NOTES FOR SECTION 2.6 OF ASH

SAM EVENS

1. Divisibility

The purpose of these notes is explain the proof that each principal ideal domain (PID) is a unique factorization domain (UFD).

Let R be an integral domain.

Remark 1.1. *Let $a, b, c \in R$ and suppose that $ab = ac$. If $a \neq 0$, then $b = c$. Indeed, $ab = ac$ implies $a(b - c) = 0$. Since R is an integral domain and $a \neq 0$, then $b - c = 0$, so $b = c$.*

Definition 1.2. *Let $a, b \in R$ with $a \neq 0$. We say a divides b if there is $c \in R$ such that $b = ac$. If so, we write $a \mid b$, and if not, we write $a \nmid b$.*

Note that if $a, b \in R$ are nonzero and $c \in R$, then $a \mid a$ and if $a \mid b$ and $b \mid c$, then $a \mid c$.

Lemma 1.3. *Let $a, b \in R$ with $a \neq 0$. Then $a \mid b$ if and only if $(b) \subset (a)$.*

The proof is an easy consequence of definitions.

Definition 1.4. *For $a, b \in R - \{0\}$, we say a and b are associates if there is a unit u of R so that $b = ua$.*

Lemma 1.5. *For $a, b \in R - \{0\}$, the following conditions are equivalent.*

(1) a and b are associates.

(2) $(a) = (b)$.

(3) $a \mid b$ and $b \mid a$.

Proof. We prove the equivalence of (1) and (3). If a and b are associates, then $b = ua$ for u a unit of R. Hence, there is $v \in R$ so $uv = 1$ and v is a unit of R. Hence, $vb = vua = a$. Thus, $a \mid b$ and $b \mid a$. Conversely, if $a \mid b$ and $b \mid a$, then $b = xa$ and $a = yb$ for $x, y \in R$. Thus, $b = xyb$, so $1b = xyb$. By Remark 1.1, $xy = 1$, so x is a unit, which establishes (1). The equivalence of (2) and (3) follows directly from Lemma 1.3.

Q.E.D.

Remark 1.6. *Let $a, b \in R$ with $a \neq 0$. Then if $a \mid b$, then $(b) \subset (a)$ with equality if and only if a and b are associates. Indeed, this follows from Lemma 1.3 and Lemma 1.5.*

Remark 1.7. *Let $a \in R$. Then $(a) = R$ if and only if a is a unit. Indeed, since $R = (1)$, $(a) = R$ if and only if $(a) = (1)$. By Remark 1.6, it follows easily that $(a) = (1)$ if and only if a is a unit.*

Definition 1.8. *Let $a \in R$ be nonzero, and assume a is not a unit. Then we say a is irreducible if whenever $a = bc$ for $b, c \in R$, then b or c is a unit.*

Notation 1.9. *If S and T are subsets of a set X, we write $S \subsetneq T$ if $S \subset T$ but $S \neq T$.*

Remark 1.10. *Let $a \in R$ be nonzero, and suppose $a = bc$ with $b, c \in R$ nonunits. Then $(a) \subsetneq (b)$, and similarly with b in place of c. Indeed, $b \mid a$, so by Remark 1.6, $(a) \subset (b)$ with equality if and only if a and b are associates. If a and b are associates, then $a = bu$ for a unit u, so $u = c$ by Remark 1.1, which contradicts our assumption. Thus, $(a) \subsetneq (b)$, and similarly $(a) \subsetneq (c)$.*

Definition 1.11. *Let $a \in R$ be a nonzero, nonunit. Then we say a is prime if whenever $a \mid bc$ for $b, c \in R$, then $a \mid b$ or $a \mid c$.*

Remark 1.12. *Let $a \in R$ be a nonzero, nonunit. Then a is prime if and only if (a) is a prime ideal. Indeed, let a be prime. Then by Remark 1.7, $(a) \neq R$, so (a) is a proper ideal. Let $bc \in (a)$ for $b, c \in R$. Then $a \mid bc$ by Lemma 1.3, so $a \mid b$ or $a \mid c$ since a is prime. Hence, by Lemma 1.3 again, $b \in (a)$ or $c \in (a)$, so (a) is prime. Conversely, let (a) be prime. Then if $a \mid bc$, then $bc \in (a)$ by Lemma 1.3, so $b \in (a)$ or $c \in (a)$ since (a) is prime, so $a \mid b$ or $a \mid c$ by Lemma 1.3 again.*

Proposition 1.13. *(Proposition 2.6.2 in Ash) Let $a \in R$. If a is prime, then a is irreducible.*

Proof. Let $a = b \cdot c$ with $b, c \in R$. Since $a \mid a$, we conclude that $a \mid b$ or $a \mid c$. If $a \mid b$, then $b = a \cdot x$ for some $x \in R$, so $a = a \cdot x \cdot c$, and since R is a domain, $x \cdot c = 1$, so c is a unit. Similarly, if $a \mid c$, then b is a unit. Hence, a is irreducible.

Q.E.D.

To prove the main theorem, we need to discuss greatest common divisors in PID's and Noetherian rings.

2. Greatest common divisors

We assume our ring R is a PID and discuss the notion of a greatest common divisor of two nonzero elements R. Let $a, b \in R$, not both zero, and consider the nonzero ideal $(a, b) = \{ra + sb : r, s \in R\}$. Since R is a PID, the ideal $(a, b) = (d)$ for some nonzero element $d \in R$. Since $a = 1 \cdot a + 0 \cdot b \in (a, b) = (d)$, we see that $d \mid a$. Similarly, $d \mid b$.

Definition 2.1. *For $a, b \in R$, not both zero, we say $d \in R$ is a greatest common divisor of a and b if $(a, b) = (d)$.*

Remark 2.2. *If $a, b, d \in R$ are as above, and $c \in R$ and $c \mid a$ and $c \mid b$, then $c \mid d$. Indeed, $c \mid a$ implies $a \in (c)$ and similarly, $b \in (c)$. Since $(d) = (a, b)$, then $d = ra + sb$ for some $r, s \in R$, so $d \in (c)$ and thus $c \mid d$. If d and d_1 are both greatest common divisors of a and b, then d is associate to d_1. Indeed, the assumption implies that $(d) = (d_1)$, so that d and d_1 are associates by Lemma 1.5 above.*

Lemma 2.3. *Let $a, p \in R$ with p irreducible.*

(i) if $p \mid a$, then $(a, p) = (p)$.

(ii) if $p \nmid a$, then $(a, p) = (1)$.

Proof. Let $(a, p) = (d)$. Then $d \mid p$. In case (i), $p \mid a$ so since $p \mid p$, then $p \mid d$ by Remark 2.2. Hence, $(p) = (d)$ by Lemma 1.5, so $(a, p) = (p)$. In case (ii), $p \nmid a$. Since $d \mid p$, $p = xd$ for some $x \in R$. Since p is irreducible, either d or x is a unit. If x were a unit, then p and d would be associate, so $(p) = (d) = (a, p)$, giving the contradiction $p \mid a$. Hence, d is a unit, so 1 and d are associates, and $(1) = (d)$, proving (ii).

Q.E.D.

Proposition 2.4. *Let R be a PID. If $p \in R$ is irreducible, then p is prime.*

Proof. Let $b, c \in$ and let $p \mid b \cdot c$. Suppose $p \nmid b$, and we show $p \mid c$, so p is prime.

Since $p \nmid b$, then by Lemma 2.3, $(1) = (b, p)$. Thus, $1 = xb + yp$ for some $x, y \in R$, so $c = xbc + ypc$. Since $p \mid bc$, $xbc \in (p)$. Since evidentally $ypc \in (p)$, then $c \in (p)$, so $p \mid c$.

Q.E.D.

3. Noetherian Rings

Definition 3.1. *Let R be a ring. We say R is Noetherian if for every chain*

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset I_{n+1} \subset \ldots$$

of ideals of R, there exists $n_0 \in \mathbf{Z}_{>0}$ such that for all $n > n_0$, then $I_{n_0} = I_n$.

Proposition 3.2. *Let R be a PID. Then R is Noetherian.*

Proof. Let $I_1 \subset I_2 \subset \cdots \subset I_n \subset \ldots$ be a chain of ideals of R. Let $I = \cup_{j \geq 1} I_j$. Then I is an ideal. Indeed, if $x, y \in I$, then $x \in I_r$ and $y \in I_s$ for some r, s. Let t be the maximum of r and s, so that $x, y \in I_t$. Thus, $x - y \in I_t$ since I_t is an ideal, so $x - y \in I$. Let $r \in R$. Then $rx \in I_r \subset I$, so I is an ideal.

Since R is a PID, the ideal $I = (a)$ for some $a \in R$. Since $a \in I$, we see $a \in I_{n_0}$ for some n_0. Thus, $I = (a) \subset I_{n_0} \subset I$, so $I = I_{n_0}$. Hence if $n > n_0$, then $I_n \subset I = I_{n_0} \subset I_n$, so $I_n = I_{n_0}$. Thus, R is Noetherian.

Q.E.D.

Lemma 3.3. *Let R be a Noetherian ring and let S be a nonempty collection of ideals of R. Then there exists $J \in S$ so that if $I \in S$ and $J \subset I$, then $J = I$, i.e., S has a maximal element.*

Note that the above ideal J need not be a maximal ideal of R. Indeed, if S consists only of the zero ideal (0), then (0) is evidentally maximal in S, but is a maximal ideal of R if and only if R is a field.

Proof. We argue by contradiction, so assume S has no maximal ideal. Choose $I_1 \in S$. Since I_1 is not maximal, there is an ideal $I_2 \in S$ so $I_1 \subsetneq I_2$. By induction, we construct a chain of ideals in S, $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_n$ for each n. Indeed, if such a sequence has been constructed, then since I_n is not maximal, there is an ideal $I_{n+1} \in S$ with $I_n \subsetneq I_{n+1}$. Thus, we can construct an infinite ascending chain of ideals in R, which contradicts the assumption that R is Noetherian.

Q.E.D.

4. Main Theorem

Definition 4.1. *Let R be an integral domain. R is called a unique factorization domain (UFD) if*

(UF1) If $a \in R$ is nonzero, then there is a product decomposition $a = up_1 \dots p_n$ for some $n \geq 0$, $u \in R^\times$, and $p_1, \dots, p_n$ irreducible;

(UF2) Suppose $a = up_1 \dots p_n$ as in (UF1) and also $a = vq_1 \dots q_m$ for some $m \geq 0$ with $v \in R^\times$ and $q_1, \dots, q_m$ irreducible. Then $n = m$, and after renumbering the q_j, we may assume p_i is associate to q_i for $i = 1, \dots, m$.

(UF1) guarantees existence of factorization into irreducibles, and (UF2) asserts that a factorization is essentially unique. If a is not a unit, then in (UF1), we can omit the unit u by absorbing it into the first irreducible factor.

Theorem 4.2. *If R is a PID, then R is a UFD.*

Proof. Since R is a PID, R is Noetherian by Proposition 3.2. Let S be the collection of ideals I of R such that $I = (a)$ for some $a \in R$ which cannot be written in the form $a = up_1 \dots p_n$ as in (UF1). We show that S is empty, and this proves (UF1) for R.

We argue by contradiction. If S is nonempty, then by Lemma 3.3, S has a maximal element $J = (a)$ such that a does not satisfy (UF1). Since a does not satisfy (UF1), then a is not irreducible, since if a were irreducible, $a = a$ would be a factorization as in (UF1). Thus, we can factor $a = bc$ with $b, c \in R$ non-units. Hence, by Remark 1.10, $(a) \subsetneq (b)$ and $(a) \subsetneq (c)$. Since (a) is maximal in S, it follows that neither (b) nor (c) is in S. Hence, b and c satisfy (UF1), so $b = ux_1 \dots x_s$ and $c = vy_1 \dots y_t$ with $u, v \in R^\times$ and $x_1, \dots, x_s, y_1, \dots, y_t$ irreducible. Hence, $a = bc = uvx_1 \dots x_s y_1 \dots y_t$ has a factorization

as in (UF1), which contradicts our assumption that a does not satisfy (UF1). Hence, S must be empty, so each nonzero $a \in R$ satisfies (UF1).

We now show (UF2). Let $a = up_1 \dots p_n = vq_1 \dots q_m$ with $u, v \in R^\times$ and $p_1, \dots, p_n, q_1, \dots, q_m$ irreducible. We prove by induction on the maximum t of m and n that $m = n$. If m or $n = 0$, then a is a unit, and the result is clear. Let $t > 0$ and assume WLOG that $t = n$. Then p_n divides a so p_n divides $vq_1 \dots q_m$. Since p_n is irreducible, then p_n is prime by Proposition 2.4. Since $p_n \mid vq_1 \dots q_m$, then by an easy induction, either $p_n \mid v$ or $p_n \mid q_j$ for some j with $1 \leq j \leq m$. If $p_n \mid v$, then since $v \mid 1$, we see that $p_n \mid 1$ using easy facts about divisibility. Thus, p_n is a unit, which is a contradiction. Hence, $p_n \mid q_j$ for some j, and by renumbering the q_i, we may assume $j = m$. Thus, $q_m = u_n p_n$ for some $u_n \in R$. Since q_m is irreducible, either u_n or p_n is a unit, so that u_n is a unit. Hence, p_n and q_m are associates. Thus, we see $a = up_1 \dots p_n = vq_1 \dots q_{m-1} u_n p_n$, so by Remark 1.1, $up_1 \dots p_{n-1} = wq_1 \dots q_{m-1}$ with $w = vu_n \in R^\times$. Thus, by induction, $n - 1 = m - 1$ and we can renumber the q_i so that q_i is associate to p_i for all i. Hence, (UF2) is satisfied.

Q.E.D.

5. Consequences

Proposition 5.1. *(Proposition 2.6.4 in Ash) Let R be a UFD. Then every irreducible element of R is prime.*

See the proof in Ash.

Theorem 5.2. *(Theorem 2.6.9 in Ash) Let R be an integral domain. Then R is a PID if and only if R is a UFD and every prime ideal of R is maximal.*

Proof. Assume R is a PID. By Theorem 4.2, R is a UFD. Let P be a prime ideal of R. Since R is a PID, $P = (\pi)$ for some $\pi \in R$. By Theorem 2.4.2 of Ash, there is a maximal ideal M of R with $P \subset M$, and as before $M = (q)$ for some $q \in R$. Thus, $\pi \in P \subset M = (q)$, so $q \mid \pi$. Thus, $\pi = u \cdot q$ for some $u \in R$. Since P is a prime ideal, the element π is a prime element by Remark 1.12, so π is irreducible by Proposition 1.13. Hence, u or q is a unit. If q were a unit, then $(q) = R$, so (q) would not be maximal. Hence, u is a unit, so π and q are associates, and thus $P = (\pi) = (q) = M$ by Lemma 1.5, so that P is maximal.

The converse is less important, and is proved in the exercises in Ash.

Q.E.D.

Department of Mathematics, University of Notre Dame, Notre Dame, IN, 46556
Email address: sevens@nd.edu