Basic ring theory

written by Night Shift in Math on Functor Network
original link: https://functor.network/user/854/entry/409

Definition 1. *A ring is a nonempty set R together with two binary operations $(+, \cdot)$ such that*

(i) $(R, +)$ *is an abelian group*

(ii) $\forall a, b, c \in R, (ab)c = a(bc)$

(iii) $\forall a, b, c \in R, a(b + c) = ab + ac, \quad (a + b)c = ac + bc$

If in addition, multiplication is commutative, R is said to be a commutative ring. If R contains a multiplicative identity element 1_R, then R is said to be a ring with identity. The additive identity element of a ring is called the zero element, denoted 0.

Theorem 1. *Let R be a ring. Then $\forall a, b, a_i, b_j \in R, n \in \mathbb{Z}$,*

(i) $0a = a0 = 0$

(ii) $(-a)b = a(-b) = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) $(na)b = a(nb) = n(ab)$

(v) $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$

Definition 2. *A nonzero element a in a ring R is said to be a left (resp. right) zero divisor if there exists a nonzero $b \in R$ such that $ab = 0$ (resp. $ba = 0$). A zero divisor is an element of R which is both a left and right zero divisor.*

It is easy to verify that a ring R has no zero divisors iff the left and right cancellation laws hold in R.

Definition 3. *An element a in a ring R is said to be left invertible iff $\exists c \in R, ca = 1_R$. Right invertible iff $\exists c \in R, ac = 1_R$. The element c is called a left inverse or right inverse of a. An element $a \in R$ that is both left and right invertible is said to be invertible or a unit.*

The set of units forms a group under multiplication.

Definition 4. *A commutative ring R with identity $1_R \neq 0$ and no zero divisors is called an integral domain. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is called a division ring. A field is a commutative division ring.*

Theorem 2. *Let R be a ring with identity, n a positive integer, and $a, b, a_1, a_2, \cdots, a_s, b_1, b_2, \cdots, b_n \in R$.*

(i) If $ab = ba$, then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

(ii) If $a_i a_j = a_j a_i$ for all i, j, then

$$\left(\sum_{i=1}^{s} a_i \right)^n = \sum_{i_1, i_2, \cdots, i_s} \frac{n!}{(i_1)!(i_2)! \cdots (i_s)!} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$$

Where the sum is over nonnegative integers such that $\sum_{j=1}^{s} i_j = n$.

Proof. Use that $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ for $k < n$. Use induction. □

Definition 5. *Let R and S be rings. A function $f : R \to S$ is a homomorphism of rings provided that $\forall a, b \in R, f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$. The kernel of f is $\ker f = \{r \in R \mid f(r) = 0\}$. The image of f is $\operatorname{Im} f = \{s \in S \mid \exists r \in R, s = f(r)\}$. We do not require that a homomorphism of rings maps 1_R to 1_S.*

Definition 6. *Let R be a ring. If there is a least positive integer n such that $\forall a \in R, na = 0$, then R is said to have characteristic n. If no such n exists, R is said to have characteristic zero.*

Theorem 3. *Let R be a ring with identity 1_R and characteristic $n > 0$.*

(i) If $\phi : \mathbb{Z} \to R$ is given by $m \mapsto m1_R$, then ϕ is a homomorphism of rings with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$

(ii) n is the least positive integer such that $n1_R = 0$.

(iii) If R has no zero divisors, then n is prime.

Proof. (ii). If k is the least positive integer such that $k1_R = 0$, $\forall a \in R, ka = k(1_R a) = 0$.
(iii). If $n = kr$, $1 < k, r < n$, then $0 = n1_R = (k1_R)(r1_R)$ implies that $k1_R = 0$ or $r1_R = 0$, a contradiction. □

Theorem 4. *Every ring R may be embedded in a ring S with identity. The ring S may be chosen to be characteristic zero or the same characteristic as R.*

Proof. Let $S = R \oplus \mathbb{Z}$ and define multiplication in S by

$$(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, k_1 k_2)$$

S is a ring with identity $(0, 1)$ and characteristic zero and the map $R \to S$ given by $r \mapsto (r, 0)$ is a ring monomorphism. If $\operatorname{char} R = n > 0$, use a similar proof with $S = R \oplus \mathbb{Z}_n$ and multiplication defined by

$$(r_1, \bar{k}_1)(r_2, \bar{k}_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, \bar{k}_1 \bar{k}_2)$$

Then $\operatorname{char} S = n$. □

Definition 7. *Let R be a ring and S a nonempty subset of R that is closed under addition and multiplication in R. If S is itself a ring under these operations, then S is called a subring of R. A subring I of a ring R is a left ideal provided that*

$$r \in R, x \in I \implies rx \in I$$

I is a right ideal provided that

$$r \in R, x \in I \implies xr \in I$$

I is an ideal iff it is both a left and right ideal.

If R is any ring, the center of R is the set $C = \{c \in R \mid \forall r \in R, cr = rc\}$. C is easily a subring of R but may not be an ideal. A left ideal I of R that is not 0 or R is called a proper left ideal. Observe that if R has an identity 1_R and I is an ideal of R, $I = R$ iff $1_R \in I$. A nonzero ideal I of R is proper iff I contains no units of R. A division ring D has no proper left or right ideals since every nonzero element of D is a unit. The ring of $n \times n$ matrices over a division ring has proper left and right ideals, but no proper ideals.

Theorem 5. *A nonempty subset I of a ring R is a left [resp. right] ideal iff $\forall a, b \in I, \forall r \in R$,*

(i) $a, b \in I \implies a - b \in I$

(ii) $a \in I, r \in R \implies ra \in I$ *[resp.* $ar \in I$*]*

Corollary 1. *Let $\{A_i \mid i \in I\}$ be a family of left ideals in a ring R. Then $\bigcap_{i\in I} A_i$ is a left ideal.*

Definition 8. *Let X be a subset of a ring R. Let $\{A_i \mid i \in I\}$ be the family of all [left] ideals in R which contain X. Then $\bigcap_{i\in I} A_i$ is called the [left] ideal generated by X. This ideal is denoted (X).*

The elements of X are called generators of the ideal (X). If $X = \{x_1, x_2, \cdots, x_n\}$ then the ideal (X) is denoted $(x_1, x_2, \cdots, x_n)$ and said to be finitely generated. An ideal (x) generated by a single element is called a principal ideal. A principal ideal ring is a ring in which every ideal is principal. A principal ideal domain is an integral domain and a principal ideal ring.

Theorem 6. *Let R be a ring, $a \in R$ and $X \subseteq R$.*

(i) $(a) = \{ra + as + na + \sum_{i=1}^{m} r_i a s_i \mid r, s, r_i, s_i \in R, n \in \mathbb{Z}\}$

(ii) If R has an identity, then $(a) = \{\sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, n \in \mathbb{N}\}$

(iii) If a is in the center of R, then $(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$

(iv) $Ra = \{ra \mid r \in R\}$ *is a left ideal in R which may not contain a.*

(v) If R has an identity and a is in the center of R, then $Ra = (a) = aR$.

(vi) If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums $r_1a_1 + \cdots + r_na_n, r_i \in R, a_i \in X$.

Let $A_1, A_2, \cdots, A_n$ be nonempty subsets of a ring R. Denote by $A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i\}$. If A and B are nonempty subsets of R let AB denote $\{a_1b_1 + \cdots + a_nb_n \mid n \in \mathbb{N}, a_i \in A, b_i \in B\}$. More generally, let $A_1A_2 \cdots A_n$ denote the set of all finite sums of the form $a_1a_2 \cdots a_n$. In the special case when all are the same set A, denote it by A^n.

Theorem 7. *Let $A, A_1, A_2, \cdots, A_n, B, C$ be [left] ideals in a ring R.*

(i) $A_1 + A_2 + \cdots + A_n$ and $A_1A_2 \cdots A_n$ are [left] ideals

(ii) $(A + B) + C = A + (B + C)$

(iii) $(AB)C = ABC = A(BC)$

(iv)

$$B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$$
$$(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$$

Let R be a ring and I an ideal of R. Since the additive group of R is abelian, I is a normal subgroup. R/I is a well-defined quotient group.

Theorem 8. *Let R be a ring, I an ideal of R. The additive quotient group R/I with mulitplication given by $(a+I)(b+I) = ab+I$ is a ring. If R is commutative or has an identity, the same is true of R/I.*

Isomorphism theorems also exist for rings.

Theorem 9. *If $f : R \to S$ is a homomorphism of rings, then the kernel of f is an ideal in R. Conversely, if I is an ideal in R, then the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is an epimorphism of rings with kernel I.*

Proof. $\ker f$ is an additive subgroup of R. If $x \in \ker f, r \in R, f(rx) = f(r)f(x) = f(r)0 = 0$ whence $rx \in \ker f$. Thus $\ker f$ is an ideal. π is an epimorphism of groups with kernel I. $\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b)$. π is also an epimorphism of rings. □

Theorem 10. *If $f : R \to S$ is a homomorphism of rings and I is an ideal of R contained in the kernel of f, then there is a unique homomorphism of rings $\bar{f} : R/I \to S$ such that $\bar{f}(a + I) = f(a)$ for all $a \in R$. $\operatorname{im} \bar{f} = \operatorname{im} f$ and $\ker f = \ker \bar{f} = \ker f/I$. $\bar{f}$ is an isomorphism iff f is an epimorphism and $I = \ker f$.*

Proof. Let $b \in a + I$. Then $b - a \in I$ and $f(b) = f(b - a + a) = f(a)$. Thus f has the same effect on every element of $a + I$. The map $\bar{f} : R/I \to S$ defined by $\bar{f}(a+I) = f(a)$ is well-defined. Since f is a homomorphism, $\bar{f}$ is easily shown to be a homomorphism of rings. $\bar{f}$ is unique since it is completely determined by f. Clearly $\operatorname{im} \bar{f} = \operatorname{im} f$ and $a + I \in \ker \bar{f}$ iff $a \in \ker f$. $\ker \bar{f} = \ker f/I$. $\bar{f}$ is an epimorphism iff f is an epimorphism. $\bar{f}$ is a monomorphism iff $I = \ker f$. □

Corollary 2 (First Isomorphism theorem)**.** *If $f : R \to S$ is a homomorphism of rings, then f induces an isomorphism of rings $R/\ker f \cong \operatorname{im} f$.*

Corollary 3. *If $f : R \to S$ is a homomorphism of rings, I an ideal of R and J an ideal of S such that $f(I) \subseteq J$, then f induces a homomorphism of rings $\bar{f} : R/I \to S/J$ given by $a + I mapsto f(a) + J$. $\bar{f}$ is an isomorphism iff $\operatorname{im} f + J = S$ and $f^{-1}(J) \subseteq I$. In particular, if f is an epimorphism such that $f(I) = J$ and $\ker f \subseteq I$, then $\bar{f}$ is an isomorphism.*

Proof. $\pi \circ f : R \to S/J$ is a homomorphism of rings and $I \subseteq f^{-1}(J) = \ker(\pi \circ f)$. There is a unique homomorphism of rings $\bar{f} : R/I \to S/J$ such that $\bar{f}(a + I) = f(a) + J$. $\operatorname{im} \bar{f} = \operatorname{im}(\pi \circ f)$, $\ker \bar{f} = \ker(\pi \circ f)/I$. $\operatorname{im} \bar{f} = S/J$ iff $\operatorname{im} f + J = S$. $\ker \bar{f} = 0$ iff $\ker(\pi \circ f) = I$ iff $f^{-1}(J) \subseteq I$. Note that $f(I) = J$ and $\ker f \subseteq I$ implies $f^{-1}(J) \subseteq I$. □

Theorem 11. *(i) Isomorphism of rings $I/(I \cap J) \cong (I + J)/J$*

(ii) If $I \subseteq J$, then J/I is an ideal in R/I and there is an isomorphism of rings $(R/I)/(J/I) \cong R/J$.

(i) is the second isomorphism theorem and (ii) is the third isomorphism theorem.

Theorem 12 (Fourth isomorphism theorem)**.** *If I is an ideal in a ring R, then there is a one-to-one correspondence between the set of all ideals of R which contain I and the set of all ideals of R/I, given by $J \mapsto J/I$.*

Definition 9. *An ideal P in a ring R is said to be prime iff $P \neq R$ and for any ideals A, B in R*

$$AB \subset P \implies A \subseteq P \vee B \subseteq P$$

Theorem 13. *If P is an ideal in a ring R such that $P \neq R$ and $\forall a, b \in R$*

$$ab \in P \implies a \in P \vee b \in P$$

then P is prime. Conversely, if P is prime and R is commutative, then P satisfies the above condition.

Proof. Suppose A and B are ideals such that $AB \subseteq P$ and $\exists a \in A \setminus P$. $\forall b \in B, ab \in AB \subseteq P$ whence $a \in P$ or $b \in P$. Thus $b \in P$ so $B \subseteq P$ and P is prime. Conversely, if P is a prime ideal, R is commutative, and $ab \in P$, then $(ab) \subseteq P$. Note that $(a)(b) \subseteq (ab)$ whence $(a)(b) \subseteq P$. Either $(a) \subseteq P$ or $(b) \subseteq P$, whence $a \in P$ or $b \in P$. □

Theorem 14. *In a commutative ring R, with identity $1_R \neq 0$ an ideal P is prime iff R/P is an integral domain.*

Proof. If P is prime, since $P \neq R$, $1_R + P \neq P$. R/P has no zero divisors since $(a+P)(b+P) = P$ implies $ab \in P$ implies $a \in P$ or $b \in P$ implies $a+P = P$ or $b+P = P$. Therefore R/P is an integral domain. If R/P is an integral domain, then $1_R + P \neq 0 + P$ whence $1_R \notin P$. Thus $P \neq R$. Also, $ab \in P$ implies $(a+P)(b+P) = P$ implies $a \in P$ or $b \in P$. □

Definition 10. *An ideal [resp. left] M in a ring R is said to be maximal iff $M \neq R$ and for every [resp. left] ideal N such that $M \subseteq N \subseteq R$, either $M = N$ or $N = R$.*

Theorem 15. *In a nonzero ring R with identity, maximal [left] ideals will always exist. In fact every [left] ideal in R except R is contained in some maximal [left] ideal.*

Theorem 16. *If R is a commutative ring such that $R^2 = R$, then every maximal ideal M in R is prime.*

Proof. Suppose $ab \in M$ but $a \notin M, b \notin M$. $M + (a)$ and $M + (b)$ properly contains M. By maximality, $M + (a) = R = M + (b)$. Since R is commutative and $ab \in M$, $(a)(b) \subseteq (ab) \subseteq M$.

$$R = R^2 = (M + (a))(M + (b)) = M^2 + (a)M + M(b) + (a)(b) \subseteq M$$

This contradicts that $M \neq R$. Thus $a \in M$ or $b \in M$, whence M is prime. □

In particular, $R^2 = R$ whenever R has an identity.

Theorem 17. *Let M be an ideal in a ring R with identity $1_R \neq 0$.*

(i) If M is maximal and R is commutative, then R/M is a field.

(ii) If R/M is a division ring, then M is maximal.

Proof. (i). If M is maximal, then M is prime. Whence R/M is an integral domain. We must show if $a + M \neq M$, $a + M$ has a multiplicative inverse in R/M. M is properly contained in $M + (a)$.Since M is maximal, $M + (a) = R$. $1_R = m + ra$ for some $m \in M$, $r \in R$. $1_R - ra = m \in M$.

$$1_R + M = ra + M = (r + M)(a + M)$$

Thus $r + M$ is a multiplicative inverse of $a + M$ in R/M.
(ii). If R/M is a division ring, then $1_R + M \neq M$ whence $1_R \notin M$ and $M \neq R$. If N is an ideal such that $M \subset N$, let $a \in N \setminus M$. $a + M$ has a multiplicative inverse say $b + M$. $ab + M = 1_R + M$. $ab - 1_R \in M$. But $a \in N$ and $M \subset N$ implies that $1_R \in N$. Thus $N = R$. Therefore M is maximal. □

Corollary 4. *The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent:*

(i) R is a field.

(ii) R has no proper ideals.

(iii) 0 is a maximal ideal in R

(iv) Every nonzero homomorphism of rings $R \to S$ is a monomorphism.

Proof. $R \cong R/0$ is a field iff 0 is maximal. 0 is maximal iff R has no proper ideals. □

Theorem 18. *Let $A_1, A_2, \cdots, A_n$ be ideals in a ring R such that*

(i) $A_1 + A_2 + \cdots + A_n = R$

(ii) $\forall 1 \leq k \leq n$, $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots + A_n) = 0$

Then $R \cong A_1 \times A_2 \times \cdots \times A_n$.

Let A be an ideal and $a, b \in R$. a is said to be congruent to b modulo A denoted $a \equiv b \pmod{A}$ iff $a - b \in A$.

Theorem 19 (Chinese remainder theorem)**.** *Let $A_1, A_2, \cdots, A_n$ be ideals in a ring R such that $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$. If $b_1, b_2, \cdots, b_n \in R$ then there exists $b \in R$ such that*

$$\forall i, b \equiv b_i \pmod{A_i}$$

Furthermore b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Proof. Since $A_1 + A_2 = R$ and $A_1 + A_3 = R$,

$$R^2 = (A_1 + A_2)(A_1 + A_3) \subseteq A_1 + A_2 A_3 \subseteq A_1 + A_2 \cap A_3$$

Since $R = A_1 + R^2$, $R = A_1 + R^2 \subseteq A_1 + A_2 \cap A_3 \subseteq R$. Thus $R = A_1 + A_2 \cap A_3$. Assume that $R = A_1 + A_2 \cap A_3 \cap \cdots \cap A_{k-1}$. Then $R^2 = (A_1 + A_2 \cap A_3 \cap \cdots \cap A_{k-1})(A_1 + A_k) \subseteq A_1 + A_2 \cap A_3 \cap \cdots \cap A_k$ and hence $R = R^2 + A_1 \subseteq A_1 + A_2 \cap \cdots \cap A_k \subseteq R$. Thus $R = A_1 + A_2 \cap \cdots \cap A_k$ and the induction step is proved. $R = A_1 + A_2 \cap A_3 \cap \cdots \cap A_n$. Similarly, $R = A_k + \bigcap_{i \neq k} A_i$. Thus $\exists a_k \in A_k, r_k \in \bigcap_{i \neq k} A_i$ such that $b_k = a_k + r_k$. Note that $r_k \equiv b_k \pmod{A_k}$ and $r_k \equiv 0 \pmod{A_i}$ for $i \neq k$. Let $b = r_1 + r_2 + \cdots + r_n$. Verify that $bequivb_k$ (mod A_k). Finally, if $c \in R$ is such that $c \equiv b_i \pmod{A_i}$ for each i, then $b \equiv c \pmod{A_i}$ for each i. Whence $b - c \in \bigcap_{i=1}^{n} A_i$. □

Corollary 5. *If $A_1, A_2, \cdots, A_n$ are ideals in a ring R, then there is a monomorphism of rings*

$$\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$$

If $R^2 + A_i = R$ for all i and for $i \neq j$, $A_i + A_j = R$, then θ is an isomorphism.

Proof. Let $\pi_i : R \to R/A_i$ be the canonical epimorphism. The π_i induces a homomorphism $\theta_1 : R \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$ with $\theta_1(r) = (r + A_1, r + A_2, \cdots, r + A_n)$. $\ker \theta_1 = A_1 \cap A_2 \cap \cdots \cap A_n$. Thus θ_1 induces a monomorphism $\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$. If the hypotheses of the Chinese remainder theorem are satisfied, for $(b_1 + A_1, b_2 + A_2, \cdots, b_n + A_n) \in R/A_1 \times R/A_2 \times \cdots \times R/A_n$, there exists $b \in R$ such that $b \equiv b_i \pmod{A_i}$ for all i. Thus $\theta(b + \bigcap_{i=1}^n A_i) = (b + A_1, b + A_2, \cdots + b + A_n) = (b_1 + A_1, b_2 + A_2, \cdots, b_n + A_n)$. Whence θ is an isomorphism. $\square$

Definition 11. *A nonzero element a of a commutative ring R is said to divide an element $b \in R$ (notated $a \mid b$) iff $\exists x \in R, ax = b$. Elements a, b of R are said to be associates iff $a \mid b$ and $b \mid a$.*

Theorem 20. *Let $a, b, u \in R$ where R is a commutative ring with identity.*

(i) $a \mid b \iff (b) \subseteq (a)$

(ii) *a and b are associates iff $(a) = (b)$*

(iii) *u is a unit iff $u \mid r$ for all $r \in R$*

(iv) *u is a unit iff $(u) = R$*

(v) *The relation "a is an associate of b" is an equivalence relation on R.*

(vi) *If $a = br$ with $r \in R$ a unit, then a and b are associates. If R is an integral domain, the converse is true.*

Definition 12. *Let R be a commutative ring with identity. An element $c \in R$ is irreducible iff*

(i) *c is a nonzero nonunit.*

(ii) $c = ab \implies$ *a or b is a unit*

An element $p \in R$ is prime iff

(i) *p is a nonzero nonunit*

(ii) $p \mid ab \implies p|a \vee p|b$

Theorem 21. *Let p and c be nonzero elements in an integral domain R.*

(i) *p is prime iff (p) is a nonzero prime ideal*

(ii) *c is irreducible iff (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 iff p is irreducible.*

(v) Every associate of an irreducible [resp. prime] element of R is irreducible [resp. prime]

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

Proof. (i). If p is prime, $ab \in (p) \iff p \mid ab \implies p \mid a \vee p \mid b \iff a \in (p) \vee b \in (p)$. If (p) is a nonzero prime ideal, $p \mid ab \iff ab \in (p) \implies a \in (p) \vee b \in (p) \iff p \mid a \vee p \mid b$.
(ii). If c is irreducible, then (c) is a proper ideal of R. If $(c) \subseteq (d)$, then $c = dx$. Since c is irreducible, d or x is a unit. Hence (c) is maximal. Conversely, if (c) is maximal in S, then c is a nonzero nonunit in R. If $c = ab$, then $(c) \subseteq (a)$ whence $(c) = (a)$ or $(a) = R$. If $(a) = R$, then a is a unit. If $(c) = (a)$, then $a = cy$ hence $c = ab = cyb$. Thus b is a unit. Therefore b is irreducible.
(iii). If $p = ab$, $p \mid a \vee p \mid b$. Say $p \mid a$. Then $px = a$ and $p = ab = pxb$. Thus b is a unit.
(iv). If p is irreducible, then (p) is maximal, hence prime, thus p is prime.
(v). If c is irreducible, d is an associate of c, $c = du$ where u is a unit. If $d = ab$, then $c = abu$ whence a is a unit or bu is a unit. If bu is a unit, so is b hence d is irreducible.
(vi). If c is irreducible and $a \mid c$, then $(c) \subseteq (a)$ whence $(c) = (a)$ or $(a) = R$. Thus a is an associate of c or a unit. □

Definition 13. *An integral domain R is a unique factorization domain iff*

(i) Every nonzero unit element a of R can be written $a = c_1 c_2 \cdots c_n$ with $c_1, c_2, \cdots, c_n$ irreducible.

(ii) If $a = c_1 c_2 \cdots c_n, a = d_1 d_2 \cdots d_m$, c_i, d_j irreducible, then $n = m$ and for some permutation σ of $\{1, 2, \cdots, n\}$, c_i and $d_{\sigma(i)}$ are associates for every i.

Lemma 1. *If R is a principal ideal ring and $(a_1) \subseteq (a_2) \subseteq \cdots$ is a chain of ideals in R, then for some integer n, $(a_j) = (a_n)$ for all $j \geq n$.*

Proof. Let $A = \bigcup_{i \geq 1} (a_i)$. A is an ideal. Let $A = (a)$. $\exists n, a \in (a_n)$. Thus $(a) = (a_n)$. □

Theorem 22. *Every principal ideal domain is a unique factorization domain.*

Proof. Let R be PID and S be the set of all nonzero nonunit elements of R which cannot be factored as a finite product of irreducible elements. Suppose S is not empty and $a \in S$. Then (a) is a proper ideal and is contained in a maximal ideal (c). c is irreducible. $c \mid a$. Therefore, it is possible to choose for each $a \in S$ an irreducible divisor c_a of a. Since R is an integral domain, c_a uniquely determines a nonzero $x_a \in R$ such that $c_a x_a = a$. We claim $x_a \in S$. If x_a were a unit, a would be irreducible hence x_a is not a unit. If x_a were not in S, then x_a has a factorization as a product of irreducibles, whence a also does. Thus $x_a \in S$. We claim $(a) \subset (x_a)$. Since $(a) = (x_a)$ implies $x_a = ay$ for some $y \in R$ whence $a = x_a c_a = ayc_a$. Contradicting that c_a is irreducible and hence a nonunit. The function $f : S \to S$ given by $f(a) = x_a$ is well defined. By the recursion theorem, there is a function $\phi : \mathbb{N} \to S$ such that $\phi(0) = a$, $\phi(n+1) = f(\phi(n))$. Denote $\phi(n) = a_n$. There is an ascending chain of ideals $(a) \subset (a_1) \subset (a_2) \subset \cdots$ contradicting the previous lemma. Thus S must be empty. Finally, if $c_1 c_2 \cdots c_n = a = d_1 d_2 \cdots d_m$ then c_1 divides some d_i. Since c_1 is not a unit, c_1 is associate to d_i. We can cancel c_1 and d_i (with a factor of a unit), and proceed by induction to canceling the associates. If $n \neq m$, this would imply that some of the c_i or d_i are units, a contradiction. □

Definition 14. *Let R be a commutative ring. R is a Euclidean ring iff there is a function $\phi : R \setminus \{0\} \to \mathbb{N}$ such that*

(i) If $a, b \in R$, $ab \neq 0$, then $\phi(a) \leq \phi(ab)$

(ii) If $a, b \in R, b \neq 0, \exists q, r \in R, a = qb + r$ with $r = 0$ or $r \neq 0$ and $\phi(r) < \phi(b)$.

A Euclidean ring which is an integral domain is called a Euclidean domain.

Theorem 23. *Every Euclidean ring R is a principal ideal ring with identity. Every Euclidean domain is a unique factorization theorem.*

Proof. If I is a nonzero ideal in R, choose $a \in I$ such that $\phi(a)$ is the least integer in the set $\{\phi(x) \mid x \neq 0, x \in I\}$. If $b \in I$, then $b = aq + r$ with $r = 0$ or $r \neq 0$ and $\phi(r) < \phi(a)$. $r \in I$ so that $r = 0$, whence $b = aq$. $I = (a)$. R is a principal ideal ring. Since R itself is an ideal, $R = Ra$ for some $a \in R$. $\exists e \in R, a = ea = ae$. If $b \in R, \exists x \in R, b = xa$. Thus $be = xae = xa = b$. Whence e is a multiplicative identity for R. □

Definition 15. *Let X be a nonempty subset of a commutative ring R. An element $d \in R$ is a greatest common divisor of X provided*

(i) $\forall a \in X, d \mid a$

(ii) $\forall a \in X, c \mid a \implies c \mid d$

Greatest common divisors need not exist. When it exists, it may not be unique. However, two greatest common divisors are associates by (ii). Furthermore, any associate of a greatest common divisor is a greatest common divisor. If R has an identity and $a_1, a_2, \cdots, a_n$ have 1_R as a greatest common divisor, then $a_1, a_2, \cdots, a_n$ are said to be relatively prime.

Theorem 24. *Let $a_1, a_2, \cdots, a_n$ be elements of a commutative ring R with identity.*

(i) $d \in R$ is a greatest common divisor of $\{a_1, a_2, \cdots, a_n\}$ such that $d = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ for some $r_i \in R$ iff $(d) = (a_1) + (a_2) + \cdots + (a_n)$

(ii) *If R is a principal ideal ring, then a greatest common divisor of $a_1, a_2, \cdots, a_n$ exists and every one is of the form $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$*

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

Proof. (i). Routinely follows. (ii) follows from (i). (iii). Each a_i has a factorization $a_i = c_1^{m_{i,1}} c_2^{m_{i,2}} \cdots c_t^{m_{i,t}}$ with $c_1, \cdots, c_t$ distinct irreducible elements and each $m_{ij} \geq 0$. $d = c_1^{k_1} c_2^{k_2} \cdots c_t^{k_t}$ where $k_j = \min\{m_{1j}, m_{2j}, \cdots, m_{nj}\}$ is a greatest common divisor. □