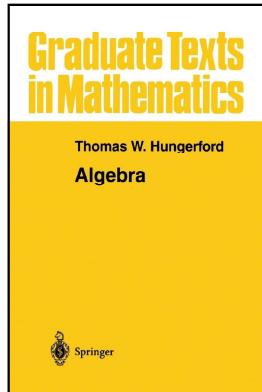


Modern Algebra

Chapter III. Rings

III.3. Factorization in Commutative Rings—Proofs of Theorems



Theorem III.3.4

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (i) p is prime if and only if (p) is a nonzero prime ideal.
- (ii) c is irreducible if and only if (c) is maximal in the set S of all proper principal ideals of R .
- (iii) Every prime element of R is irreducible.
- (iv) If R is a principal ideal domain, then p is prime if and only if p is irreducible.
- (v) Every associate of an irreducible (respectively, prime) element of R is irreducible (respectively, prime).
- (vi) The only divisors of an irreducible element of R are its associates and the units of R .

Theorem III.3.4 (continued 1)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (i) p is prime if and only if (p) is a nonzero prime ideal.

Proof. (i) Let p be prime. Since R is an integral domain then R is commutative with an identity, so p is in the center of R and by Theorem III.2.5(v), $(p) = \{rp \mid r \in R\}$. Let $ab \in (p)$. Then $ab = rp$ for some $r \in R$ and $p \mid ab$. Since p is prime then (by Definition III.3.3), either $p \mid a$ or $p \mid b$. But then either $a = r_1p$ or $b = r_2p$ for some $r_1, r_2 \in R$, which implies that either $a \in (p)$ or $b \in (p)$. By Theorem III.2.15, we have that principal ideal (p) is prime.

Let (p) be a nonzero prime ideal. Let $p \mid ab$. Then $ab = rp$ for some $r \in R$ and $ab \in (p)$. Since R is commutative, Theorem III.2.15 implies that either $a \in (p)$ or $b \in (p)$. So, by Theorem III.2.5(v), either $a = r_1p$ or $b = r_2p$; that is, either $p \mid a$ or $p \mid b$. Hence p is prime.

Theorem III.3.4 (continued 2)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (ii) c is irreducible if and only if (c) is maximal in the set S of all proper principal ideals of R .

Proof. (ii) Suppose c is irreducible. Then by definition, c is a nonunit and so by Theorem III.3.2(iv), (c) is a proper ideal of R (i.e., $(c) \neq R$). If $(c) \subset (d)$ then by Theorem III.3.2(i), $c = dx$ for some $x \in R$. Since c is irreducible then (by definition) either d is a unit or x is a unit. If d is a unit then by Theorem III.3.2(iv), $(d) = R$. If x is a unit then by Theorem III.3.2(vi), c and d are associates and then by Theorem III.3.2(ii), $(c) = (d)$. Hence (c) is maximal in the set of proper principal ideals of R .

Theorem III.3.4 (continued 3)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (ii) c is irreducible if and only if (c) is maximal in the set S of all proper principal ideals of R .

Proof (continued). (ii) Conversely, suppose (c) is maximal in set S . Then c is a nonzero nonunit in R by Theorem III.3.2(iv) since $(c) \neq R$. If $c = ab$ then $(c) \subset (a)$ by Theorem III.3.2(i), whence $(c) = (a)$ or $(a) = R$. If $(a) = R$ then a is a unit by Theorem III.3.2(iv). If $(c) = (a)$ then $a = cy$ (as in part (i) or by Theorem III.3.2(i)) and $c = ab = (cy)b = c(yb)$. Since R is an integral domain then by left cancellation (which holds by Lemma III.1.A) $1_R = yb$ whence b is a unit. Hence, either a is a unit or b is a unit, and c is irreducible.

Theorem III.3.4 (continued 5)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (iv) If R is a principal ideal domain, then p is prime if and only if p is irreducible.

Proof. (iv) Suppose R is a principal ideal domain. If p is irreducible then by (ii), (p) is maximal in the set of all proper principal ideals of R . Since R is a principal ideal domain then (by definition) every ideal is principal, so in fact (p) is maximal in R itself. Since R is an integral domain by hypothesis, then (by definition) R has an identity. So by Theorem III.2.19, (p) is prime. By (i), p is prime (notice that $p \neq 0$ since the definition of "irreducible" implies $p \neq 0$).

Conversely, suppose p is prime. Then by (iii) p is irreducible (all we need for this is the hypothesis that R is an integral domain).

Theorem III.3.4 (continued 4)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (iii) Every prime element of R is irreducible.

Proof. (iii) Let p be prime in R . If $p = ab$ then either $p \mid a$ or $p \mid b$. WLOG, say $p \mid a$. Then $a = px$ for some $x \in R$ and so $p = ab = pxb$. Since R is an integral domain (no zero divisors) then left cancellation holds (by Lemma III.1.A) and $1_R = xb$. Therefore b is a unit. So (by definition) p is irreducible.

Theorem III.3.4 (continued 6)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (v) Every associate of an irreducible (respectively, prime) element of R is irreducible (respectively, prime).

Proof. (v) Let c be irreducible and d an associate of c . Then by Theorem III.3.2(vi) $c = du$ where $u \in R$ is a unit. To show d is irreducible, suppose $d = ab$. Then $c = du = abu$, whence (since c is irreducible) either a or bu is a unit. But if bu is a unit then $(bu)v = 1$ for some $v \in R$ and so $b(uv) = 1$ and b is a unit. So either a or b is a unit and d is irreducible. Let c be prime and d an associate of c . Then by Theorem III.3.2(vi), $c = du$ where $u \in R$ is a unit. To show d is prime, suppose $d \mid ab$. Then $dx = ab$ for some $x \in R$. So $dux = abu$ or $cx = abu$. Since c is prime, either c divides a or c divides bu . If c divides a then $cy = a$ for some $y \in R$ and so $duy = (du)y = cy = a$ and d divides a . If c divides bu then $cz = bu$ for some $z \in R$, or $(du)z = bu$ or $dz = b$ (since u is a unit) and d divides b . So d is prime.

Theorem III.3.4 (continued 7)

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R .

- (vi) The only divisors of an irreducible element of R are its associates and the units of R .

Proof. (vi) Let c be irreducible and suppose a is a divisor of c : $a \mid c$. By Theorem III.3.2(i), $(c) \subset (a)$. By (ii), since c is irreducible, then (c) is maximal in the set of principal ideals of R . So it must be that either $(a) = (c)$ or $(a) = R$. If $(a) = (c)$ then a is an associate of c by Theorem III.3.2(ii). If $(a) = R$ then a is a unit by Theorem III.3.2(iv). So a is either an associate of c or a unit. That is, the divisors of c are its associates and the units of R , as claimed. \square

Lemma III.3.6

Lemma III.3.6. If R is a principal ideal ring and $(a_1) \subset (a_2) \subset \cdots$ is a chain of ideals in R , then for some positive integer n , $(a_j) = (a_n)$ for all $j \geq n$.

Proof. Let $A = \cup_i (a_i)$. We claim that A is an ideal. If $b, c \in A$, then $b \in (a_i)$ and $c \in (a_j)$ for some i, j . WLOG, say $i \geq j$. Consequently, $(a_j) \subset (a_i)$ and $b, c \in (a_i)$. Since (a_i) is an ideal then by Theorem III.2.2(i) $b - c \in (a_i) \subset A$. Similarly if $r \in R$ and $b \in A$ then $b \in (a_i)$ for some i , whence $rb \in (a_i) \subset A$ and $br \in (a_i) \subset A$ by Theorem III.2.2(ii). Then, Theorem III.2.2 implies that A is an ideal. Since R is a principal ideal ring (by definition, all ideals are principal) then A is principal, say $A = (a)$. Since $a \in A = \cup_i (a_i)$ then $a \in (a_n)$ for some n . By Definition III.2.4 (of a generating set of an ideal), $A = (a) \subset (a_n)$. Therefore, for every $j \geq n$ we have $A = (a) \subset (a_n) \subset (a_j) \subset A$ and whence $(a_j) = (a_n)$. \square

Theorem III.3.7

Theorem III.3.7. Every principal ideal domain R is a unique factorization domain. That is, “every PID is a UFD.”

Proof. Let S be the set of all nonzero nonunit elements of R which cannot be factored as a finite product of irreducible elements. We first show that S is empty (and so all nonzero nonunits have at least one factorization into irreducibles).

ASSUME S is not empty and $a \in S$. Then a is not a unit and by Theorem III.3.2(iv), $(a) \neq R$ is a proper ideal of R . By Theorem III.2.18, $(a) \subset (c)$ where (c) is some maximal ideal (since R is a principal ideal domain, by definition, all ideals are principal). By Theorem III.3.4(ii), c is irreducible. Since $(a) \subset (c)$ then by Theorem III.3.2(i), c divides a . So there is an irreducible c dividing a for any $a \in S$. Hence, by the AXIOM OF CHOICE, for each $a \in S$ there is an irreducible divisor c_a of a in R . Since $c_a \mid a$ then there exists a $x_a \in R$ such that $c_a x_a = a$. Since R is an integral domain it has no zero divisors and this x_a is unique ($c_a x_a = c_a y_a$ implies $c_a(x_a - y_a) = 0$ implies $x_a - y_a = 0$ since there are no zero divisors).

Theorem III.3.7 (continued 1)

Theorem III.3.7. Every principal ideal domain R is a unique factorization domain. That is, “every PID is a UFD.”

Proof (continued). We claim $x_a \in S$. First, ASSUME that x_a is a unit (in which case $x_a \notin S$ by the definition of S), then $a = c_a x_a$ implies by Theorem III.3.2(iv) that a and c_a are associates. Then by Theorem III.3.4(v), a is irreducible since c_a is irreducible. But then a is a finite product of irreducibles (namely, a itself) and so $a \notin S$, a CONTRADICTION. So x_a is not a unit. Let x_a be a nonunit and ASSUME $x_a \notin S$. Then x_a has a factorization as a product of irreducibles, whence a also does (just add irreducible c_a to the product), which implies that $a \notin S$, a CONTRADICTION. So it must be that $x_a \in S$.

Theorem III.3.7 (continued 2)

Proof (continued). Furthermore, we claim that (a) is properly contained in (x_a) . Since $x_a \mid a$ then by Theorem III.3.2(i) we have $(a) \subset (x_a)$. ASSUME $(a) = (x_a)$. Then by Theorem III.3.2(ii), a and x_a are associates and by Theorem III.3.2(vi) (since R is an integral domain) $x_a = ay$ for some unit $y \in R$, whence $a = x_a c_a = a y c_a$ and $1 = y c_a$ (cancellation holds in an integral domain by Lemma III.1.A). But then c_a is a unit, a CONTRADICTION since c_a is irreducible (and by definition, “irreducibles” are nonunits). Therefore, $(a) \subsetneq (x_a)$. We now define $f : S \rightarrow S$ as $f(a) = x_a$ where x_a is described above (and f is well-defined since x_a is uniquely determined by c_a ; but the Axiom of Choice is required to get c_a). For each $n \in \mathbb{N} \cup \{0\}$, define $f_n = f$. Then by the Recursion Theorem (Theorem 0.6.2) there exists a function $\varphi : \mathbb{N} \cup \{0\} \rightarrow S$ such that $\varphi(0) = a$ and $\varphi(n+1) = f_n(\varphi(n)) = f(\varphi(n)) = x_{\varphi(n)}$ (this last one from the definition of f) for all $n \in \mathbb{N} \cup \{0\}$.

Theorem III.3.7 (continued 3)

Proof (continued). Denote $\varphi(n) \in S$ as a_n and then we have the sequence $a_0 = a, a_1, a_2, \dots$ such that (since $\varphi(n+1) = x_{\varphi(n)}$): $a_1 = x_a; a_2 = x_{a_1}; a_3 = x_{a_2}; \dots; a_{n+1} = x_{a_n}; \dots$. Consequently, since from the previous paragraph $(a) \subsetneq (x_a)$, we have $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$, but this CONTRADICTS Lemma III.3.6, so the assumption that S is not empty is false, and so $S = \emptyset$. That is, every nonzero nonunit in R has a factorization as a finite product of irreducibles and (i) of the definition on UFD follows.

Finally, if $c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m$ are two factorizations of an element of R into a product of irreducibles, then c_1 is prime by Theorem III.3.4(iv) and so (by definition of prime, and some induction) c_1 divides some d_i . Since d_i is irreducible, then by Theorem III.3.4(vi) c_1 and d_i are associates (since c_1 is irreducible, it is not a unit).

Theorem III.3.7 (continued 4)

Theorem III.3.7. Every principal ideal domain R is a unique factorization domain. That is, “every PID is a UFD.”

Proof (continued). By Theorem III.3.2(vi), we then have that $c_1 = d_i r_1$ for some unit $r_1 \in R$ (R is given to be an integral domain). So $c_1 c_2 \cdots c_n = d_1 d_2 \cdots d_m$ implies that $(d_i r_1) c_2 c_3 \cdots c_n = d_1 d_2 \cdots d_i \cdots d_m$ or $r_1 c_2 c_3 \cdots c_n = d_1 d_2 \cdots d_{i-1} d_{i+1} \cdots d_m$. (WLOG $n \leq m$.) Then we similarly have that $r_1 r_2 \cdots r_m = \underbrace{d_\alpha d_\beta \cdots d_\omega}_{m-n \text{ factors}}$.

ASSUME $m - n > 0$. Then we can reverse the argument above and use the facts that d_α is prime (Theorem III.3.4(iv)) and d_α divides $r_1 r_2 \cdots r_m$ to see that d_α must divide some unit r_j . But then $d_\alpha x = r_j$ for some $x \in R$. But since r_j is a unit, then $d_\alpha (x r_j^{-1}) = 1$ (integral domains have 1) and so d_α is a unit, CONTRADICTING the fact that d_α is irreducible and hence is not a unit (by the definition of “irreducible”). So $m - n = 0$, $m = n$, and (ii) of the definition of UFD holds. \square

Theorem III.3.9

Theorem III.3.9. Every Euclidean ring R is a principal ideal ring with identity. Consequently every Euclidean domain is a unique factorization domain.

Proof. If I is a nonzero ideal in R , choose $a \in I$ such that $\varphi(a)$ is the least nonnegative integer in the set $\{\varphi(x) \mid x \neq 0; x \in I\}$ (where $\varphi : R \setminus \{0\} \rightarrow \mathbb{N}$ as described in Definition III.3.8; so a is a “ φ -least nonzero element of I ”). If $b \in I$ then $b = qa + r$ for some $q, r \in R$ with either $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(a)$ (by part (ii) of Definition III.3.8). Since $b \in I$ and $qa \in I$ (I is an ideal), then $r = b - qa \in I$. Since $\varphi(a)$ is minimal as chosen, then we cannot have $\varphi(r) < \varphi(a)$ if $r \neq 0$, and so it must be that $r = 0$ (that is, $r \in I$ but $r \notin \{x \in I \mid x \neq 0\}$; the x 's for which we consider $\varphi(x)$ above). Whence $b = qa$ and a divides b . Therefore, every element of I is a multiple of a . So $I \subset Ra$.

Theorem III.3.9 (continued)

Proof (continued). Since Euclidean ring R is a commutative ring, a is in the center of R and so by Theorem III.2.5(iii), $Ra \subset (a)$. Since $a \in I$, then $(a) \subset I$. So we have $I \subset Ra \subset (a) \subset I$. Therefore $I = Ra = (a)$ and arbitrary ideal I of R is principal. So R is a principal ideal ring.

In the previous paragraph, we showed that any nonzero ideal I satisfies $I = Ra = (a)$. Since R itself is a nonzero ideal of R , then we have $R = Ra = (a)$ for some $a \in R$. Consequently, for some $e \in R$ we have $a = ea = ae$. If $b \in R = Ra$ then $b = xa$ for some $x \in R$. Therefore, $be = (xa)e = x(ae) = xa = b$, whence e is a multiplicative identity element for R .

In the first paragraph we have that a Euclidean ring is a principal ideal ring. By Theorem III.3.7, every principal ideal domain is a unique factorization domain. “Whence” every Euclidean domain is a unique factorization domain. \square

Theorem III.3.11

Theorem III.3.11. Let a_1, a_2, \dots, a_n be elements of a commutative ring R with identity.

- (i) $d \in R$ is a greatest common divisor of $\{a_1, a_2, \dots, a_n\}$ such that $d = r_1a_1 + r_2a_2 + \dots + r_na_n$ for some $r_i \in R$ if and only if $(d) = (a_1) + (a_2) + \dots + (a_n)$.
- (ii) If R is a principal ideal ring, then a greatest common divisor of a_1, a_2, \dots, a_n exists and every one is of the form $r_1a_1 + r_2a_2 + \dots + r_na_n$, where each $r_i \in R$.
- (iii) If R is a unique factorization domain, then there exists a greatest common divisor of a_1, a_2, \dots, a_n .

Proof. (i) Suppose $d = r_1a_1 + r_2a_2 + \dots + r_na_n$ is a greatest common divisor of $\{a_1, a_2, \dots, a_n\}$. Then by Definition III.3.10(i), $d \mid a_1, d \mid a_2, \dots, d \mid a_n$ and so by Theorem III.3.2(i), $(a_1) \subset (d), (a_2) \subset (d), \dots, (a_n) \subset (d)$.

Theorem III.3.11 (continued 1)

Theorem III.3.11. Let a_1, a_2, \dots, a_n be elements of a commutative ring R with identity.

- (i) $d \in R$ is a greatest common divisor of $\{a_1, a_2, \dots, a_n\}$ such that $d = r_1a_1 + r_2a_2 + \dots + r_na_n$ for some $r_i \in R$ if and only if $(d) = (a_1) + (a_2) + \dots + (a_n)$.

Proof (continued). (i) Since (d) is an ideal it is closed under addition and so $(a_1) + (a_2) + \dots + (a_n) \subset (d)$. But $d = r_1a_1 + r_2a_2 + \dots + r_na_n \in (a_1) + (a_2) + \dots + (a_n)$. So $(a_1) + (a_2) + \dots + (a_n)$ is an ideal (Theorem III.2.6(i)) containing d and so $(d) \subset (a_1) + (a_2) + \dots + (a_n)$. Therefore $(d) = (a_1) + (a_2) + \dots + (a_n)$. Now suppose $(d) = (a_1) + (a_2) + \dots + (a_n)$. Since R has an identity and a_1, a_2, \dots, a_n are in the center of R (since R is commutative), by Theorem III.2.5(v) we have that $(a_i) = a_iR = Ra_i$ for each a_i . Also, $d \in (d)$ by Theorem III.2.5(iv), so $d = r_1a_1 + r_2a_2 + \dots + r_na_n$ for some $r_i \in R$. Now $(d) = (a_1) + (a_2) + \dots + (a_n)$ implies that each $(a_i) \subset (d)$ and so by Theorem III.3.2(i), $d \mid a_i$ for each a_i . So d is a divisor of each a_i .

Theorem III.3.11 (continued 2)

Theorem III.3.11. Let a_1, a_2, \dots, a_n be elements of a commutative ring R with identity.

- (i) $d \in R$ is a greatest common divisor of $\{a_1, a_2, \dots, a_n\}$ such that $d = r_1a_1 + r_2a_2 + \dots + r_na_n$ for some $r_i \in R$ if and only if $(d) = (a_1) + (a_2) + \dots + (a_n)$.

Proof (continued). (i) Suppose now that c also divides each a_i : $c \mid a_i$ for each a_i . Then Theorem III.3.2(i) implies that $(a_i) \subset (c)$ for each a_i . But then $(d) = (a_1) + (a_2) + \dots + (a_n) \subset (c)$ (since (c) is an ideal and hence closed under addition) and again by Theorem III.3.2(i) we have that $c \mid d$. Therefore, by Definition III.3.10, d is the greatest common divisor of a_1, a_2, \dots, a_n .

Theorem III.3.11 (continued 3)

Theorem III.3.11. Let a_1, a_2, \dots, a_n be elements of a commutative ring R with identity.

- (ii) If R is a principal ideal ring, then a greatest common divisor of a_1, a_2, \dots, a_n exists and every one is of the form $r_1 a_1 + r_2 a_2 + \dots + r_n a_n$, where each $r_i \in R$.

Proof. (ii) Suppose R is a principal ideal ring and let $a_1, a_2, \dots, a_n \in R$. By Theorem III.2.6(i), $(a_1) + (a_2) + \dots + (a_n)$ is an ideal of R . Since R is a principal ideal ring, then $(a_1) + (a_2) + \dots + (a_n) = (d)$ for some $d \in R$. By (i), we have that d is a greatest common divisor of a_1, a_2, \dots, a_n and is of the form $d = r_1 a_1 + r_2 a_2 + \dots + r_n a_n$.

Theorem III.3.11 (continued 4)

Theorem III.3.11. Let a_1, a_2, \dots, a_n be elements of a commutative ring R with identity.

- (iii) If R is a unique factorization domain, then there exists a greatest common divisor of a_1, a_2, \dots, a_n .

Proof. (iii) Suppose R is a unique factorization domain. Then for each a_i we have $a_i = c_1^{m_{i1}} c_2^{m_{i2}} \dots c_t^{m_{it}}$ for distinct irreducible c_k 's and with each $m_{ij} \geq 0$ (we get the c_k 's for each a_i and then use exponents of 0 as necessary). Then $d = c_1^{k_1} c_2^{k_2} \dots c_t^{k_t}$ where $k_j = \min\{m_{1j}, m_{2j}, \dots, m_{nj}\}$ is a divisor of each a_1, a_2, \dots, a_n .

Let c be a divisor of each a_i . Write c in terms of irreducibles d_i : $c = d_1 d_2 \dots d_\ell$, which can be done since R is a unique factorization domain. Since $c = d_1 d_2 \dots d_\ell$ divides $a_i = c_1^{m_{i1}} c_2^{m_{i2}} \dots c_t^{m_{it}}$, then each d_j divides a_i . Now each of the c_i 's are irreducible (and so are not units by definition), so $d_j \mid a_i$ implies that irreducible $d_j = c_i$ for some c_i .

Theorem III.3.11 (continued 5)

Theorem III.3.11. Let a_1, a_2, \dots, a_n be elements of a commutative ring R with identity.

- (iii) If R is a unique factorization domain, then there exists a greatest common divisor of a_1, a_2, \dots, a_n .

Proof (continued). (iii) Hence $c = c_1^{n_1} c_2^{n_2} \dots c_t^{n_t}$ for some $n_i \geq 0$. If each $n_i \leq k_i$ then $c \mid d$. ASSUME $n_{i^*} > k_{i^*}$ for some i^* . Then there is an a_i where $a_i = c_1^{m_{i1}} c_2^{m_{i2}} \dots c_{i^*}^{k_{i^*}} \dots c_t^{m_{it}}$ and c does not divide this a_i , a CONTRADICTION. So each $n_i \leq k_i$ and $c \mid d$. That is, d is a greatest common divisor. \square