1. Introduction to Rings

Definition 1.1.

1. a ring R is a set together with two binary operations $+$ and $\times$ satisfying the following axioms
   (a) $(R, +)$ is an abelian group
   (b) $\times$ is associative
   (c) the distributive laws hold in R
2. The ring R is commutative if $\times$ is commutative
3. The ring R is said to have identity if there is an element $1 \in R$.

Definition 1.2. A ring with identity R is said to be a *division ring* if very nonzero element has a multiplicative inverse. A commutative division ring is called a *field*.

Definition 1.3.

1. A nonzero element a of R is called a *zero divisor* if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.
2. Assume that R has identity $1 \neq 0$. An element u of R is called a ***unit*** in R if there is some v in R such that $uv = vu = 1$. The set of units is denoted $R^{\times}$.

Definition 1.4. A commutative ring with identity is called an ***integral domain*** if it has no zero divisors.

Proposition 1.5. Assume that a, b, and c are elements of any ring with a not a zero divisor. If $ab = ac$ then either $a = 0$ or $b = c$.

Corollary 1.6. Any finite integral domain is a field.

Definition 1.7. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

Proposition 1.8. Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

1. $deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$,
2. the units of $R[x]$ are just the units of R,
3. $R[x]$ is an integral domain.

Definition 1.9. Let R and S be rings.

1. A *ring homomorphism* is a map $\varphi : R \to S$ satisfying
   (a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$, and
   (b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$
2. The *kernel* of the ring homomorphism φ is the set of elements that map to 0_S.
3. A bijective ring homomorphism is called an isomorphism.

Proposition 1.10. Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

1. The image of φ is a subring of S.
2. The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker(\varphi)$ then $r\alpha$ and αr are in $\ker(\varphi)$ for every $r \in R$.

Definition 1.11. Let R be a ring, let I be a subset of R and let $r \in R$.

1. $rI = \{ra \mid a \in I\}$
2. A subset I of R is a ***left ideal*** of R if
   (a) I is a subring of R, and
   (b) I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.

   There is a similar definition for a right ideal.
3. A subset I that is both a left ideal and a right ideal is called an ideal of R.

Proposition 1.12. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I)=(r+s)+I \qquad \text{and} \qquad (r+I)\times(s+I)=(rs)+I$$

for all $r, s \in R$. Conversely if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition 1.13. When I is an ideal of R the ring R/I with the operations in the previous proposition is called the ***quotient ring*** of R by I.

Theorem 1.14.

1. *(The First Isomorphism Theorem for Ring)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S, and $R/\ker(\varphi)$ is isomorphic as a ring to $\varphi(R)$.
2. If I is any ideal of R, then the map

   $$R \to R/I \qquad \text{defined by} \qquad r \mapsto r+I$$

   is a surjective homomorphism with kernel I. Thus every ideal is the kernel of a ring homomorphism and vice versa.

Theorem 1.15.

1. *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A+B=\{a+b \mid a \in A,\ b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A, and $(A+B)/B \cong A/(A\cap B)$.
2. *(The Third Isomorphism Theorem for Rings)* Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
3. *(The Fourth or Lattice Isomorphism Theorem for Rings)* Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I Furthermore, A is an ideal of R if and only if A/I is an ideal of R/I.

Definition 1.16. Let R be a ring. Then the ***characteristic*** of the ring R is the smallest number n such that $n1 = 1+1+1+\cdots+1 = 0$. If this never happens, then the characteristic of R is said to be 0.

Proposition 1.17. Let R be an integral domain. Then $char(R)$ is either prime or 0.

Definition 1.18. Let A be any subset of the ring R.

1. Let (A) denote the smallest ideal of R containing A, called ***the ideal generated by*** A.
2. Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$.
3. An ideal generated by a single element is called a ***principal ideal***.
4. An ideal generated by a finite set is called a ***finitely generated ideal***.

Proposition 1.19. Let I be an ideal of R.

1. $I = R$ if and only if I contains a unit.
2. Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Corollary 1.20. If R is a field then any nonzero ring homomorphism from R into another ring is an injection (the kernel of the ring homomorphism is an ideal).

Definition 1.21. An ideal M in an arbitrary ring S is called a ***maximal ideal*** if $M \neq S$ and the only ideals containing M are M and S.

Proposition 1.22. In a ring with identity every proper ideal is contained in a maximal ideal. [NB: This is important because this means ideals in a ring with identity satisfy the ascending chain condition. This becomes really important in the study of infinite rings like the power series ring $\mathbb{Z}[\![x]\!]$.]

Proposition 1.23. Assume R is commutative. The ideal M is maximal if and only if the quotient ring R/M is a field.

Definition 1.24. Assume R is commutative. An ideal P is called a ***prime ideal*** if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

Proposition 1.25. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Corollary 1.26. Assume R is commutative. Every maximal ideal of R is a prime ideal.

Theorem 1.27. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication. Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties:

1. every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R\backslash\{0\}$ then Q is a field.
2. (uniqueness of Q) The ring Q is the *"smallest"* ring containing R in which all the elements of D become units, in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Definition 1.28. Let R, D, and Q be as in the above theorem.

1. The ring Q is called the ***ring of fractions*** of D with respect to R and is denoted $D^{-1}R$.
2. If R is an integral domain and $D = R\backslash\{0\}$, Q is called the ***field of fractions*** or *quotient field* of R.

Corollary 1.29. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

Definition 1.30. The ideals A and B of the ring R are said to be ***comaximal*** if $A + B = R$.

Theorem 1.31. *(Chinese Remainder Theorem)* Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \quad \text{defined by} \quad r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $\cap A_i$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Corollary 1.32. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$Z/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(Z/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

Corollary 1.33. Let $a, b \in \mathbb{Z}$ then

$$\mathbb{Z}/(m) \times \mathbb{Z}/(n) \cong \mathbb{Z}/(\gcd(m, n)) \times \mathbb{Z}/(\operatorname{lcm}(m, n))$$

2. Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

All rings in this section are commutative.

Definition 2.1. Any function $N : R \to \mathbb{Z}_{\geq 0}$ with $N(0) = 0$ is called a ***norm*** on the integral domain R. If $N(a) > 0$ for all $a \neq 0$ define N to be a *positive norm*.

Definition 2.2. The integral domain R is said to be a ***Euclidean Domain*** if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = qb + r \qquad \text{with } r = 0 \text{ or } N(r) < N(b).$$

Definition 2.3. Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

1. a is said to be a ***multiple*** of b if $a = bx$ for some $x \in R$. In this case b is said to divide or be a divisor of a, written $b \mid a$.
2. A ***greatest common divisor*** of a and b is a nonzero element d such that
   (a) $d \mid a$ and $d \mid b$, and
   (b) if $d' \mid a$ and $d' \mid b$ then $d \mid d'$.

   A greatest common divisor of a and b will be denoted by $\gcd(a, b)$.

Proposition 2.4. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

Proposition 2.5. Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, then $d' = ud$ for some unit $u \in R$. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Theorem 2.6. Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then

1. d is a greatest common divisor of a and b, and

2. the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an ***R-linear combination*** of a and b, i.e., there are elements x and y in R such that

$$d = ax + by.$$

Definition 2.7. A domain R in which every ideal is principal is called a ***Principal Ideal Domain*** (PID).

Proposition 2.8. Let R be a PID and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

1. d is a greatest common divisor of a and b
2. d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R with

$$d = ax + by$$

3. d is unique up to multiplication by a unit in R.

Proposition 2.9. Every nonzero prime ideal in a PID is a maximal ideal.

Corollary 2.10. If R is any commutative ring such that the polynomial ring $R[x]$ is a PID (or Euclidean Domain), then R is necessarily a field.

Definition 2.11. Let R be an integral domain

1. Suppose $r \in R$ is nonzero and is not a unit. Then r is called ***irreducible*** if R if whenever $r = ab$ with $a, b \in R$ at least one of a or b is a unit in R.
2. The nonzero element $p \in R$ is called ***prime*** in R it the ideal (p) generated by p is a prime ideal. In other words, for any $a, b \in R$ if $p \mid ab$ then either $p \mid a$ or $p \mid b$.
3. Two elements $a, b \in R$ differing by a unit are said to be ***associate*** in R.

Proposition 2.12. In an integral domain a prime element is always irreducible.

Proposition 2.13. In a PID a nonzero element is prime if and only if it is irreducible.

Definition 2.14. A ***Unique Factorization Domain (UFD)*** is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

1. r can be written as the finite product of irreducibles p_i of R: $r = p_1 p_2 \cdots p_n$ and
2. the decomposition given in (1) is unique up to associates.

Proposition 2.15. In a UFD a nonzero element is a prime if and only if it is irreducible.

Proposition 2.16. Let a and b be two nonzero elements of the UFD R and suppose

$$a = u\, p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n} \qquad \text{and} \qquad b = v\, p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \ldots, p_n$ are *distinct* and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} p_3^{\min(e_3,f_3)} \cdots p_n^{\min(e_n,f_n)}$$

is a greatest common divisor of a and b.

Theorem 2.17. Every PID is a UFD. In particular, every Euclidean Domain is a UFD.

Lemma 2.18. The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if p is either 2 or is an odd prime congruent to $1 \mod 4$.

Proposition 2.19.

1. *(Fermat's Theorem on sums of squares)* The prime p is the sum of two integer squares, $p = a^2 + b^2$ if and only if $p = 2$ or $p \equiv 1 \mod 4$. Except for the interchanging a and b, the representation of p as the sum of two squares is unique.
2. The irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ are as follows
   (a) $1 + i$
   (b) the primes $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$
   (c) $a + bi,\ a - bi$, the distinct irreducible factors of $p = a^2 + b^2$ for the primes $p \in \mathbb{Z}$ with $p \equiv 1 \mod 4$.