Chapter 11. Factorization in Commutative Rings

11.1 Definition: Let R be a ring. An ideal P in R is called **prime** when $P \neq R$ and for all ideals A and B in R, if $AB \subseteq P$ then either $A \subseteq P$ or $B \subseteq P$. An ideal M in R is called **maximal** when $M \neq R$ and there is no ideal A in R with $M \subsetneqq A \subsetneqq R$.

11.2 Example: As an exercise, use the above definition to show that the maximal ideals in $\mathbb{Z}$ are the ideals of the form $\langle p \rangle$ with p prime, and the prime ideals in $\mathbb{Z}$ are the ideals of the form $\langle p \rangle$ with $p = 0$ or p prime.

11.3 Theorem: *Let R be a commutative ring with 1. Let P be an ideal in R with $P \neq R$. Then P is prime if and only if P has the property that for all $a, b \in R$, if $ab \in P$ then either $a \in P$ or $b \in P$.*

Proof: Since R is commutative with 1, we have $\langle a \rangle = \left\{ ar \middle| r \in R \right\}$ and $\langle b \rangle = \left\{ bs \middle| s \in R \right\}$ and so

$$\begin{aligned} \langle a \rangle \langle b \rangle &= \left\{ \sum_{i=1}^{n} a_i b_i \middle| a_i \in \langle a \rangle, b_i \in \langle b \rangle \right\} = \left\{ \sum_{i=1}^{n} (ar_i)(bs_i) \middle| r_i, s_i \in R \right\} \\ &= \left\{ \sum_{i=1}^{n} (ab)t_i \middle| t_i \in R \right\} = \langle ab \rangle. \end{aligned}$$

Suppose that P is prime. Let $a, b \in R$ with $ab \in P$. Then $\langle a \rangle \langle b \rangle = \langle ab \rangle \subseteq P$ and so, since P is prime, either $\langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$, and hence either $a \in P$ or $b \in P$.

Conversely, suppose that P has the property that for all $a, b \in R$, if $ab \in P$ then either $a \in P$ or $b \in P$. Let A and B be ideals in R with $AB \subseteq P$. Suppose that $A \not\subseteq P$. Choose $a \in A$ with $a \notin P$. Let $b \in B$ be arbitrary. Then $ab \in AB \subseteq P$ and so, because of the property held by P, either $a \in P$ or $b \in P$. Since $a \notin P$ we must have $b \in P$. Thus $B \subseteq P$.

11.4 Theorem: *Let R be a commutative ring with 1. Let P be an ideal in R. Then P is prime if and only if R/P is an integral domain.*

Proof: Suppose that P is prime. Since $P \neq R$ we have $1 \notin P$ (since $\langle 1 \rangle = R$) and so $1 + P \neq 0 + P \in P/R$. Since R is commutative, so is R/P. Finally, note that R/P has no zero divisors because for $a, b \in R$ we have

$$\begin{aligned} (a+P)(b+P) = (0+P) &\Longrightarrow ab + P = 0 + P \Longrightarrow ab \in P \Longrightarrow a \in P \text{ or } b \in P \\ &\Longrightarrow a + P = 0 + P \text{ or } b + P = 0 + P. \end{aligned}$$

Conversely, suppose that R/P is an integral domain. Since $1 + P \neq 0 + P \in R/P$, it follows that $1 \notin P$ and so $P \neq R$. Let $a, b \in R$ with $ab \in P$. Then we have $ab + P = 0 + P$, and so $(a+P)(b+P) = 0 + P$. Since R/P has no zero divisors, this implies that either $a + P = 0 + P$ or $b + P = 0 + P$, and so either $a \in P$ or $b \in P$.

11.5 Example: Let R be a commutative ring with 1. Show that every maximal ideal in R is also prime.

Solution: Let M be a maximal ideal in R. Let $a, b \in R$ with $ab \in M$. Suppose that $a \notin M$. Then we have $M \subsetneqq M + \langle a \rangle$ and so, since M is maximal, we must have $M + \langle a \rangle = R$. In particular $1 \in M + \langle a \rangle$, so we have $1 = m + ar$ for some $r \in R$. Thus

$$b = b \cdot 1 = b(m + ar) = bm + ab\,r \in M\,.$$

We remark that this result also follows from the following theorem.

11.6 Theorem: *Let R be a commutative ring with 1. Let M be an ideal in R. Then M is maximal if and only if R/M is a field.*

Proof: Suppose M is maximal. Since $M \neq R$ we have $1 \notin M$ and so $1+M \neq 0+M \in R/M$. Since R is commutative, so is R/M. Let $a+M$ be a nonzero element in R/M. We must show that $a+M$ is a unit. Since $a+M \neq 0+M$ we have $a \notin M$. Since $a \notin M$ we have $M \subsetneqq M+\langle a\rangle$. Since M is maximal, we must have $M+\langle a\rangle = R$. In particular, $1 \in M+\langle a\rangle$, say $1 = m+ar$ with $r \in R$. Then $1+M = ar+M = (a+M)(r+M)$ and so $r+M$ is the inverse of $a+M$.

Conversely, suppose that R/M is a field. Since $1+M \neq 0+M$ in R/M, we have $1 \notin M$ so $M \neq R$. Let A be an ideal with $M \subseteq A \subseteq R$. Suppose $A \neq M$. Choose $a \in A$ with $a \notin M$. Since $a \notin M$ we have $a+M \neq 0+M$ in R/M. Since R/M is a field, $a+M$ has an inverse, say $(a+M)(b+M) = 1+M$. Then $ab+M = 1+M$ so we have $1-ab \in M$. Since $M \subseteq A$ we have $1-ab \in A$. Since $a \in A$ we have $ab \in A$, so $1 \in A$ and hence $A = R$.

11.7 Example: Find all prime and maximal ideals in $\mathbb{Z}$ (that is redo example 10.2) using Theorems 10.4 and 10.6.

11.8 Example: Since $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}[\sqrt{2}]$, which is a field, it follows that $\langle x^2-2\rangle$ is maximal (and prime). In $\mathbb{R}[x]$, however, we have $(x^2-2) = (x-\sqrt{2})(x+\sqrt{2})$, and so the ideal $\langle x^2-2\rangle$ is not maximal because $\langle x^2-2\rangle \subsetneqq \langle x-\sqrt{2}\rangle \subsetneqq \mathbb{R}[x]$ and it is not prime because $(x-\sqrt{2})(x+\sqrt{2}) \in \langle x^2-2\rangle$ but $(x-\sqrt{2}) \notin \langle x^2-2\rangle$ and $(x+\sqrt{2}) \notin \langle x^2-2\rangle$.

11.9 Example: In $\mathbb{Z}[x]$, we have $\langle x\rangle = \big\{f \in \mathbb{Z}[x] \big| f(0) = 0\big\}$. The ideal $\langle x\rangle$ is prime because for $f,g \in \mathbb{Z}[x]$, if $fg \in \langle x\rangle$ then $f(0)g(0) = 0$ and so either $f(0) = 0$ or $g(0) = 0$. But the ideal $\langle x\rangle$ is not maximal since $\langle x\rangle \subsetneqq \langle 2,x\rangle = \big\{f \in \mathbb{Z}[x] \big| f(0) \text{ is even}\big\} \subsetneqq \mathbb{Z}[x]$.

11.10 Definition: Let R be a commutative ring with 1. Let $a,b \in R$. We say that a **divides** b (or that a is a **divisor** or **factor** of b, or that b is a **multiple** of a), and we write $a\big|b$, when $b = ar$ for some $r \in R$. We say that a and b are **associates**, and we write $a \sim b$, when $a\big|b$ and $b\big|a$. Note that association is an equivalence relation on R.

11.11 Theorem: *Let R be a commutative ring with 1. Let $a,b \in R$. Then*
(1) $a\big|b$ if and only if $b \in \langle a\rangle$ if and only if $\langle b\rangle \subseteq \langle a\rangle$,
(2) $a \sim b$ if and only if $\langle a\rangle = \langle b\rangle$ if and only if a and b have the same multiples and divisors,
(3) $a \sim 0$ if and only if $a = 0$ if and only if $\langle a\rangle = \{0\}$,
(4) $a \sim 1$ if and only if a is a unit if and only if $\langle a\rangle = R$.
(5) if R is an integral domain then $a \sim b$ if and only if $b = au$ for some unit $u \in R$.

Proof: We prove Part (5) and leave the other proofs as an exercise. Suppose that $b = au$ where $u \in R$ is a unit. Since $b = au$ we have $a|b$ and since $a = bu^{-1}$ we have $b|a$. Since $a|b$ and $b|a$ we have $a \sim b$ (we did not need to assume that R is an integral domain for this direction). Now suppose that R is an integral domain and that $a \sim b$, say $a = br$ and $b = as$ with $r,s \in R$. Then we have $b = as = brs$ so that $b(1-rs) = 0$. Since R is an integral domain, either $b = 0$ or $1-rs = 0$. If $b = 0$ then $a = br = 0$, so we have $b = a \cdot u$ for any unit u (for example $u = 1$). If $1-rs = 0$ then $rs = 1$ so that r and s are units, so we have $b = au$ where $u = s$ (which is a unit).

11.12 Example: In the ring $\mathbb{Z}$, we have $k \sim \ell \iff k = \pm\ell$. Verify that in $\mathbb{Z}_{12}$ the association classes are $\{0\}$, $\{1,5,7,11\}$, $\{2,10\}$, $\{3,9\}$, $\{4,8\}$, $\{6\}$.

11.13 Definition: Let R be a commutative ring with 1. Let $a \in R$ be a non-zero non-unit. We say that a is **reducible** when $a = bc$ for some non-units $b, c \in R$, and otherwise we say that a is **irreducible**. We say that a is **prime** when for all $b, c \in R$, if $a \big| bc$ then either $a \big| b$ or $a \big| c$.

11.14 Theorem: *Let R be a commutative ring with 1. Let $a, b \in R$ with $a \sim b$. Then*
(1) $a = 0$ if and only if $b = 0$,
(2) a is a unit if and only if b is a unit,
(3) a is reducible if and only if b is reducible,
(4) a is irreducible if and only if b is irreducible,
(5) a is prime if and only if b is prime.

Proof: The proof is left as an exercise.

11.15 Example: In the ring $\mathbb{Z}$, for $k \in \mathbb{Z}$, k is irreducible if and only if k is prime if and only if $k = \pm p$ for some (positive) prime number p.

11.16 Example: As an exercise, verify that in the ring $\mathbb{Z}_{12}$, the irreducible elements are 2 and 10 and the prime elements are 2, 3, 9 and 10.

11.17 Example: Use the method of the Sieve of Eratosthenes to find several irreducible elements in $\mathbb{Z}[\sqrt{3}\,i]$ and also some irreducible elements which are not prime.

11.18 Theorem: *Let R be a commutative ring with 1. Let $a \in R$. Then*
(1) If a is irreducible then the divisors of a are the units in R and the associates of a in R.
(2) a is prime if and only if $\langle a \rangle$ is a non-zero prime ideal.

Proof: The proof is left as an exercise.

11.19 Theorem: *Let R be an integral domain and let $a \in R$. Then*
(1) if a is prime then a is irreducible,
(2) a is irreducible if and only if $\langle a \rangle$ is maximal amongst non-zero proper principal ideals,
(3) if R is a PID and a is irreducible, then a is prime.

Proof: To Prove Part (1), suppose that a is prime. Suppose that $a = bc$ with $b, c \in R$. Since $a = bc$ we have $a \big| bc$ and hence, since a is prime, either $a|b$ or $a|c$. Suppose that $a|b$, say $b = ar$. Then $a = bc = arc$ so that $a(1 - rc) = 0$. Since R is an integral domain and $a \neq 0$ it follows that $rc = 1$ so that c is a unit. A similar argument shows that if $a|c$ then b is a unit, and so a is irreducible, as required.

To prove Part (2), suppose that a is irreducible. Since $a \neq 0$ we have $\langle a \rangle \neq 0$ and since a is not a unit we have $\langle a \rangle \neq R$. Let $b \in R$ and suppose that $\langle a \rangle \subseteq \langle b \rangle \subseteq R$. Since $\langle a \rangle \subseteq \langle b \rangle$ we have $a \in \langle b \rangle$, say $a = bc$ with $c \in \mathbb{R}$. Since a is irreducible, either b is a unit, in which case $\langle b \rangle = R$, or c is a unit in which case $b \sim a$ so that $\langle b \rangle = \langle a \rangle$.

Suppose, conversely, that $\langle a \rangle$ is maximal amongst nonzero proper principal ideals in R. Since $\langle a \rangle \neq \{0\}$ we have $a \neq 0$ and since $\langle a \rangle \neq R$ it follows that a is not a unit. Suppose that $a = bc$ where $b, c \in R$. Since $a = bc$ we have $a \in \langle b \rangle$ so that $\langle a \rangle \subseteq \langle b \rangle$. By the maximality of $\langle a \rangle$, either $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = R$. If $\langle b \rangle = R$ then b is a unit. Suppose that $\langle b \rangle = \langle a \rangle$, say $b = ar$ with $r \in R$. Then $a = bc = arc$ so that $a(1 - rc) = 0$. Since $a(1 - rc) = 0$ and $a \neq 0$ and R is an integral domain, it follows that $rc = 1$ so that c is a unit. This completes the proof of Part (2).

Finally note that if a is irreducible and R is a PID then, by Part (2), $\langle a \rangle$ is a maximal ideal, hence $\langle a \rangle$ is a prime ideal, hence a is prime. This proves Part (3).

11.20 Definition: A **Euclidean domain** (or ED) is an integral domain R together with a function $N : R \setminus \{0\} \to \mathbb{N}$, called a **norm**, with the property that for all $a, b \in R$ with $a \neq 0$ there exist $q, r \in R$ such that $b = qa + r$ and either $r = 0$ or $N(r) < N(a)$.

11.21 Definition: A **principal ideal domain** (or PID) is an integral domain R such that every ideal in R is principal.

11.22 Definition: A **unique factorization domain** (or UFD) is an integral domain R with the property that for every nonzero non-unit $a \in R$ we have
(1) $a = a_1 a_2 \cdots a_l$ for some $l \in \mathbb{Z}^+$ and some irreducible elements $a_i \in R$, and
(2) if $a = a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_m$ where $l, m \in \mathbb{Z}^+$ and each a_i and b_j is irreducible, then $m = l$ and for some permutation $\sigma \in S_m$ we have $a_i \sim b_{\sigma(i)}$ for all i.

11.23 Example: The ring $\mathbb{Z}$ is a Euclidean domain with norm given by $N(k) = |k|$.

11.24 Example: Every field F is a Euclidean domain, using any function $N : F \setminus \{0\} \to \mathbb{N}$ as a norm. Indeed, given $a, b \in F$ with $a \neq 0$ we can choose $q = \frac{b}{a}$ and $r = 0$ to get $b = aq + r$.

11.25 Example: If F is a field then $F[x]$ is a Euclidean domain with norm $N(f) = \deg(f)$.

11.26 Example: Show that in the ring $\mathbb{Z}[\sqrt{3}\, i]$, the elements 2 and $1 \pm \sqrt{3}\, i$ are irreducible and $2 \not\sim 1 \pm \sqrt{3}\, i$. It follows that $\mathbb{Z}[\sqrt{3}\, i]$ not a unique factorization domain because $4 = 2 \cdot 2 = (1 + \sqrt{3}\, i)(1 - \sqrt{3}\, i)$.

11.27 Theorem: *Every Euclidean domain is a principal ideal domain.*

Proof: Let R be a Euclidean domain with norm N. Let A be an ideal in R. If $A = \{0\}$ then A is principal with $A = \langle 0 \rangle$. Suppose that $A \neq \{0\}$. Choose a nonzero element $0 \neq a \in A$ of smallest possible norm. We claim that $A = \langle a \rangle$. Since $a \in A$ we have $\langle a \rangle \subseteq A$. Let $b \in A$ be arbitrary. Choose $q, r \in R$ such that $b = qa + r$ and either $r = 0$ or $N(r) < N(a)$. Note that $r = b - qa \in A$ so we must have $r = 0$ by the choice of a. Thus $b = qa \in \langle a \rangle$.

11.28 Definition: A ring R is called **Noetherian** when it satisfies the following condition, which is called the **ascending chain condition**: for every ascending chain of ideals $A_1 \subseteq A_2, \subseteq A_3 \subseteq \cdots$ in R, there exists $n \in \mathbb{Z}^+$ such that $A_k = A_n$ for all $k \geq n$.

11.29 Theorem: *Every principal ideal domain is Noetherian.*

Proof: Let R be a principal ideal domain. Let $a_1, a_2, a_3, \cdots \in R$ with

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots .$$

Let $A = \bigcup_{k=1}^{\infty} \langle a_k \rangle$. Verify that A is an ideal. Choose $a \in R$ so that $A = \langle a \rangle$. Since $a \in A$, we can choose $n \in \mathbb{Z}^+$ so that $a \in \langle a_n \rangle$. For all $k \geq n$, we have $\langle a_k \rangle \subseteq A = \langle a \rangle \subseteq \langle a_n \rangle \subseteq \langle a_k \rangle$ and so $\langle a_k \rangle = \langle a_n \rangle$.

11.30 Theorem: *Every principal ideal domain is a unique factorization domain.*

Proof: Let R be a principal ideal domain. Let $a \in R$ be a non-zero non-unit. We claim that a has an irreducible factor. If a is irreducible then we are done. Suppose that a is reducible, say $a = a_1 b_1$ where a_1 and b_1 are non-units. Note that $\langle a \rangle \subsetneqq \langle a_1 \rangle$. If a_1 is irreducible then we are done. Suppose that a_1 is reducible, say $a_1 = a_2 b_2$ where a_2 and b_2 are non-units. Then $a = a_1 b_1 = a_2 b_2 b_1$ and $\langle a \rangle \subsetneqq \langle a_1 \rangle \subsetneqq \langle a_2 \rangle$. If a_2 is irreducible then we are done, and otherwise we continue this procedure. Eventually, the procedure must end giving us an irreducible factor a_n of a, otherwise we would obtain an infinite chain of ideals $\langle a \rangle \subsetneqq \langle a_1 \rangle \subsetneqq \langle a_2 \rangle \subsetneqq \cdots$, contradicting the fact that R is Noetherian.

Next we claim that $a = a_1 a_2 \cdots a_l$ for some $l \in \mathbb{Z}^+$ and some irreducible $a_i \in R$. If a is irreducible then we are done. Suppose that a is reducible. Let a_1 be an irreducible factor of a, and say $a = a_1 b_1$. Note that b_1 is not a unit since, if it was then we would have $a \sim a_1$, but a is reducible and a_1 is not. If b_1 is irreducible then we are done. Suppose b_1 is reducible. Let a_2 be an irreducible factor of b_1 and say $b_1 = a_2 b_2$. As above, note that b_2 is not a unit. If b_2 is irreducible then we are done, and otherwise we continue the procedure. Eventually, the procedure must end giving us $a = a_1 a_2 \cdots a_n b_n$ with each a_i and n_n irreducible, otherwise we would obtain an infinite chain $\langle a \rangle \subsetneqq \langle b_1 \rangle \subsetneqq \langle b_2 \rangle \subsetneqq \cdots$.

Finally, we claim that if $a = a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_l$ with $l, m \in \mathbb{Z}^+$ and each a_i and b_j irreducible, then $m = l$ and for some permutation $\sigma \in S_m$ we have $a_i \sim b_{\sigma(i)}$ for all i. Suppose that $a = a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_m$ where $l, m \in \mathbb{Z}^+$ and the a_i and b_j are irreducible. Since $a_1 \big| a_1 a_2 \cdots a_l$, we have $a_1 \big| b_1 b_2 \cdots b_m$. Since a_1 is irreducible and R is a principal ideal domain, it follows that a_1 is prime by Part 3 of Theorem 10.19. Since a_1 is prime and $a_1 \big| b_1 b_2 \cdots b_m$, it follows that $a_1 \big| b_k$ for some k. After permuting the elements b_i we can assume $a_1 \big| b_1$. Since b_1 is irreducible, its divisors are units and associates and, since a_1 is not a unit, we have $a_1 \sim b_1$. Since $a_1 \sim b_1$ we have $b_1 = a_1 u$ for some unit u. Thus we have $a_1 a_2 \cdots a_l = b_1 b_2 \cdots b_m = a_1 u b_2 b_3 \cdots b_m$, and by cancellation, $a_2 a_3 \cdots a_l = u b_2 b_3 \cdots b_m$. A suitable induction argument gives $l = m$ and $a_i \sim b_i$ for all i.

11.31 Example: Show that $\mathbb{Z}[i]$ is a ED.

11.32 Example: Since $\mathbb{Z}[\sqrt{3}\, i]$ is not aUFD, it cannot be a PID. Find an ideal in $\mathbb{Z}[\sqrt{3}\, i]$ which is not principal.

11.33 Example: Show that $\mathbb{Z}\left[\frac{1+\sqrt{19}\, i}{2}\right]$ is a PID, but not a ED (under any norm).