MA 312 Commutative Algebra / January-April 2015

(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/(CSA 2239) **E-mails :** patil@math.iisc.ernet.in / dppatil@csa.iisc.ernet.in

Lectures : Monday and Thursday ; 11:00–12:30 **Venue:** MA LH-3 (**if LH-1 is not free**) / LH-1

Midterms : Monday, Feb 16, 2015, 2PM–5PM

Final Examination :

Evaluation Weightage : Exercises : 10% **Seminar :** 10% **Midterms :** 30% **Final Examination :** 50%

Range of Marks for Grades (Total 100 Marks)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	76–90	61–75	46–60	35–45	< 35

3. Free Modules

3.1 Every $\mathbb{Q}$-vector space $V \neq 0$ is not free over the subring $\mathbb{Z}$ of $\mathbb{Q}$.

3.2 Let V be a free module over a ring A and let $a \in A$ be an element which is not a left zero-divisor in A. Then the homothecy $\vartheta_a : V \to V$, $x \mapsto ax$ by a is injective.

3.3 Let B be a ring and A be a subring of B such that B is a free A-module. Then :

(a) An element $a \in A$ is not a left zero-divisor in A if and only if a is not a left zero-divisor in B.

(b) $(\mathfrak{a}B) \cap A = \mathfrak{a}$ for every left-ideal $\mathfrak{a} \subseteq A$.

(c) $A^\times = A \cap B^\times$. Moreover, if B is a field, then so is A. (**Hint :** If $a \in A \cap B^\times$, then $B = aB$.)

3.4 Let U and W be free A-submodules of an arbitrary A–module V with bases x_i $i \in I$ and y_j, $j \in J$, respectively. Show that x_i, y_j, $i \in I$, $j \in J$, together form a basis of $U + W$ if and only if $U \cap W = 0$.

3.5 Let A be a non-zero commutative ring. Show that A is a principal ideal domain if and only if every ideal in A is a free A-submodule of A.

3.6 Let K be a division ring and let A be a commutative subring of K such that K is a finite A-module. Show that A itself is a field. (**Hint :** This is a generalisation of the Exercise T2.4. Note that K contains a quotient field $\mathrm{Q}(A)$ of A. Let $x_1, \ldots, x_m$ be a A-generating system of K and let $y_1, \ldots, y_n$ be a $\mathrm{Q}(A)$-basis of K with $y_1 = 1$. Then $y_1^*(x_1), \ldots, y_1^*(x_m)$ is an A-generating system of $\mathrm{Q}(A)$, where y_1^* is the first coordinate function with respect to the basis $y_1, \ldots, y_n$. Now use the Exercise T2.4.)

3.7 Let x_i, $i \in I$, be a family of n-tuples from $\mathbb{Z}^n$. For a prime number p, let $\mathbf{F}_p (= \mathbb{Z}/\mathbb{Z}p$ denote the prime field of characteristic p. Show that the following statements are equivalent:

(i) The x_i, $i \in I$, are linearly independent over $\mathbb{Z}$.
(ii) The images of x_i, $i \in I$, in $\mathbb{Q}^n$, are linearly independent over $\mathbb{Q}$.
(iii) There exists a prime number p such that the images of x_i, $i \in I$, in $\mathbf{F}_p^n$, are linearly independent over $\mathbf{F}_p$.
(iv) For almost all prime numbers p, the images of x_i, $i \in I$, in $\mathbf{F}_p^n$, are linearly independent over $\mathbf{F}_p$.
Moreover, if $|I| = n$, then the above statements are further equivalent to the following statement:

(v) There exists a non-zero integer m such that $m\mathbb{Z}^n \subseteq \sum_{i \in I} \mathbb{Z}x_i$.

3.8 Let x_i, $i \in I$, be a family of n–tuples from $\mathbb{Z}^n$. For every prime number p let $\mathbf{F}_p$ denote a field with p elements. Show that the following statements are equivalent:

(i) The x_i, $i \in I$, generate (the $\mathbb{Z}$–module) $\mathbb{Z}^n$. (ii) For every prime number p, the images of x_i, $i \in I$, in $\mathbf{F}_p^n$, generate the $\mathbf{F}_p$-vector space $\mathbf{F}_p^n$. (**Hint :** ((ii) $\Rightarrow$ (i): Let $U := \sum_{i \in I} \mathbb{Z}x_i$. Note that by Exercise 3.7, there exists a non-zero integer m with $m\mathbb{Z}^n \subseteq U$. Further: to every prime number p and every

$x \in \mathbb{Z}^n$ there exist $x' \in U$, $y \in \mathbb{Z}^n$ such that $x = x' + py$, i.e. $\mathbb{Z}^n \subseteq U + p\mathbb{Z}^n$ for every prime number p. From this deduce that $U = \mathbb{Z}^n$.)

3.9 Let K be a field and let $b_0, \ldots, b_m$ be elements of K, all of which are not equal to 0. Then there exist atmost m distinct elements $x \in K$, which satisfy the equation

$$0 = b_0 \cdot 1 + b_1 x + \cdots + b_m x^m .$$

(**Hint :** If $x_1, \ldots, x_{m+1}$ are distinct elements in K, then by Exercise T3.2 and Exercise T3.6, the elements $h_j := (x_1^j, \ldots, x_{m+1}^j)$, $0 \leq j \leq m$, are linearly independent over K. — **Remark :** The same result is also true for integral domains, since every integral domain is contained in a field, for example, in its quotient field. With the help of concept of polynomials the above assertion can be formulated as : *A non-zero polynomial of degree $\leq m$ over a field (or an integral domain) K has at most m zeros in K.*)

3.10 Let A be an integral domain and let Q be a field which contains A. Show that:

(a) Every subgroup U of the unit group $A^\times$ of A with a positive exponent[1] is cyclic (and finite). In particular, every finite subgroup of $A^\times$ is cyclic.

(b) The unit group of every finite field is cyclic.) (**Hint :** The equation $x^m = 1$ has at most m solutions in A by Exercise 3.9. Now use the following Exercise on groups : *Let G be a finite group with neutral elements e. Suppose that for every divisor $d \in \mathbb{N}^*$ of the order* Ord$G$ *there are at most d elements $x \in G$ such that $x^d = e$. Then G is a cyclic group.*))

Below one can see some Supplements / Test-Exercises to the results proved in the class.

[1] **Exponent of a group.** Let G be a group with neutral element e. Then the set of integers n with $a^n = e$ for all $a \in G$ forms a subgroup U_G of the additive group of $\mathbb{Z}$, i.e. $U_G := \{n \in \mathbb{Z} \mid a^n = e \text{ for all } a \in G\}$ and hence there is a unique $m \in \mathbb{N}$ such that $U_G = \mathbb{Z}m$. This natural number m is called the exponent of G and usually denoted by Exp G. For example, if G is a finite cyclic group, then $\operatorname{Exp} G = \operatorname{Ord} G$; $\operatorname{Exp} \mathfrak{S}_3 = \operatorname{Ord} \mathfrak{S}_3$; In general : *$\operatorname{Exp} G$ and $\operatorname{Ord} G$ have the same prime divisors.* (proof!).

Supplements / Test-Exercises

T3.1 An element a in a ring A is a basis of the A–module A, if and only if a is a unit in A.

T3.2 **(a)** The elements $1,\ a\in\mathbb{R}$ are linearly independent over $\mathbb{Q}$, if and only if a is irrational (i.e. not rational). (**Remark :** Two real numbers b,c, which are linearly independent over $\mathbb{Q}$ are called *incommensurable*. Classical example: the length of the side and the length of the diagonal of a square are incommensurable, since the real number $\sqrt{2}\in\mathbb{R}$ is irrational.)

(b) Let $\mathbb{P}$ be the set of all prime numbers $p\in\mathbb{N}^*$. Show that the family $(\log p)_{p\in\mathbb{P}}$ is linearly independent over $\mathbb{Q}$.

T3.3 Let $a,b\in\mathbb{N}^*$ and $d:=\gcd(a,b)$. Then the relation submodule $\mathrm{Rel}_{\mathbb{Z}}(a,b)$ of $\mathbb{Z}^2$ is generated by $(bd^{-1},-ad^{-1})\in\mathbb{Z}^2$.

T3.4 In the subspace U of the $\mathbb{R}$–vector space $\mathbb{R}^{\mathbb{R}}$ of all functions from $\mathbb{R}$ into itself, generated by the functions $x\mapsto\sin(x+a)$, $a\in\mathbb{R}$, show that the two functions $x\mapsto\sin x$, $x\mapsto\cos x(=\sin(x+\pi/2))$ form a basis of U.

T3.5 Let $x_1,\dots,x_{n+1}$, $n\in\mathbb{N}$, be linearly independent elements of a vector space V over the division ring K. Suppose that n elements among $x_1,\dots,x_{n+1}$ are linearly independent over K. Then show that $\mathrm{Dim}_K(\mathrm{Rel}_K(x_1,\dots,x_{n+1}))=1$.

T3.6 Let K be a divison ring, V be a finite dimensional K–vector space and let V_i, $i\in I$, be a family of subspaces of V. Then there exists a finite subset J of I such that $\bigcap_{i\in I}V_i=\bigcap_{i\in J}V_i$ and $\sum_{i\in I}V_i=\sum_{i\in J}V_i$.

T3.7 Let K be a division ring and let V be not finite dimensional K–vector space. Construct an infinite sequences $U_0\subset U_1\subset\cdots\subset U_i\subset\cdots$ and $W_0\supset W_1\supset\cdots\supset W_i\supset\cdots$ of subspaces of V.

T3.8 Let I be a non-empty open interval in $\mathbb{R}$ and let $\mathrm{C}^0_{\mathbb{R}}(I)$ be the $\mathbb{R}$-vector space of all continuous real-valued functions on I. Show that $|\mathrm{C}^0_{\mathbb{R}}(I)|=|\mathbb{R}|$. (**Hint :** The map $\mathrm{C}^0_{\mathbb{R}}(I)\to\mathbb{R}^{\mathbb{Q}}$ defined by $f\mapsto f|\mathbb{Q}$ is injective.)

T3.9 Let K be a divison ring and let M be a maximal K–linear independent subset in the set of 0-1–sequences from $K^{\mathbb{N}}$. Show that : M has the cardinality of the continuum. (**Hint :** We may assume that K is the quotient field of its prime ring $\mathbb{Z}\cdot 1_K$. Using cardinality arguments show that the dimension of the subspace generated by the 0-1–sequences in $K^{\mathbb{N}}$ is the cardinality of the continuum.)

T3.10 Let I be a non-empty open interval in $\mathbb{R}$ and let $\mathrm{C}^{\omega}_{\mathbb{R}}(I)$ (respectively, $\mathrm{C}^0_{\mathbb{R}}(I)$) be the $\mathbb{R}$-vector space of all real-analytic[2] (respectively, continuous) real-valued functions on I. Then $\mathrm{C}^{\omega}_{\mathbb{R}}(I)\subseteq\mathrm{C}^0_{\mathbb{R}}(I)$ and if U is a $\mathbb{R}$-subspace of $\mathrm{C}^0_{\mathbb{R}}(I)$ with $\mathrm{C}^{\omega}_{\mathbb{R}}(I)\subseteq U$, then show that $\mathrm{Dim}_{\mathbb{R}}U$ has the cardinality of the continuum. (**Hint :** Without loss of generality let $I=]-1,1[$. Let $(a_{ij})_{i\in\mathbb{N}}$, $j\in J$, be a linearly independent family of 0-1–sequences in $\mathbb{R}^{\mathbb{N}}$, where $|J|=\aleph:=|\mathbb{R}|$, see T3.11. Then the functions $t\mapsto\sum_{i\geq 0}a_{ij}t^i$, $j\in J$, in $\mathrm{C}^{\omega}_{\mathbb{R}}(I)$ are linearly independent over $\mathbb{R}$. **Alternative hint :** the family of the functions $t\mapsto\exp(at)$, $a\in\mathbb{R}$, on I is linearly independent. Similarly, the rational functions $t\mapsto 1/(t-a)$, $a\in\mathbb{R}$, $|a|\geq 1$, are linearly independent in $\mathrm{C}^{\omega}_{\mathbb{R}}(]-1,1[)$.) Prove the analogous results for the complex vector space $\mathrm{H}(U)$ of holomorphic functions defined on a domain $U\subseteq\mathbb{C}$.

T3.11 For a given $n\in\mathbb{N}$, let $a_1,\dots,a_n\in K$ be n distinct elements in a field K. Then the sequences $g_i:=(a_i^{\nu})_{\nu\in\mathbb{N}}\in K^{\mathbb{N}}$, $i=1,\dots,n$, are linearly independent over K. (**Hint :** Suppose that the g_i are linearly dependent. Without loss of generality we may assume that $\mathrm{Dim}_K(\mathrm{Rel}_K(g_1,\dots,g_n))=1$, see T3.4. Let $(b_1,\dots,b_n)$ be a basis element of relations. Then the element $(b_1a_1,\dots,b_na_n)$ is also a relation of the g_i. This is a contradiction.)

T3.12 Let K be a field and let I be an infinite set. Then $\mathrm{Dim}_K(K^I)=|K^I|$. (**Hint :** In view of[3], it is

[2] A function $f:I\to\mathbb{R}$ is called *real-analytic at* $a\in I$, if there exist a open neighbourhood U of a and a convergent power series $\sum_{i=0}^{\infty}a_i(x-a)^i$ such that $f(x)=\sum_{i=0}^{\infty}a_i(x-a)^i$ for all $x\in U\cap I$. A function $f:I\to\mathbb{R}$ is called *real-analytic* if it is real-analytic at every $a\in I$.

[3] Let A be a ring and let V be a free A–module of infinite rank. Then $|V|=|A|\cdot\mathrm{rank}_A V=\mathrm{Sup}\{|A|,\mathrm{rank}_A V\}$.

enough to prove that $|K| \leq \mathrm{Dim}_K K^I$. Let $\sigma : \mathbb{N} \to I$ be injective and for $a \in K$, let g_a denote the I–tuple with $(g_a)_{\sigma(\nu)} := a^\nu$ for $\nu \in \mathbb{N}$ and $(g_a)_i := 0$ for $i \in I \smallsetminus \mathrm{im}\,\sigma$. Then by T3.11, $(g_a)_{a\in K}$ are linearly independent.) Deduce that $\mathrm{Dim}_K K^I > \mathrm{Dim}_K K^{(I)}$. – **Remark :** This dimension formula for K^I is also valid for division rings K. Proof!.)

T3.13 Let K be a division ring. Further, let $x_i = (a_{i1}, \ldots, a_{in}) \in K^n$, $i = 1, \ldots, n$. With the j-th components of this n–tuple we form the new n–tuples $y_j := (a_{1j}, \ldots, a_{nj})$, $j = 1, \ldots, n$. Show that the elements $x_1, \ldots, x_n$ of the K–*Left*-vector space K^n are linearly independent if and only if the elements $y_1, \ldots, y_n$ of the K–*right*-vector space K^n are linearly independent. (**Hint :** Suppose that $x_1, \ldots, x_n$ are linearly independent and $y_1 b_1 + \cdots + y_n b_n = 0$, $b_j \in K$. Then $x_1, \ldots, x_n \in \mathrm{Rel}_K(b_1, \ldots, b_n)$, and a dimension argument shows that $\mathrm{Rel}_K(b_1, \ldots, b_n) = K^n$, this means $b_1 = \cdots = b_n = 0$.)

T3.14 Let K be a division ring, I be a set and let $f_1, \ldots, f_n \in K^I$, $n \in \mathbb{N}$. The following statements are equivalent:

(i) The $f_1, \ldots, f_n$ are linearly independent over K.
(ii) There exists a subset $J \subseteq I$ such that $|J| = n$ and that the restrictions $f_1|J, \ldots, f_n|J \in K^J$ are linearly independent (and hence form a basis of K^J).
(iii) The value n-tuples $(f_1(i), \ldots, f_n(i)) \in K^n$, $i \in I$, generate K^n as a K–*right*-vector space. (**Hint :** The implication (i) $\Rightarrow$ (ii) can be proved by induction on n: Suppose that there exists a subset $J' \subseteq I$ with $(n-1)$–elements is found for $f_1, \ldots, f_{n-1}$ such that $f_1|J', \ldots, f_{n-1}|J'$ are linearly independent over K and so form a basis of $K^{J'}$. Then $f_n|J' = a_1(f_1|J') + \cdots + a_{n-1}(f_{n-1}|J')$ with $a_1, \ldots, a_{n-1} \in K$. Now, by (i) there exists an element $j \in I \smallsetminus J'$ such that $f_n(j) \neq a_1 f_1(j) + \cdots + a_{n-1} f_{n-1}(j)$. Now, choose $J := J' \cup \{j\}$. — For the equivalence (ii) $\Leftrightarrow$ (iii) use T3.13.)

T3.15 Let K be a division ring and let $a_1, \ldots, a_n \in K$. Let $g_i := (a_i^\nu)_{\nu\in\mathbb{N}} \in K^{\mathbb{N}}$ and $f_i := (1, a_i, \ldots, a_i^{n-1}) \in K^n$, $i = 1, \ldots, n$. Then $g_1, \ldots, g_n$ are linearly independent over K if and only if $f_1, \ldots, f_n$ are linearly independent over K. (**Hint :** Let $h_j := (a_1^j, \ldots, a_n^j) \in K^n$, $j \in \mathbb{N}$. Note that $f_i = g_i|\{0, \ldots, n-1\}$ and $(f_1(j), \ldots, f_n(j)) = (g_1(j), \ldots, g_n(j)) = h_j$ for all $j = 1, \ldots, n$. Therefore by T3.14, $g_1, \ldots, g_n$ are linearly independent if and only if h_j, $j = 1, \ldots, n$ generates the *right*-vector space K^n. Suppose that the elements $h_0, \ldots h_m$ are linearly independent in the K–*right*-vector space K^n, but the elements $h_0, \ldots, h_{m+1}$ are not linearly independent, so h_{m+1} and hence h_j for every $j \geq m+1$ is a linear combination of $h_0, \ldots, h_m$. Now again use T3.14.)

T3.16 Let A be a ring $\neq 0$ with finitely many elements and let V be an A–module with a generating system of n elements, $n \in \mathbb{N}$. Show directly (without using the theorem) that every $n+1$ elements of V are linearly dependent. (**Hint :** Proceed as in the Example given in the class which uses only cardinality argument.)

T3.17 What is the rank of $\mathbb{Q}$ as an abelian group?

T3.18 Let K be a field, I be a set and let $g \in K^I$ be a function on I into K, such that the image $\mathrm{im}(g)$ is an infinite subset of K. Then the powers g^ν, $\nu \in \mathbb{N}$ of g are linearly independent over K. (For example from this it follows that: the functions $t \mapsto \cos^\nu t$, $\nu \in \mathbb{N}$, from $\mathbb{R}$ to itself are linearly independent; similarly, the functions $x \mapsto x^\nu$, $\nu \in \mathbb{N}$, from K to itself for an arbitrary infinite field K, are linearly independent.)

T3.19 Let L be a division ring, K be a subdivision ring of L and I be a set. For an arbitrary family $(f_j)_{j\in J}$ of functions $f_j \in K^I$ show that: the f_j, $j \in J$, are linearly independent over K if and only if they are linearly independent over L as a family of functions in L^I. (Use the exercise 6 and and exercise 4.11(a).)

†**T3.20** Let A be a ring and let J be an indexed set with cardinality of the continuum. Then there exists a family x_j, $j \in J$, of A–linearly independent 0-1–sequences in $A^{\mathbb{N}}$. (**Hint :** (H. Brenner) Let $\mathbb{P}$ be the set of prime numbers. For a subset $R \subseteq \mathbb{P}$, let $\mathrm{N}(R)$ be the set of those positive natural numbers whose prime divisors belong to R, i.e. $\mathrm{N}(R) = \{n \in \mathbb{N}^* \mid \text{prime divisors of } n \subseteq R\}$. Then the family x_R, $R \in \mathfrak{P}(\mathbb{P})$, is linearly independent, where x_R denote the indicator function of $\mathrm{N}(R)$.)