III.I. Unique factorization domains

Let R be a commutative domain, and $\alpha \in R \backslash \{0\}$. We recall (cf. III.H.6) that

$$\text{(III.I.1)} \qquad \alpha \text{ is irreducible} \iff (\alpha) \text{ is maximal in } \mathcal{PP}(R).$$

We are interested in

(a) when $r \in R\backslash\{0\}$ can be expressed as a product of irreducibles, and
(b) when (and in what sense) such a factorization is unique.

III.I.2. DEFINITION. R satisfies the **ascending chain condition for principal ideals (ACCPI)** iff for each chain $I_1 \subseteq I_2 \subseteq \cdots$ in $\mathcal{PP}(R)$, there exists $n \in \mathbb{N}$ such that $I_m = I_n$ for all $m \geq n$.

III.I.3. REMARK. If $I_k = (a_k)$, this says that

$$\cdots \mid a_3 \mid a_2 \mid a_1 \implies \exists n \in \mathbb{N} \text{ such that } a_m \sim a_n \ (\forall m \geq n).$$

That is, there are no infinite sequences $\{a_i\} \subseteq R$ where each a_{i+1} is a *proper* factor of a_i ($a_{i+1} \mid a_i$ but $a_i \nmid a_{i+1}$). In this form, the ACCPI is known as the **divisor chain condition (DCC)**, which is the terminology I'll use for both.

III.I.4. LEMMA. *DCC holds $\implies$ every $I \in \mathcal{PP}(R)$ is contained in a maximal element.*

PROOF. $(a) \in \mathcal{PP}(R) \implies (a)$ maximal or $(a) \subsetneq (a')$. Rinse and repeat; DCC implies this terminates. $\square$

III.I.5. THEOREM. *DCC holds $\implies$ any $r \in R\backslash(R^* \cup \{0\})$ is a finite product of irreducibles.*

PROOF. Clearly $(r) \in \mathcal{PP}(R)$. Assume r is not itself irreducible. Then (r) is not maximal in $\mathcal{PP}(R)$, so that III.I.4 gives a *proper* containment $(r) \subsetneq (a_1)$ in a maximal element $(a_1) \in \mathcal{PP}(R)$; we thus have $r = a_1 r_1$, with $r_1 \in R\backslash(R^* \cup \{0\})$. If r_1 is not irreducible, repeat to get $(r_1) \subsetneq (a_2)$ maximal in $\mathcal{PP}(R)$, which gives $r_1 = a_2 r_2$.

Suppose this process doesn't terminate. Then we obtain sequences

$$\begin{cases} a_1, a_2, a_3, \ldots & \text{of irreducible elements} \\ r_1, r_2, r_3, \ldots & \text{of elements of } R \backslash (R^* \cup \{0\}) \end{cases}$$

such that $r = a_1 a_2 \cdots a_n r_n$ ($\forall n$). Hence $r_n = r_{n+1} a_{n+1}$, with $a_{n+1} \notin R^*$, so that $(r_n) \subsetneq (r_{n+1})$ ($\forall n$), a contradiction by the DCC.

Conclude that for some n, r_n is irreducible, and $r = a_1 a_2 \cdots a_n r_n$ presents r as a product of irreducibles. $\square$

III.I.6. Definition. (i) Let $r \in R$. Two factorizations

$$r_1 \cdots r_m = r = s_1 \cdots s_n$$

into irreducibles are **essentially equivalent** if

$$m = n \text{ and } \exists \sigma \in \mathfrak{S}_n \text{ such that } s_i \sim r_{\sigma(i)} \ (i = 1, \ldots, n).$$

(ii) R is a **unique factorization domain (UFD)** if

$$\begin{cases} \text{(a) every } r \in R \backslash (R^* \cup \{0\}) \text{ is a product of irreducibles, and} \\ \text{(b) this product is essentially unique.} \end{cases}$$

(iii) Given a UFD R and $r = r_1 \cdots r_n \in R \backslash (R^* \cup \{0\})$ (with $r_1, \ldots, r_n$ irreducible), we define the **length** $\ell(r)$ to be n. (The length of a unit is defined to be 0.) Clearly $\ell(rs) = \ell(r) + \ell(s)$ for all $r, s \in R \backslash \{0\}$.

Continuing for the time being with a general commutative domain R, we have the

III.I.7. Definition. An element $a \in R \backslash (R^* \cup \{0\})$ is **prime** if

$$a \mid bc \implies a \mid b \text{ or } a \mid c.$$

(Note that this is the same as saying that (a) is a prime ideal.)

III.I.8. Lemma. *For $a \in R \backslash (R^* \cup \{0\})$, a prime $\implies$ a irreducible.*

Proof. Given $a \in R$ prime, suppose $a = bc$. Then $a \mid b$ or $a \mid c$. If $a \mid b$, we have $b = ar$ (for some $r \in R$) $\implies a = arc \implies rc = 1 \implies c \in R^*$. Likewise, if $a \mid c$, then $b \in R^*$. So a is irreducible. $\square$

The converse does *not* hold in general:

III.I.9. EXAMPLE. In $\mathbb{Z}[\sqrt{10}]$, 3 is irreducible (by a norm argument, cf. III.D.6). But 3 is *not* prime:

$$3 \mid 9 = (1+\sqrt{10})(-1+\sqrt{10}),$$

but 3 divides neither $1+\sqrt{10}$ nor $-1+\sqrt{10}$.

One way to think of all this is that for a principal ideal (a),

$$\text{(III.I.10)} \qquad \begin{array}{ccccc} (a) \text{ maximal} & \Longrightarrow & (a) \text{ prime} & \Longrightarrow & \begin{array}{c}(a) \text{ maximal} \\ \text{in } \mathcal{PP}(R)\end{array} \\ & & \updownarrow & & \updownarrow \\ & & a \text{ prime} & \Longrightarrow & a \text{ irreducible.} \end{array}$$

III.I.11. DEFINITION. R satisfies the **primeness condition (PC)** if every irreducible element is also prime.

III.I.12. THEOREM. *Let R be a commutative domain. Then*

$$R \text{ is a UFD} \quad \Longleftrightarrow \quad R \text{ satisfies DCC and PC.}$$

PROOF. ($\Longrightarrow$): Suppose given an ascending chain $(a_1) \subseteq (a_2) \subseteq \cdots$ in $\mathcal{PP}(R)$; without loss of generality we may assume $(a_1) \neq \{0\}$. Then $\ell(a_1)$, $\ell(a_2)$, ... is a non-increasing[27] sequence in $\mathbb{N}$. So there exists an $n \in \mathbb{N}$ such that $(\forall m \geq n)$ $\ell(a_m) = \ell(a_n) =: \ell$. Now

$$(a_m) \supseteq (a_n) \quad \Longrightarrow \quad a_m \mid a_n \quad \Longrightarrow \quad a_n = a_m r$$

and factoring into irreducibles gives

$$a_{n,1} \cdots a_{n,\ell} = a_{m,1} \cdots a_{m,\ell}(r_1, \cdots r_j u)$$

(where $u \in R^*$ and the rest are irreducible). By (essential) uniqueness, $j = 0$ (i.e. $r \in R^*$) and after reordering $a_{n,i} \sim a_{m,i} \implies a_m \sim a_n$ $\implies (a_m) = (a_n)$ $(\forall m \geq n)$. So DCC holds.

Next, if r is irreducible and $r \mid ab$, write $ab = rc$. If $a \in R^*$ then $r \mid b$, and if $b \in R^*$ then $r \mid a$; otherwise, write $a = a_1 \cdots a_k$, $b = b_1 \cdots b_\ell$, $c = c_1 \cdots c_m$ (for factorizations into irreducibles), which

[27] e.g. factor both sides of $a_1 = a_2 r$ into irreducibles to see $\ell(a_2) \leq \ell(a_1)$.

gives $a_1 \cdots a_k b_1 \cdots b_\ell = rc_1 \cdots c_m$. By (essential) uniqueness, $r \sim$ some a_i or $b_j \implies r \mid a$ or b. So r is prime, i.e. PC holds.

($\Longleftarrow$): Let $r \in R \backslash (R^* \cup \{0\})$ be given. Since DCC holds, r is a product of irreducibles by III.I.5. To check the (essential) uniqueness, let $\mu(r)$ denote the minimum number of irreducible factors in such a product. If $\mu(r) = 1$, then r is irreducible, and can't split as a product of more than one, so clearly uniqueness holds.

Suppose we have uniqueness for all r with $\mu(r) < M$, and let $\mu(r) = M$; write $r = r_1 \cdots r_M$ for a (minimal length) factorization into irreducibles. By PC, the r_i are prime. If $r = s_1 \cdots s_N$ is another factorization into irreducibles, then $r_M \mid s_1 \cdots s_N \implies r_M \mid$ some s_j, say s_N. Since s_N is irreducible (and $r_M \notin R^*$), we get $s_N = r_M u$ (for some $u \in R^*$), i.e. $r_M \sim s_N$. But now $r' = (u^{-1} r_1) r_2 \cdots r_{M-1}$ has $\mu(r') < M$ and $r' = s_1 \cdots s_{N-1}$. By induction, $M - 1 = N - 1$ and (permuting factors if needed) $s_j \sim r_j$ ($j = 1, \ldots, M-1$) and we are done. $\square$

In particular, in a UFD, prime and irreducible elements are the same thing. So we get the following analogue of III.H.8:

III.I.13. COROLLARY. *Let R be a UFD, $\alpha \in R \backslash (R^* \cup \{0\})$. Then $R/(\alpha)$ is a domain $\iff$ α is irreducible.*

PROOF. Combine III.F.6 with the fact that (α) is prime iff α is. $\square$

III.I.14. EXAMPLES.
(A) All PIDs (and hence all Euclidean domains) are UFDs.
(B) $\mathbb{F}[x, y]$ and $\mathbb{Z}[x]$ are UFDs but (as we know) not PIDs.
(C) There is no number ring that is a UFD but not a PID.

We will prove (B) and (C) in §§III.K-III.L; for now, here is the

PROOF OF (A). Consider an ascending chain $I_1 \subseteq I_2 \subseteq \cdots$ in $\mathcal{PP}(R)$, and consider the ideal $J = \cup_{j \geq 1} I_j \subset R$. Since R is a PID, $J = (a)$ for some $a \in J$. But then $a \in I_n$ for some n, so $J = (a) \subset I_n$ $\implies I_m = I_n$ for all $m \geq n$. So DCC holds.

Next suppose that $a \in R$ is irreducible, and $a \mid bc$ but $a \nmid b$. Then $b \notin (a) \implies (a,b) \supsetneq (a)$. By (III.I.1), (a) is maximal in $\mathcal{PP}(R)$. Since R is a PID, (a,b) is principal. So $(a,b) = R$. It follows that there exist $p, q \in R$ such that $ap + bq = 1$; multiplying by c gives $apc + bcq = c$. Since $a \mid bc$, we therefore have $a \mid c$. Conclude that a is prime. So PC holds, and III.I.12 finishes the job. $\square$