Department of Mathematics, IISc, Bangalore, Prof. Dr. D. P. Patil MA 312 Commutative Algebra / Jan-April 2020

MA 312 Commutative Algebra / Jan-April 2020 (BS, Int PhD, and PhD Programmes)

Download from : http://www.math.iisc.ac.in/patil/courses/Current Courses/	
Tel: +91-(0)80-2293 3212/09449076304	E-mails: patil@math.ac.in
Lectures : Tuesday and Thursday ; 15:30–17:00	Venue: MA LH-5 / LH-1
1.Rings and Idea	ls
Submit a solutions of * - Exercises ONLY. Recommended to solve the violet colored ^R Exercises	Due Date : Tuesday, 28-01-2020

All rings considered are commutative with identity element (unity) 1. When necessary we write 1_A for the identity element of the ring A. The zero ring $A = \{0\}$ is the only ring such that $1_A = 0$. For a ring A, the subsets A^{\times} and A^* denote the set of all units and non-zero divisors in A, respectively. Note that A^{\times} is a (multiplicative) subgroup and A^* is a (multiplicative) monoid of the multiplicative monoid (A, \cdot) of the ring A with $A^{\times} \subseteq A^*$. Further, the subset $Z(R) := A \setminus A^*$ denote the set of all zero divisors in A. Let $\mathcal{I}(A)$ (resp. SpecA, SpmA) denote the set of all ideals (resp. prime ideals, maximal ideals) in a ring A.

1.1 (Minimal rings and Characteristic of a ring) Let A be aring.

(a) The multiples of the unit element 1_A form the smallest subring $\mathbb{Z} \ 1_A := \{n \ 1_A \mid n \in \mathbb{Z}\}$ of *A* and is called the minimal ring of *A*. A ring which coincides with its minimal ring is called a minimal ring.¹

(b) There is a unique ring homomorphism $\chi = {}_{A}\chi : \mathbb{Z} \longrightarrow A$ which is called the c h a r-acteristic homomorphism of A. Its image is the minimal ring $\mathbb{Z} 1_A$ of A and its kernel is $\mathbb{Z} \operatorname{Ord} 1_A = \mathbb{Z} \operatorname{Char} A$ (by definition $\operatorname{Ord} 1_A = \operatorname{Char} A$). In particular, χ induces an isomorphism $\overline{\chi} : \mathbb{Z}/\mathbb{Z} \operatorname{Char} A \xrightarrow{\sim} \mathbb{Z} 1_A$ of rings. (Remark : The order $\operatorname{Ord} 1_A \in \mathbb{N}$ is the order of 1_A in the additive group (A, +) is called the c h aracteristic of A and is denoted by $\operatorname{Char} A$. —Recall that : Let G be a (multiplicative) group with neutral (identity) element e_G , $a \in G$ and $\operatorname{H}(a) := \{a^n \mid n \in \mathbb{Z}\}$ be the cyclic subgroup of G generated by a. Then the map $\varphi_a : (\mathbb{Z}, +) \longrightarrow \operatorname{H}(a)$, $n \mapsto a^n$ is a surjective homomorphism of groups with the kernel $\operatorname{Ker} \varphi_a = \{n \in \mathbb{Z} \mid a^n = e_G\} \subseteq \mathbb{Z}$. Therefore there exists a unique natural number $m \in \mathbb{N}$ such that $\operatorname{Ker} \varphi_a = \mathbb{Z} \operatorname{Ord} a$ and $a^n = e_G$, for $n \in \mathbb{Z}$, if and only if n is a multiple of $\operatorname{Ord} a$. If $m = \operatorname{Ord} a = 0$ then φ_a is injective and hence bijective, i.e. all powers a^n , $n \in \mathbb{Z}$, of a are pairwise distinct and φ_a is an isomorphism of groups from $(\mathbb{Z}, +)$ onto $\operatorname{H}(a)$.²

(c) Char A = Exp (A, +) := the exponent of the additive group (A, +). (Remark: Recall that: Let *G* be a (multiplicative) group with neutral element e_G . For $n \in \mathbb{Z}$, let $\chi_n : G \longrightarrow G$ be the power-map $x \longmapsto x^n$. Then the map $\chi : (\mathbb{Z}, \cdot) \longrightarrow (G^G, \circ), n \mapsto \chi_n$, is a monoid homomorphism from the multiplicative monoid (\mathbb{Z}, \cdot) into the monoid (G^G, \circ) of maps (with the composition \circ as the binary operation). The subset $\{k \in \mathbb{Z} \mid x^k = e_G \text{ for all } x \in G\}$ is a subgroup of the additive group $(\mathbb{Z}, +)$. The unique generator ≥ 0 of this subgroup is called the exponent of *G* and is denoted by Exp*G*. Now, assume that *G* is an (additive) abelian group. Then for each $n \in \mathbb{Z}$, the power-map $\chi_n : G \longrightarrow G$ is an endomorphism of *G*, i. e. $\chi_n \in \text{End } G$ for all $n \in \mathbb{Z}$. Altogether, the map $\chi : \mathbb{Z} \longrightarrow \text{End } G$ is a ring homomorphism with Ker $\chi = \mathbb{Z}$ Exp*G*. Moreover, χ induces an injective ring homomorphism $\overline{\chi} : \mathbb{Z}/\mathbb{Z}$ Exp $G \longrightarrow \text{End } G$.

D. P. Patil/IISc

2020MA-MA312-ca-ex01.tex

July 5, 2020 ; 6:09 p.m.

¹ Minimal rings are also called prime rings.

² In this case, often one also (and some authors) say that the order of a is ∞ , since H(a) has infinitely many elements.

Now, let $G = H(a) = \mathbb{Z}_m$ be the cyclic group with $m = \operatorname{Exp} G$. Then $\overline{\chi}$ is also surjective and hence a canonical isomorphism of rings $\mathbb{Z}/\mathbb{Z}m \xrightarrow{\sim} \operatorname{End} \mathbb{Z}_m$, $[n]_m \mapsto (\chi_n \colon x \mapsto nx)$. If, namely $f \colon \mathbb{Z}_m \to \mathbb{Z}_m$ is an endomorphism with f(a) = na, then $f = \chi_n$.

In particular, $\overline{\chi}$ induces an isomorphism of groups $(\mathbb{Z}/\mathbb{Z}m, \cdot)^{\times} \xrightarrow{\sim} (\text{Aut } \mathbb{Z}_m, \circ)$. If G is finite, i. e. if m > 0, then the order of the unit-group $(\mathbb{Z}/\mathbb{Z}m)^{\times}$ is $\varphi(m)$ and hence by the Fermat's Little Theorem, we have (Euler's Formula) : $n^{\varphi(m)} \equiv 1 \mod m$, if gcd(n,m) = 1.)

(d) Every minimal ring A of characteristic $m \in \mathbb{N}$ is isomorphic to the residue-class ring $\mathbb{Z}/\mathbb{Z}m$ and there is exactly one isomorphism $\mathbb{Z}/\mathbb{Z}m \xrightarrow{\sim} A$. (Remark: The residue-class rings $\mathbb{Z}/\mathbb{Z}m, m \in \mathbb{N}$, upto unque isomorphism, represents all minimal rings. We use

 $\mathbf{A}_m := (\mathbb{Z}/\mathbb{Z}m, +, \cdot), \quad m \in \mathbb{N}^*, \quad \text{resp.} \quad \mathbf{A}_0 := (\mathbb{Z}, +, \cdot)$

as standard models for a minimal ring of the characteristic $m \in \mathbb{N}^*$ resp. for a minimal ring of the characteristic 0, but we shall also denote every other minimal ring of the characteristic m by \mathbf{A}_m . Then the identification of cyclic groups with $\mathbb{Z}/\mathbb{Z}m$ is unique. In particular, $\mathbf{A}_m = \mathbb{Z} \mathbf{1}_A \subseteq A$ is the minimal ring for every ring A of the characteristic m. The additive group of the *ring* \mathbf{A}_m is the cyclic group $\mathbf{Z}_m = (\mathbf{A}_m, +)$. The unit-group $\mathbf{A}_m^* = (\mathbf{A}_m, \cdot)^{\times}$ contains precisely the elements $a \cdot \mathbf{1}_{\mathbf{A}_m}$ with $a \in \mathbb{Z}$, $\gcd(a,m) = 1$. If m > 0, then its order is $\varphi(m)$. In particular, \mathbf{A}_m is an integral domain if and only if $m \in \mathbb{P} := \mathbb{P} \uplus \{0\}^3$ and is a field if and only if $m \in \mathbb{P}$ is a prime number. For a positive integer m > 0, the unit-group \mathbf{A}_m^* is called the prime residue-class group modulo m.)

1.2 The additive group (K, +) and the multiplicative group (K^{\times}, \cdot) of a field *K* are never isomorphic.

1.3 (a) A ring A is a minimal ring if and only if its additive group is cyclic. If A is finite with square-free cardinal number, then A is a minimal ring.

(b) If A is a finite ring, then |A| and CharA have the same prime factors. In particular, the cardinality of a finite field is a prime-power. (**Remark**: The additive group of K is even an elementary abelian p-group, p := CharK.—For a prime number p, an (additive) abelian group H is called an elementary abelain p-group if px = 0 for all $x \in H$, i.e. if every element of H

1.4 Give an example of a ring *B* with a subring $A \subseteq B$ such that $A^{\times} \subseteq B^{\times} \cap A$ and $A^{*} \supseteq B^{*} \cap A$. (The inclusions $A^{\times} \subseteq B^{\times} \cap A$ and $A^{*} \supseteq B^{*} \cap A$ are trivial.)

1.5 Let *A* be a ring. The operations sum, intersection and product on $\mathcal{I}(A)$ are commutative and associative. Moreover, for all $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathcal{I}(A)$, we have :

(a) (Distributive law) $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}$.

(b) (Modular law) If $\mathfrak{a} \supseteq \mathfrak{b}$ or $\mathfrak{a} \supseteq \mathfrak{c}$, then $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$.

(c) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$. (Remark : In the ring \mathbb{Z} the equality $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{ab}$ holds.)

(d) $ab \subseteq a \cap b$ and the equality $a \cap b = ab$ holds if a and b are comaximal, i.e. a + b = A. (**Remark :** For a ring *A*, the set $\mathcal{I}(A)$ is a (multiplicative and additive) monoid (with binary operations product and sum of ideals, respectively) and also an ordered set ⁴ (with respect to the natural inclusion) which is compatible with the multiplication. Therefore $\mathcal{I}(A)$ is an ordered monoid. Moreover, it is a lattice, i.e. for any two elements $a, b \in \mathcal{I}(A)$, both Sup $\{a, b\}$ and Inf $\{a, b\}$ exist.)

D. P. Patil/IISc

is of order 1 or p.)

2020MA-MA312-ca-ex01.tex

July 5, 2020 ; 6:09 p.m.

³ $\overline{\mathbb{P}}$ is the set of *all* prime elements of (\mathbb{N}, \cdot) .

⁴ An ordered set (X, \leq) is a set with the order \leq which is a reflexive, transitive, antisymmetric relation on X.

1.6 (Ideal quotient) For \mathfrak{a} , $\mathfrak{b} \in \mathfrak{I}(A)$, the ideal quotient of \mathfrak{a} by \mathfrak{b} is the ideal $(\mathfrak{a}:\mathfrak{b}) := \{a \in A \mid a\mathfrak{b} \subseteq \mathfrak{a}\}$. In particular, $(0:\mathfrak{b})$ is $\{a \in A \mid a\mathfrak{b} = 0\}$ is the annihilator Ann_A($\mathfrak{b}) := \{a \in A \mid a\mathfrak{b} = 0\}$ of \mathfrak{b} . If $\mathfrak{b} = Ab$, then we simply write $(\mathfrak{a}:b)$ for $(\mathfrak{a}:\mathfrak{b})$. (In the ring $A = \mathbb{Z}$, let $\mathfrak{a} = \mathbb{Z}m$, $\mathfrak{b} = \mathbb{Z}n$. Then $(\mathfrak{a}:\mathfrak{b}) = \mathbb{Z}q$, where $q = \prod_p \text{ prime } p^{r_p}$, $r_p := \max(v_p(m) - v_p(n), 0) = v_p(m) - \min(v_p(m) - v_p(n))$. Therefore $q = m/\gcd(m, n)$.)

For ideals $\mathfrak{a}, \mathfrak{a}_i, i \in I$; $\mathfrak{b}, \mathfrak{b}_i, i \in I$; $\mathfrak{c} \in \mathfrak{I}(A)$, verify the following computational rules :

(a)
$$\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$$
. (b) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$. (c) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}$
(d) $(\cap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \cap_{i \in I} (\mathfrak{a}_i : \mathfrak{b})$. (e) $(\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i) = \cap_{i \in I} (\mathfrak{a} : \mathfrak{b}_i)$.

1.7 (Radical of an ideal) For $a \in \mathcal{J}(A)$, the radical of a is the ideal $r(a) = \sqrt{a} := \{a \in A \mid a^n \in a \text{ for some } n \in \mathbb{N}^+\}.$

For ideals $\mathfrak{a}, \mathfrak{b} \in \mathfrak{I}(A)$, verify the following computational rules :

(a)
$$a \subseteq \sqrt{a}$$
. (b) $\sqrt{\sqrt{a}} = \sqrt{a}$. (c) $\sqrt{ab} = \sqrt{a \cap b} = \sqrt{a} \cap \sqrt{b}$.
(d) $\sqrt{a+b} = \sqrt{\sqrt{a}+\sqrt{b}}$. (e) $\sqrt{a} = A$ if and only if $a = A$.

(f) If p is a prime ideal in A, then $\sqrt{p^n} = p$ for all $n \in \mathbb{N}^+$.

1.8 (Extensions and Contractions of ideals) Let $\varphi : A \longrightarrow B$ be a ring homomorphism. We can use φ to transport ideals from A to B and also to transport ideals from B to A. More precisely:

If \mathfrak{a} is an ideal in A, then the set $\varphi(\mathfrak{a})$ need not be an ideal in B. The ideal $B\varphi(\mathfrak{a})$ generated by $\varphi(\mathfrak{a})$ is called the extension or the pushforward of \mathfrak{a} in B. Similarly, if \mathfrak{b} is an ideal in B, then $\varphi^{-1}(\mathfrak{b})$ is always an ideal in A which is called the contraction or the pullback of \mathfrak{b} in A. Therefore, we have the maps:

 $\varphi_* : \mathfrak{I}(A) \to \mathfrak{I}(B), \ \mathfrak{a} \mapsto \varphi_*(\mathfrak{a}) := B\varphi(\mathfrak{a}) \text{ and } \varphi^* : \mathfrak{I}(B) \to \mathfrak{I}(A), \ \mathfrak{b} \mapsto \varphi^*(\mathfrak{b}) := \varphi^{-1}(\mathfrak{b}),$ which are obviously homomorphisms of ordered sets.

(a) Suppose that the homomorphism $\varphi : A \longrightarrow B$ is surjective. Then $\varphi_*(\mathfrak{a}) = \varphi(\mathfrak{a})$ for all $\mathfrak{a} \in \mathfrak{I}(A)$ and the map φ^* is injective with image $\operatorname{Img} \varphi^* = \{\mathfrak{a} \in \mathfrak{I}(A) \mid \operatorname{Ker} \varphi \subseteq \mathfrak{a}\}$. Moreover, the map $\varphi^* : \mathfrak{I}(B) \longrightarrow \operatorname{Img} \varphi^*$ is an isomorphism of lattices with inverse $\varphi_* \mid_{\operatorname{Img} \varphi^*}$. In particular, one can identify the lattice of ideals $\mathfrak{I}(B)$ of *B* with the sublattice $\mathfrak{I}(A)$ of ideals of *A* via the map φ^* . Moreover :

(Push-pull formula) $\varphi^* \varphi_* \mathfrak{a} = \mathfrak{a} + \operatorname{Ker} \varphi$ for all $\mathfrak{a} \in \mathfrak{I}(A)$ and

(Pull-push formula) $\varphi_*\varphi^*\mathfrak{b} = \mathfrak{b}$ for all $\mathfrak{b} \in \mathfrak{I}(B)$.

(**Remark :** These formulas are extremely useful in the study of ring theory. More generally, it is extremely useful to ask about properties of φ_* and φ^* , in particular, when is φ^* is injective or surjective. Can one identify the composite maps $\varphi^*\varphi_*$ and $\varphi_*\varphi^*$? The most satisfying answers will come for localizations and integral extensions.)

(b) Let $\mathfrak{a} \in \mathfrak{I}(A)$, $\pi := \pi_{\mathfrak{a}} : A \to A/\mathfrak{a}$ be the natural surjective map, $\iota : A \to A[X]$ be the natural inclusion and let $\pi[X] : A[X] \to (A/\mathfrak{a})[X]$ be the ring homomorphism defined by $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \pi(a_i) X^i$. Then : Ker $\pi[X] = \mathfrak{a}A[X]$ and $\mathfrak{a}A[X] \cap A = \mathfrak{a}$. In particular, the map $\iota^* : \mathfrak{I}(A[X]) \longrightarrow \mathfrak{I}(A)$ is surjective. Further, the map $\iota_* : \mathfrak{I}(A) \longrightarrow \mathfrak{I}(A[X])$

D. P. Patil/IISc

2020MA-MA312-ca-ex01.tex

July 5, 2020 ; 6:09 p.m.

Page 4

1. Rings and Ideals

is compatible with intersections, i.e. for ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \in \mathfrak{I}(A)$, $(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r)A[X] = (\mathfrak{a}_1A[X]) \cap \cdots \cap (\mathfrak{a}_rA[X])$ and $\iota_*(\operatorname{Spec} A) \subseteq \operatorname{Spec} A[X]$, but $\iota_*(\operatorname{Spm} A) \not\subseteq \operatorname{Spm} A[X]$.

(c) Find an ideal in the polynomial ring $\mathbb{Z}[X]$ which is not extended from \mathbb{Z} under the natural inclusion $\iota : \mathbb{Z} \to \mathbb{Z}[X]$, i.e. not in the image of the map $\iota_* : \mathfrak{I}(Z) \longrightarrow \mathfrak{I}(\mathbb{Z}[X])$.

(d) $\varphi^*(\operatorname{Spec} B) \subseteq \operatorname{Spec} A$, in other words, *contraction of a prime ideal is always a prime ideal*. But, in general, $\varphi^*(\operatorname{Spm} B) \not\subseteq \operatorname{Spm} A$, i. e. contraction of a maximal ideal need not be a maximal ideal. (**Remark :** The behavior of prime ideals under φ_* under the ring extensions $\iota : \mathbb{Z} \longrightarrow B$, where *B* is the ring of algebraic integers in a number field, is one of the central problems of algebraic number theory.)

*1.9 Let \mathfrak{a} be an ideal in a ring A and $a \in A$.

(a) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be *prime* ideals in *A* such that $a + \mathfrak{a} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_r$. Then the ideal $Aa + \mathfrak{a} = \langle a, \mathfrak{a} \rangle \subseteq \mathfrak{p}_i$ for some $i \in \{1, \ldots, r\}$. (**Remark :** There is an example of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}$ and an element $a \in A$ such that $a + \mathfrak{a} \subseteq \mathfrak{a}_1 \cup \mathfrak{a}_2$, but $a + \mathfrak{a} \not\subseteq \mathfrak{a}_i$ for i = 1, 2.)

(b) (Prime Avoidance Lemma) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be ideals in A such that *at most two* of them are not prime. If $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$, then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some $i \in \{1, \ldots, r\}$. (Remark : This is a weaker version of Urysohn's Lemma⁵ in SpecA viz. one can "separate" a closed set in SpecA from a finite set of points outside it.)

R 1.10 Let $A := C_{\mathbb{R}}([0,1])$ be the \mathbb{R} -algebra of continuous real valued functions on the closed interval $[0,1] \subseteq \mathbb{R}$. For $f \in A$, let $V(f) := \{t \in [0,1] \mid f(t) = 0\}$ denote the set of zeros of f in [0,1] and $U(f) := [0,1] \setminus V(f)$. For $f \in A$, prove that :

(a) $f \in A^{\times}$ if and only if $V(f) = \emptyset$.

(b) $f \in A$ is a non-zero divisor in A if and only if V(f) is nowhere dense in [0, 1], i.e. the complement U(f) of V(f) is dense in [0, 1]. (Hint: (\Rightarrow) Let U := U(f). If $\overline{U} \subseteq [0, 1]$, then $U \cap V = \emptyset$ for some non-empty subset $V \subseteq [0, 1]$, i.e. $V \subseteq V(f)$. By Exercise⁶ there exists $g \in A$ with $V(f) = [0, 1] \setminus V$. But, then fg = 0 and $g \neq 0$, i.e. f is a zero-divisor in A. (\Leftarrow) Suppose that fg = 0 and $g \neq 0$. Then g = 0 on U which is dense in [0, 1] and hence g = 0 on [0, 1] by continuity of g.)

(c) $A^{\times} \subsetneq S_0 := A \setminus Z(A)$, i.e. there are non-zero divisors which are non-units in A. (Hint: Consider $f \in A$ with $V(f) = \{x_1, \dots, x_r\}$, $U(f) := [0, 1] \setminus \{x_1, \dots, x_r\} = \bigcap_{i=1}^r ([0, 1] \setminus \{x_i\})$ is dense in [0, 1].)

(d) For a subset $Y \subset [0,1]$, let $I(Y) := \{f \in A \mid f(y) = 0 \text{ for all } y \in Y\}$. For example, $I(\{t\}) = \mathfrak{m}_t := \{f \in A \mid f(t) = 0\}$ is a maximal ideal in *A*. Show that I(Y) is an ideal in *A* and $I(Y) \in \text{Spm } A$ if and only if *Y* is singleton. (Hint: Note that if $Y' \subseteq Y \subseteq [0,1]$, then $I(Y) \subseteq I(Y')$.)

D. P. Patil/IISc

2020MA-MA312-ca-ex01.tex

July 5, 2020 ; 6:09 p.m.

 $^{^{5}}$ Pavel Samuilovich Urysohn (1898-1924) was a Soviet mathematician who is best known for his contributions in dimension theory in topology, and for developing Urysohn's metrization theorem and Urysohn's lemma, both of which are fundamental results in topology. This gave Urysohn an international platform for his ideas which immediately attracted the interest of mathematicians such as David Hilbert.

⁶ Exercise : For every closed subset $Z \subseteq \mathbb{R}$, there exists a continuous function $f : \mathbb{R} \to \mathbb{R}$ such that $Z = Z(f) = \{t \in \mathbb{R} \mid f(t) = 0\}$. (Hint : Consider the distance function $t \mapsto d(t, Z)$.)