $f, g \in K[x]$, and $a \in D$. If $fD[x] \subseteq gD[x]$, then $f(a)D \subseteq g(a)D$.

Supplemental Reading and Exercises

- Read Chapter 3 (pages 36–38 and pages 41 (the last third)–43 of M. F. Atiyah and I. G. MacDonald Introduction to Commutative Algebra.

- Work exercises # 3 and # 9.