# MA 312 Commutative Algebra / Aug–Dec 2017

(Int PhD. and Ph. D. Programmes)

Download from : http://www.math.iisc.ernet.in/patil/courses/courses/Current Courses/...

**Tel :** +91-(0)80-2293 3212/09449076304 **E-mails :** patil@math.iisc.ernet.in

**Lectures :** Wednesday and Friday ; 14:00–15:30 **Venue:** MA LH-2 ( **if LH-1 is not free** ) / LH-1

**Seminars :** Sat, Nov 18 (10:30–12:45) ; Sat, Nov 25 (10:30-12:45)

**Final Examination :** Tuesday, December 05, 2017, 09:00–12:00

## Supplement 4

## Direct Sums and Direct Products — Idempotent Endomorphisms

**S4.1** (Direct product representations of rings) Let $B_i, i\in I$, be a family of rings, $B := \prod_{i\in I} B_i$ its direct product and let $\pi_i : B \to B_i$, $i\in I$, be the canonical projections. For an arbitrary ring $A$, the map $\varphi \mapsto (\pi_i\varphi)_{i\in I}$ from $\operatorname{Hom}(A,B)$ into $\prod_{i\in I}\operatorname{Hom}(A,B_i)$ is bijective. If $\varphi_i : A \to B_i$ is a family of ring homomorphisms, then this family is called a representation of $A$ as a (direct) product of the rings $B_i, i\in I$, if the corresponding ring homomorphism $\varphi : A \to \prod_{i\in I} B_i$ with $\varphi_i = \pi_i\varphi$ is an isomorphism. In this case, all the $\varphi_i$, $i\in I$, are necessarily surjective.

From now on we discuss representations of a ring as *finite* products.

**4.S.1 Theorem** *A finite family $\varphi_i$, $i\in I$, of surjective ring homomorphisms $\varphi_i : A \to B_i$ represents $A$ as direct product of the rings $B_i$, $i\in I$, if and only if the two-sided ideals $\mathfrak{a}_i := \operatorname{Ker}\varphi_i$ satisfy the two conditions:* (1) $\mathfrak{a}_i + \mathfrak{a}_j = A$ *for all* $i \neq j$ *and* (2) $\bigcap_{i\in I}\mathfrak{a}_i = 0$.

**Proof** Let $B := \prod_{i\in I} B_i$ and let $\varphi : A \to B$ be the homomorphism with $\varphi_i = \pi_i\varphi$ for $i\in I$. Then $\varphi(a) = (\varphi_i(a))_{i\in I}$ for all $a\in A$, and hence $\operatorname{Ker}\varphi = \bigcap_{i\in I}\mathfrak{a}_i$. Therefore $\varphi$ is injective if and only if (2) holds. — Now we show that the surjectivity of $\varphi$ is equivalent to (1). Suppose that $\varphi$ is surjective and let $i,j\in I$ with $i\neq j$. By hypothesis on $\varphi$, there exists an $a\in A$ such that $\varphi_i(a) = 0$ and $\varphi_j(a) = 1$. Then $a\in\mathfrak{a}_i$ and $1-a\in\mathfrak{a}_j$, and so $1 = a + (1-a) \in \mathfrak{a}_i + \mathfrak{a}_j$. It follows that $\mathfrak{a}_i + \mathfrak{a}_j = A$. Conversely, suppose that (1) is fulfilled. Then

$$\mathfrak{a}_i + \bigcap\nolimits_{j\neq i}\mathfrak{a}_j = A \qquad \text{for every} \quad i\in I\,.$$

To prove this formula, it is enough to show: *If $\mathfrak{a},\mathfrak{b},\mathfrak{c}$ are two-sided ideals in $A$ with $\mathfrak{a}+\mathfrak{b} = A$ and $\mathfrak{a}+\mathfrak{c} = A$, then $\mathfrak{a} + (\mathfrak{b}\cap\mathfrak{c}) = A$.* But, if $a'+b = 1$ and $a''+c = 1$ with elements $a',a''\in\mathfrak{a}$, $b\in\mathfrak{b}$, $c\in\mathfrak{c}$, then $1 = (a'+b)(a''+c) = (a'a''+a'c+ba'') + bc \in \mathfrak{a} + (\mathfrak{b}\cap\mathfrak{c})$. (Note that even $\mathfrak{a}+\mathfrak{b}\mathfrak{c} = A$.) By the formula just proven, there is a representation $1 = a_i + d_i$ with $a_i\in\mathfrak{a}_i$ and $d_i \in \bigcap_{j\neq i}\mathfrak{a}_j$. Therefore $\varphi_i(d_i) = \varphi_i(1-a_i) = \varphi_i(1) - \varphi_i(a_i) = 1-0 = 1$ and $\varphi_j(d_i) = 0$ for $j\neq i$, and we have $\varphi(d_i) = (\varphi_j(d_i))_{j\in I} = (\delta_{ij}\cdot 1_{B_j})_{j\in I}$, where $\delta_{ij}$ is the Kronecker symbol. Now, if $b_i\in A$, $i\in I$, are arbitrary, then, for $a := \sum_{i\in I} b_i d_i \in A$,

$$\varphi(a) = \sum_{i\in I}\varphi(b_i)\,\varphi(d_i) = \sum_{i\in I}\big(\varphi_j(b_i)\big)_{j\in I}\cdot(\delta_{ij}\cdot 1_{B_j})_{j\in I} = \big(\varphi_j(b_j)\big)_{j\in I}\,.$$

This proves that $\varphi$ is surjective. •

Two two-sided ideals $\mathfrak{a}$, $\mathfrak{b}$ in a ring $A$ are called comaximal (or coprime) ideals if $\mathfrak{a}+\mathfrak{b} = A$. With this concept, condition (1) in 4.S.1 can be reformulated as follows: The two-sided ideals $\mathfrak{a}_i$, $i\in I$, are pairwise comaximal. By the way, *if $\mathfrak{a},\mathfrak{b}$ are comaximal two-sided ideals in $A$, then $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}+\mathfrak{b}\mathfrak{a}$ and, in particular, $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}$ if $A$ is commutative.* For, if $1 = a+b$, $a\in\mathfrak{a}$, $b\in\mathfrak{b}$ and $c\in\mathfrak{a}\cap\mathfrak{b}$, then $c = 1\cdot c = (a+b)c = ac+bc \in \mathfrak{a}\mathfrak{b}+\mathfrak{b}\mathfrak{a}$.

**4.S.2 Solving Simultaneous Congruences** *Let $\mathfrak{a}_i$, $i\in I$, be a finite family of pairwise comaximal two-sided ideals in a ring $A$. For every family $a_i$, $i\in I$, of elements $a_i\in A$, there exists an $a\in A$ such that*

$$a \equiv a_i \bmod \mathfrak{a}_i\,,\ \ i\in I\,.$$

*Moreover, any two solutions of these simultaneous congruences are congruent modulo the two-sided ideal $\bigcap_{i\in I}\mathfrak{a}_i$.*

**Proof** Let $\mathfrak{a} := \bigcap_{i\in I}\mathfrak{a}_i$. The canonical projections $A \to A/\mathfrak{a}_i$ induce surjective homomorphisms $\varphi_i : A/\mathfrak{a} \to A/\mathfrak{a}_i$. By Theorem 4.S.1, the $\varphi_i$, $i\in I$, define a representation of the ring $A/\mathfrak{a}$ as the direct product of the family $A/\mathfrak{a}_i$, $i\in I$. But, congruences modulo $\mathfrak{a}_i/\mathfrak{a}$ in $A/\mathfrak{a}$ are congruences modulo $\mathfrak{a}_i$ in $A$. •

For the ring $\mathbb{Z}$, Theorem 4.S.2 is the Chinese Remainder Theorem. For this reason its generalization given in 4.S.2 is also called the (generalised) Chinese Remainder Theorem.

Under the assumptions of Theorem 4.S.1, $B_i$ is canonically isomorphic to $A/\mathfrak{a}_i$ and therefore $\prod_{i\in I} B_i$ is canonically isomorphic to $\prod_{i\in I} A/\mathfrak{a}_i$. Therefore all finite product representations of $A$ are, up to canonical isomorphisms, obtained by finite families of quotient maps $A \to A/\mathfrak{a}_i$, where the two-sided ideals $\mathfrak{a}_i$ satisfy the conditions (1) and (2) of Theorem 4.S.1. The set of these direct product representations of $A$ can also be described with the help of central idempotent elements in $A$.

**4.S.3 Theorem** *Let $A$ be a ring and let $I$ be a finite index set. The map defined by*

$$(e_i)_{i\in I} \mapsto (\mathfrak{a}_i)_{i\in I} \quad \text{with} \quad \mathfrak{a}_i := \sum\nolimits_{j\neq i} A\, e_j = A\,(1-e_i)$$

*is a bijection from the set of the families $(e_i)_{i\in I}$ of idempotent elements $e_i \in A$ which satisfy the conditions*: (1) $e_i \in \mathrm{Z}(A)$, (2) $e_i e_j = \delta_{ij}\, e_i$, (3) $\sum_{i\in I} e_i = 1$; *onto the set of families $(\mathfrak{a}_i)_{i\in I}$ of two-sided ideals in $A$ which satisfy conditions* (1) *and* (2) *of* Theorem 4.S.1.

**Proof** Let $(e_i)$ be a family of idempotent elements in $A$ with the given properties. The associated ideals $\mathfrak{a}_i$ are two-sided since $e_i \in \mathrm{Z}(A)$. Moreover, they are pairwise comaximal since, for $i \neq j$, $1 = \sum_{r\in I} e_r \in \mathfrak{a}_i + \mathfrak{a}_j$ and hence $\mathfrak{a}_i + \mathfrak{a}_j = A$. Further, since $1 - e_i = \sum_{j\neq i} e_j$ and $e_j = e_j\,(1-e_i)$ for all $j \neq i$, it follows that $\sum_{j\neq i} A\, e_j = A\,(1-e_i)$. Finally, consider an element $a \in \mathfrak{a} := \bigcap_{i\in I} \mathfrak{a}_i$. Since $a \in \mathfrak{a}_i$, there exists a $b_i \in A$ such that $a = b_i\,(1-e_i)$. It follows $a\,e_i = b_i\,(1-e_i)e_i = 0$ and $a = a\cdot 1 = a\sum_i e_i = \sum_i a\,e_i = 0$. This proves $\mathfrak{a} = 0$.

Conversely, let $(\mathfrak{a}_i)$ be a family of two-sided ideals which satisfy the conditions (1) and (2) in 4.S.1. By 4.S.1, the canonical homomorphism $A \to B := \prod_{i\in I} A/\mathfrak{a}_i$ is an isomorphism. The elements of $B$ with 1 as one of its components and 0 as the remaining components form a family of central idempotent elements in $B$ with properties (1), (2) and (3), and the inverse of the isomorphism $A \to B$ maps this family onto a family $(e_i)$, $i \in I$, in $A$ with the same properties. This map $(\mathfrak{a}_i) \mapsto (e_i)$ is the inverse of the map in 4.S.3. •

A non-zero ring which is not isomorphic to a product of two non-zero rings is called i n d e c o m p o s a b l e or c o n n e c t e d . The above discussion yields:

**4.S.4 Corollary** *For a non-zero-ring $A$ the following statements are equivalent*:

(i) *$A$ is indecomposable.*

(ii) *There are no non-trivial two-sided comaximal ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $A$ with $\mathfrak{a} \cap \mathfrak{b} = 0$.*

(iii) *The center $\mathrm{Z}(A)$ of $A$ is indecomposable.*

(iv) 0 *and* 1 *are the only central idempotent elements in $A$.*

One has to distinguish between indecomposable rings and simple rings, see Example **??**. Every simple ring is indecomposable. Every integral domain is an indecomposable ring, but a simple ring only in case it is a field.

**S4.2** ( S i m p l e r i n g s ) A ring $A$ is called s i m p l e if $A$ is not the zero ring and if the trivial ideals 0 and $A$ are the only (two-sided) ideals of $A$. *A non-zero ring $A$ is simple if and only if every ring homomorphism $A \to B$ of $A$ into a non-zero ring $B$ is injective.* Division domains are simple rings. Furthermore :

**4.S.5 Proposition** *For a two-sided ideal $\mathfrak{a}$ in a ring $A$, the following conditions are equivalent*: (i) *$A/\mathfrak{a}$ is a simple ring.* (ii) *$\mathfrak{a}$ is a maximal two-sided ideal in $A$. — A non-zero ring $A$ has residue class rings which are simple rings. In other words, there exist surjective homomorphisms from the ring $A \neq 0$ onto simple rings.*

A commutative ring is simple if and only if it is a field. Simple rings which are no division domains are, for instance, the rings $\mathrm{M}_n(K)$, of $n \times n$-matrices over a division domain $K$, $n \geq 2$, see ???.

**S4.3** ( D i r e c t s u m d e c o m p o s i t i o n s o f m o d u l e s )
The decomposition of modules into direct sums of submodules is described in the following theorem with the help of endomorphisms.

**4.S.6 Theorem** *Let $A$ be a ring, $V$ be an $A$-module and $I$ be a set. The map defined by*

$$(P_i)_{i\in I} \mapsto (\mathrm{Img}\, P_i)_{i\in I}$$

*is a bijection from the set of families $(P_i)_{i\in I}$ of endomorphisms $P_i \in \mathrm{End}_A V$ with the properties*: (1) *$P_iP_j = \delta_{ij}P_i$ for all $i, j \in I$,* (2) *$(P_i)_{i\in I}$ is summable, and $\sum_{i\in I} P_i = 1$* $(= \mathrm{id}_V)$; *onto the set of the families $(V_i)_{i\in I}$ of submodules $V_i$ of $V$ with $V = \bigoplus_{i\in I} V_i$.*

**Proof** Let $(P_i)_{i\in I}$ be a family of endomorphisms $P_i \in \mathrm{End}_A V$ which satisfy the properties (1) and (2). Since $P_iP_j = 0$ for $i \neq j$ and $(P_i^2 =)P_iP_i = P_i$ for every $i \in I$, i.e. $P_i$ vanish on $\mathrm{Img}\, P_j$, if $i \neq j$, and the restriction of $P_i$ onto $\mathrm{Img}\, P_i$ is the identity. Therefore, since the sum of the submodules $\mathrm{Img}\, P_i$ in $V$ is direct. Namely, if $\sum_{i\in I} x_i = 0$ with elements $x_i \in \mathrm{Img}\, P_i$, with $x_i = 0$ for almost all $i \in I$; then for every $j \in I$, we have

$$0 = P_j\Big(\sum_{i\in I} x_i\Big) = \sum_{i\in I} P_j(x_i) = P_j(x_j) = x_j\,.$$

Now it follows from (2) that $V$ is also the direct sum of the submodules $\operatorname{Img} P_i$. Namely, for $x \in V$, we have

$$x = \mathrm{id}_V(x) = \Big(\sum_{i\in I} P_i\Big)(x) = \sum_{i\in I} P_i(x)\,.$$

Altogether, we have proved $V = \bigoplus_{i\in I} \operatorname{Img} P_i$ . Since $P_i$ satisfy the property (1), they are uniquely determined on the subset $E := \bigcup_{i\in I} \operatorname{Img} P_i$; and $E$ is is a generating system of $V$, it follows that the map $(P_i)_{i\in I} \mapsto (\operatorname{Img} P_i)_{i\in I}$ is injective.

Finally, we need to prove that this map is surjective. For this let $(V_i)_{i\in I}$ be a given family of submodules of $V$ with $V = \bigoplus_{i\in I} V_i$. If $x \in V$, then $x$ has a unique representation $x = \sum_{i\in I} x_i$ with uniquely determined elements $x_i \in V_i$, where $x_i = 0$ for almost all $i \in I$. Therefore the maps $P_i : V \to V$, $x \mapsto x_i$, $i \in I$, are well-defined. These maps are obviously, $A$-linear and $P_i(x) = 0$ for almost all $i \in I$. This proves that $(P_i)$ is a summable family of endomorphisms of $V$. Further, clearly $\operatorname{Img} P_i = V_i$, and (1) is satisfied for the family $(P_i)_{i\in I}$. Since

$$x = \sum_{i\in I} x_i = \sum_{i\in I} P_i(x) = \Big(\sum_{i\in I} P_i\Big)(x)\,.$$

it follows that $\sum_{i\in I} P_i = \mathrm{id}_V$. Therefore the condition (2) is also satisfied for $(P_i)_{i\in I}$. The image of this family is the given family $(V_i)_{i\in I}$. •

**4.S.7 Definition** Let $V$ be a module over the ring $A$. An $A$-endomorphism $P : V \to V$ of $V$ with $P^2 = P$ is called a projection of $V$. Therefore, the projections of an $A$-module $V$ are precisely idempotent elements of the endomorphism ring $\operatorname{End}_A V$ of $V$.

Altogether, with this, in the case, $I = \{1,2\}$, the Theorem 4.S.6 takes the following form:

**4.S.8 Theorem** *Let $A$ be a ring and $V$ be an $A$-module. The map*

$$P \mapsto (\operatorname{Img} P, \operatorname{Ker} P)$$

*is a bijection from the set of the projections of $V$ onto the set of pairs $(U,W)$, where $U$, $W$ are submodules of $V$ with $V = U \oplus W$.*

For a fixed direct summand $U$ of $V$, it follows from Theorem 4.S.8 that:

**4.S.9 Corollary** *Let $U$ be a direct summand of the $A$-module $V$. Then the set of the omplements of $U$ in $V$ is the set of the kernels of the projections $P$ of $V$ with* $\operatorname{Img} P = U$.

Let $V$ be an $A$-module and $U, W$ be submodules of $V$ with $V = U \oplus W$. Then the unique projection $P$ of $V$ with $\operatorname{Img} P = U$ and $\operatorname{Ker} P = W$ which exist by Theorem 4.S.6, is called the projection of $V$ onto $U$ along $W$ . If $P$ is the projection of $V$ onto $U$ along $W$, then $1 - P$ is the projection of $V$ onto $W$ along $U$. The identity of $V$ is the projection of $V$ onto $V$ along 0, and the zero homomorphism is the projection of $V$ onto 0 along $V$.

**4.S.10 Example** (Indecomposable modules) Let $V$ be a module over the ring $A$. If $V \neq 0$ and has no direct summands other than 0 and $V$, then $V$ is called indecomposable; otherwise $V$ is called decomposable. By Theorem 4.S.8, $V$ is indecomposable if and only if the endomorphism ring $\operatorname{End}_A V$ has only trivial idempotent elements 0 and 1 and $0 \neq 1$ i. A vector space over a division domain is indecomposable if and only if it has dimension 1.

**S4.4** (Direct sum decompositions of rings) Let $A$ be a ring. The map $\rho : A^{\mathrm{op}} \to \operatorname{End}_A A$, $a \in A^{\mathrm{op}} \mapsto \rho_a = (x \mapsto xa)$, is an isomorphism of rings. The map $A \to \operatorname{End}_A A$, $a \mapsto \rho_a$ is anti-isomorphism of rings. Therefore the projections of the $A$-module $A$ are the endomorphisms $x \mapsto xe$ of $A$, where $e \in A$ is idempotent. Further, we have the following assertion:

**4.S.11 Theorem** *Let $A$ be a ring and $I$ be a finite index set. The map defined by*

$$(e_i)_{i\in I} \mapsto (Ae_i)_{i\in I}$$

*is a bijection from the set of the families $(e_i)_{i\in I}$ of elements $e_i \in A$ which satisfy the conditions $e_ie_j = \delta_{ij}e_i$ and $\sum_{i\in I} e_i = 1$ onto the set of families $(\mathfrak{a}_i)_{i\in I}$ of left-ideals $\mathfrak{a}_i \subseteq A$ which satisfy the condition $A = \bigoplus_{i\in I} \mathfrak{a}_i$.*

The following simple exercise shows that it is not necessary to assume that the indexed set is finite.

**4.S.12 Exercise** Let $V$ be a finite module over a ring. If $V$ is a direct sum of submodules $V_i$, $i \in I$, then $V_i = 0$ for almost all $i \in I$.

The $A$-module $A$ is decomposable if and only if $A \neq 0$ and there exists a non-trivial ($\neq 0$, 1) idempotent element in $A$. If $A$ is a domain, then $A$ is always indecomposable, namely, if $e \in A$ is idempotent, then $e(1-e) = e - e^2 = 0$, and hence $e = 0$ or $1 - e = 0$.

**4.S.13 Remark** In 33.7 we have described direct product representations of a ring $A$ using the families $(e_i)$ of *central* idempotent elements in $A$. If one forgets the multiplicative structure structure of the ring $A$, then one acquires a special direct product decomposition of the $A$-module $A$ which can be formulated as direct sum decomposition of type as in Theorem 4.S.11 (with minor description of the ideals $\mathfrak{a}_i$). Note that in the application of families of idempotent elements both these situations need to be distinguished.

We still investigate the complements of left-ideals. By Theorem 4.S.8, a left-ideal $\mathfrak{a}$ in $A$ has a complement if and only if $\mathfrak{a} = Ae$ for some idempotent element $e \in A$; with corresponding complement $A(1-e)$. One can then ask when exactly there is only one element $e$ with this property.

**4.S.14 Theorem** *Let $\mathfrak{a}$ ebe a left-ideal in A. Then the following statements are equivalent*:

(1) $\mathfrak{a}$ *has only one complement in A.*

(2) $\mathfrak{a} = Ae$ *with one and only one idempotent element* $e \in A$.

(3) *There exists a two-sided ideal* $\mathfrak{b}$ *in A with* $A = \mathfrak{a} \oplus \mathfrak{b}$.

(4) $A = \mathfrak{a} \oplus \operatorname{Ann}_A \mathfrak{a}$.

**Proof** By Theorem 4.S.8 and Corollary 4.S.9 (1) and (2) are equivalent. For every two-sided ideal $\mathfrak{b}$ in $A$ with $\mathfrak{a} \cap \mathfrak{b} = 0$ ist $\mathfrak{b}\,\mathfrak{a} \subseteq \mathfrak{a} \cap \mathfrak{b} = 0$, and hence $\mathfrak{b} \subseteq \operatorname{Ann}_A \mathfrak{a}$. If, further $\mathfrak{c}$ is another complement of $\mathfrak{a}$ in $A$, then $1 = a + c$ with elements $a \in \mathfrak{a}$ and $c \in \mathfrak{c}$, $d = d \cdot 1 = da + dc = dc \in \mathfrak{c}$ for every $d \in \operatorname{Ann}_A \mathfrak{a}$, and so : $\operatorname{Ann}_A \mathfrak{a} \subseteq \mathfrak{c}$. This proves the implications $(3) \Leftrightarrow (4)$ and $(4) \Rightarrow (1)$. Now we only need to prove $(2) \Leftrightarrow (4)$. For this under the hypothesis of (2), it is enough to prove that $A(1-e) \subseteq \operatorname{Ann}_A \mathfrak{a}$, or equivalently $(1-e)\mathfrak{a} = 0$. For this, let $a \in A$ be arbitrary and $b := (1-e)ae$; it remains to show $b = 0$. It is easy to check that $e' := e - b$ and $Ae = Ae'$, and it follows that $e = e'$ by (2) and $b = 0$. •

**4.S.15 Corollary** *Let $\mathfrak{a}$ be a left-ideal in the ring A. If $\mathfrak{a} = Ae$ with a central idempotent element e, then this is the only idempotent element which generate the ideal $\mathfrak{a}$, and* $\operatorname{Ann}_A \mathfrak{a} = A(1-e)$ *is the only complement of $\mathfrak{a}$ in A.*

**4.S.16 Corollary** *In a commutative ring A, an ideal $\mathfrak{a}$ which is a direct summand of A is generated by a unique idempotent element e and has a unique complement, namely* $\operatorname{Ann}_A \mathfrak{a} = A(1-e)$.

**S4.5** We prove the following structure theorem for commutative artinian rings :

**4.S.17 Theorem** (Decomposition Theorem for commutative artinian rings) *Let A be a commutative artinain ring. Then A is a direct product of unique artinian commutative local rings which are indecomposable and uniquely ordered by the maximal ideals of A. — If A is reduced, then these local rings are fields.*

— The local direct factors of the artinian commutative ring $A$ are called the local components or the local factors of $A$.