

Definition:  $(R, +, \cdot)$  is a ring iff  $(R, +)$  is an Abelian group and  $\forall x, y, z \in R$ ,  $(xy)z = x(yz)$ ,  $(x + y)z = xz + yz$ ,  $x(y + z) = xy + xz$ . It's commutative iff  $xy = yx$  and has identity iff  $\exists 1 \in R | 1x = x1 = x$ . Convention: All rings are commutative with identity.

Definition: A ring  $R$  is a field iff  $(R - 0, \cdot)$  forms a group.

Definition: A ring homomorphism  $f : R \rightarrow S$  is a map  $| f(x + y) = f(x) + f(y)$ ,  $f(xy) = f(x)f(y)$ ,  $f(1) = 1$ .

Definition: A subring  $S \subset R$  is an additive subgroup containing 1, closed under multiplication.

Definition: An ideal  $I \triangleleft R$  is an additive subgroup  $| a \in I, b \in R \Rightarrow ab \in I$ .

Definition: If  $I \triangleleft R$ , the quotient ring  $R/I$  is the set of additive cosets of  $I$  in  $R$ , with obvious  $+$  and  $\cdot$ .

Proposition:  $f : R \rightarrow S$  a ring homomorphism  $\Rightarrow \ker f \triangleleft R$  and  $im f$  is a subring of  $S$  isomorphic to  $R/\ker f$ .

Definition: Let  $a \in R$  and  $S \subset R$ .  $(a) = \{ra | r \in R\}$ , and  $(S) = \{\sum_{finite} r_i a_i | a_i \in S, r_i \in R\}$  are the ideals generated by  $a$  and  $S$ .

Definition: Let  $I, J \triangleleft R$  or  $I_i \triangleleft R, i \in L$ .  $I + J = \{a + b | a \in I, b \in J\}$ .  $\sum_{i \in L} I_i = \{\sum_{finite} a_j | a_j \in \text{some } I_i\}$ .  $\bigcap_{i \in L} I_i$  defined as usual.  $IJ = \{\sum_{i=1}^n a_i b_i | n \in \mathbb{N}, a_i \in I, b_i \in J\}$ .  $I_1 \dots I_n$  similarly.  $I^n = I \dots I$   $n$  times.

Proposition: All the above are ideals.

Definition:  $a \in R$  is invertible or a unit iff  $\exists b \in R | ab = 1$ .

Definition:  $a, a' \in R$  are associates iff  $\exists$  unit  $b \in R | a' = ab$ .

Proposition: Being associates is an equivalence relation.

Definition: A nonzero, nonunit  $a \in R$  is irreducible if  $a = bc \Rightarrow b$  or  $c$  is a unit.

Definition:  $a \in R$  is a zero-divisor iff  $\exists b \neq 0 | ab = 0$ .

Definition:  $R$  is an integral domain iff it has no zero-divisors except 0 itself.

Definition: An ideal  $I \triangleleft R$  is principal iff  $\exists a \in R | I = (a)$ .

Definition: An integral domain is a principal ideal domain (PID) iff all ideals are principal.

Theorem:  $K$  a field  $\Rightarrow K[x]$  a PID.

Lemma (Division Algorithm): If  $f, g \in K[x]$  and  $g \neq 0$ ,  $\exists! h, k \in K[x] | f = gh + k$ ,  $deg(k) < deg(g)$  or  $k = 0$ , and  $deg(h) = deg(f) - deg(g)$ . Here,  $k$  is called the remainder.

Definition: A root of  $f \in R[x]$  is  $x_0 \in R | f(x_0) = 0$ .

Proposition: If  $f$  has a root  $x_0$ , then it's divisible by  $x - x_0$ , hence reducible if  $deg(f) > 1$ .

Corollary: A nonzero polynomial of degree  $n$  has at most  $n$  roots.

Corollary: If a field  $K$  is infinite, then polynomials in  $K[x]$  are determined by their values, i.e.  $f, g \in K[x]$ .  $\forall x \in K, f(x) = g(x) \Rightarrow f = g$ .

Definition:  $R$  is Noetherian iff it satisfies the ascending chain condition: if  $I_1 \subset I_2 \subset I_3 \subset \dots$  ideals in  $R$ , then  $\exists N \in \mathbb{N} | \forall n \geq N, I_n = I_N$ .

Proposition:  $R$  Noetherian  $\Leftrightarrow$  every ideal is finitely generated, i.e. generated by a finite set.

Corollary: PID  $\Rightarrow$  Noetherian.

Theorem: Every nonzero, nonunit element of a PID (or Noetherian domain) can be factored, i.e. expressed as a (finite) product of (one or more) irreducibles.

Definition: An integral domain is a unique factorization domain (UFD) if any nonzero, nonunit element can be expressed as a product of irreducibles, unique up to permutation and units. That is, if  $a = a_1 \dots a_n = a'_1 \dots a'_m$ ,  $a_i, a'_i$  irreducible, then  $m = n$  and  $\exists$  bijection  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  such that  $a_i$  and  $a'_i$  are associates.

Proposition: A field is a UFD.

Definition:  $p \triangleleft R$  is prime if  $p \neq R$  and  $ab \in p \Rightarrow a \in p$  or  $b \in p$ .

Proposition:  $I$  is prime  $\Leftrightarrow R/I$  is a nontrivial integral domain.

Definition:  $m \triangleleft R$  is maximal if  $m \neq R$  and  $I \triangleleft R, m \subset I \Rightarrow m = I$  or  $I = R$ .

Proposition:  $I$  is maximal  $\Leftrightarrow R/I$  is a nontrivial field.

Lemma:  $I \triangleleft R \Rightarrow \exists$  a bijective correspondence between all ideals in  $R/I$  and those ideals in  $R$  containing  $I$ , given by taking  $J \triangleleft R/I$  to  $\pi^{-1}(J) \triangleleft R$  where  $\pi : R \rightarrow R/I$  is projection.

Corollary: Maximal ideals are prime.

Proposition: For  $0 \neq a \in R$  a PID,  $(a) \triangleleft R$  is maximal  $\Leftrightarrow a$  is irreducible.

Proposition: In a PID  $R$ , if irreducible  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .

Corollary: In a PID  $R$ , if irreducible  $p \mid a_1 \dots a_n$ , then  $p \mid$  some  $a_i$ .

Theorem: PID  $\Rightarrow$  UFD.

Corollary:  $\mathbb{Z}, K[x]$ , etcetera are UFDs.

Theorem: If  $R$  is a UFD, then so is  $R[x]$ .

Corollary: If  $R$  is a UFD, then so is  $R[x_1, \dots, x_n]$ .

Theorem: For  $R$  a UFD, an element  $a \in R$  is a greatest common divisor (gcd) of  $a_1, \dots, a_n \in R$ , if  $a \mid$  each  $a_i$  and  $a' \mid$  each  $a_i \Rightarrow a' \mid a$ .

Proposition: For  $R$  a UFD, any  $a_1, \dots, a_n \in R$  have a gcd, unique up to units.

Definition:  $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$  is primitive if  $\gcd(a_0, \dots, a_n) = 1$ , and monic if  $a_n = 1$ .

Proposition: For  $R$  a UFD, any  $f(x) \in R[x]$  can be factored uniquely up to units, as  $f(x) = cg(x)$ ,  $c \in R$  called the content of  $f$ ,  $g(x) \in R[x]$  primitive.

Lemma (Gauss' Lemma): For  $R$  a UFD,  $f(x), g(x) \in R[x]$  primitive  $\Leftrightarrow f(x)g(x)$  primitive.

Corollary: For  $R$  a UFD,  $f_1, \dots, f_n \in R[x]$  primitive  $\Leftrightarrow f_1 \dots f_n$  primitive.

Theorem (Hilbert Basis Theorem):  $R$  Noetherian  $\Rightarrow R[x]$  Noetherian.

Corollary:  $R$  Noetherian  $\Rightarrow R[x_1, \dots, x_n]$  Noetherian.

Proposition:  $R$  Noetherian,  $\exists R \rightarrow S$  a surjective homomorphism  $\Rightarrow S$  Noetherian.

Definition: A ring  $S$  is finitely generated over  $R$  (algebra-finite) if  $S \cong R[x_1, \dots, x_n]/I$  for some  $I$ , finitely presented if in addition  $I$  is finitely generated.

Proposition:  $R$  Noetherian,  $S$  finitely generated over  $R$ ,  $\exists R \rightarrow S$  a surjective homomorphism  $\Rightarrow S$  finitely presented.

Definition: For  $I \triangleleft R$ , the radical  $r(I) = \{a \in R \mid \exists n \in \mathbb{N} \text{ with } a^n \in I\}$ .

Proposition: (a)  $r(I) \triangleleft R$ ; (b)  $r(r(I)) = r(I)$ ; (c)  $I \subset J \Rightarrow r(I) \subset r(J)$ ; (d)  $r(I/J) = r(I)/J \triangleleft R/J$ .

Definition:  $r(0) = \{ \text{nilpotents } a \in R \}$  is called the nilradical  $N(R)$ .

Definition:  $I \triangleleft R$  is a radical ideal if  $\exists J \triangleleft R \mid I = r(J)$ , or equivalently by (b),  $r(I) = I$ , i.e.  $a^n \in I \Rightarrow a \in I$ .

Proposition: Prime  $\Rightarrow$  radical.

Theorem:  $r(I) =$  intersection of primes  $p \supset I$ . In particular  $N(R) =$  intersection of primes  $p \triangleleft R$ .

Definition:  $S \subset R$  is multiplicatively closed if  $a, b \in S \Rightarrow ab \in S$ .

Lemma:  $S \subset R$  multiplicatively closed,  $0 \notin S$ , then  $\exists$  ideals  $I \triangleleft R$  maximal among those with  $I \cap S = \emptyset$ , and they are prime.

Proposition: Any nonzero ring which is not a field has a nonzero maximal (hence prime) ideal containing any given nonunit  $a \in R$ .

Definition: The Jacobson radical  $J(R)$  is the intersection of all maximal ideals (so  $N(R) \subset J(R)$ ).

Proposition:  $a \in J(R) \Leftrightarrow \forall b \in R, 1 - ab$  is a unit.

Corollary: For  $K$  a field, even finite,  $J(K[x_1, \dots, x_n]) = 0$ .

Definition: A ring is local if it has a unique maximal ideal.

Proposition: If  $R$  is local the maximal ideals consists of all nonunits.