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

5. Linear Independence, Relation submodules and Free Modules

Submit a solution of ANY ONE of the *Exercise ONLY. **Due Date : Thursday, 05-03-2020**
Recommended to solve the violet colored R Exercises

5.1 Let A be a commutative ring.

(a) An element a in A is a basis of the A-module A if and only if $a \in A^\times$ is a unit in A.

(b) Suppose that $A \neq 0$. Then A is a principal ideal domain if and only if every ideal in A is a free A-submodule of A.

(c) Let V be a free A-module of infinite rank. Then $|V| = |A| \cdot \operatorname{Rank}_A V = \operatorname{Sup}\{|A|, \operatorname{Rank}_A V\}$.

5.2 **(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 $b, c \in \mathbb{R}$, 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 $\mathbb{Q}$.

5.3 **(a)** Let $a, b \in \mathbb{N}^*$ and let $d := \gcd(a,b)$ be the greatest common divisor of a and b. Then the relation submodule $\operatorname{Rel}_{\mathbb{Z}}(a,b) := \{(x,y) \in \mathbb{Z}^2 \mid xa + yb = 0\} \subseteq \mathbb{Z}^2$ is generated by $(bd^{-1}, -ad^{-1}) \in \mathbb{Z}^2$ as $\mathbb{Z}$-module.

(b) Let V be a finite free $\mathbb{Z}$-module with basis $x_1, \ldots, x_n$ and let $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ be an unimodular vector, i. e. $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n = \mathbb{Z}$. Then there exists a $\mathbb{Z}$-basis $z_1, \ldots, z_n$ of V with $z_1 = a_1x_1 + \cdots + a_nx_n$. (**Hint :** Use (without proving!) submodules of finite free $\mathbb{Z}$-modules are again free. Construct a $\mathbb{Z}$-homomorphism $\pi : V \to \mathbb{Z}$ with $\pi(z_1) = 1$. Then $V = Az_1 \oplus \operatorname{Ker} \pi$.)

5.4 In the subspace $U := \sum_{a \in \mathbb{R}} \mathbb{R} \sin(x+a) \subseteq \mathbb{R}^{\mathbb{R}}$ 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.
In particular $\operatorname{Dim}_{\mathbb{R}} \sum_{a \in \mathbb{R}} \mathbb{R} \sin(x+a) = 2$.

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

5.6 Let $n \in \mathbb{N}$ and let K be a field.

(a) Let $x_1, \ldots, x_{n+1} \in V$ be linearly dependent elements of a vector space V over the field K. Suppose that n elements among $x_1, \ldots, x_{n+1}$ are linearly independent over K. Then show that the relation subspace

$$\operatorname{Rel}_K(x_1, \ldots, x_{n+1}) := \{(a_1, \ldots, a_{n+1} \in K^{n+1} \mid a_1x_1 + \cdots + a_{n+1}x_{n+1} = 0\}$$

is 1-dimensional over K, i. e. $\operatorname{Dim}_K(\operatorname{Rel}_K(x_1, \ldots, x_{n+1})) = 1$.

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

(c) Let I be an infinite set. Then $\mathrm{Dim}_K(K^I) = |K^I|$. (**Hint:** In view of Exercise 5.1 (c), it is enough to prove that $|K| \leq \mathrm{Dim}_K K^I$. Let $\sigma : \mathbb{N} \to I$ be an injective map 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 the part (b) $(g_a)_{a \in K}$ are linearly independent over K.) — Deduce that $\mathrm{Dim}_K K^I > \mathrm{Dim}_K K^{(I)}$.

***5.7** 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 a non-zerodivisor in A if and only if a is a non-zerodivisor in B.

(b) $(\mathfrak{a}B) \cap A = \mathfrak{a}$ for every 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 $B = aB$.)

5.8 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 $U \cap W = 0$.

5.9 Let $0 \to V' \xrightarrow{f'} V \xrightarrow{f} V'' \to 0$ be a short exact sequence of A-modules over a commutative ring A and let $\mathfrak{a}$ be an ideal in A. If the sequence *splits*[1], then the canonical induced sequence $0 \to V'/\mathfrak{a}V' \xrightarrow{\overline{f'}} V/\mathfrak{a}V \xrightarrow{\overline{f}} V''/\mathfrak{a}V'' \to 0$ is also exact and splits.
(**Remark:** In general the last canonical sequence need not be exact if the initial sequence is not split. For example, consider the short exact sequence $0 \to \mathbb{Z} \xrightarrow{\lambda_2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/\mathbb{Z}2 \to 0$ of abelian groups which is not split.)

5.10 An exact sequence $V \xrightarrow{f} V'' \to 0$ of A-modules over a commutative ring A splits if V'' is a free A-module.

5.11 Let A be an *Bézout domain*[2].
(a) Every finite submodule of a finite free A-module is again free. (**Hint:** Let V be a free A-module with basis $x_1, \ldots, x_m$ and let $U \subseteq V$ be a finite A-submodule. We prove the assertion by induction on m. For $m = 0$ there is nothing to prove. Assume that $m > 0$ and let π be the projection of V onto $V'' := Ax_m$ along $V' := Ax_1 + \cdots + Ax_{m-1}$ and $f = \pi \,|\, \mathrm{Img}\, \pi$ (the restriction of π to $\mathrm{Img}\, \pi$). From the canonical short exact seqeunce :

$$0 \to V' \longrightarrow V \xrightarrow{f} V'' \to 0 \,,$$

[1] **Split Exact Sequence** An exact sequence $V \xrightarrow{f} V'' \to 0$ (resp. $0 \to V' \xrightarrow{f'} V'$) of A-modules s p l i t s if $\mathrm{Ker}\, f$ (resp. $\mathrm{Img}\, f$) is a direct summand of V. Equivalently, there exists an A-module homomorphism $g'' : V'' \to V$ (resp. $g : V \to V'$) such that $f \circ g'' = \mathrm{id}_{V''}$ (resp. $g \circ f' = \mathrm{id}_{V'}$).

A short exact sequence $0 \to V' \xrightarrow{f'} V \xrightarrow{f} V'' \to 0$ s p l i t s if $\mathrm{Img}\, f' = \mathrm{Ker}\, f$ is a direct summand of V. Equivalently, one (and hence both) of the exact sequences $0 \to V' \xrightarrow{f'} V$ and $V \xrightarrow{f} V'' \to 0$ splits. Moreover, in this case $V = \mathrm{Img}\, f' \oplus U$, where $U \subseteq V$ is an A-submodule with $f\,|U : U \xrightarrow{\sim} V''$, i. e. the restriction of f to U is an A-isomorphism of U onto V''. Therefore $V \cong V' \oplus V''$.

[2] A integral domain in which every finitely generated ideal is principal is called a B é z o u t d o m a i n. Bézout domains are named after the French mathematician Étienne Bézout (1730-1783). Every PID is a Bézout domain, but not conversely.

by restrictions we get an exact sequence

$$0 \to V' \cap U \longrightarrow U \xrightarrow{f|U} f(U) \to 0\,.$$

Now, since $f(U)$ (as the image of U) is a finite submodule of a free A-module $V'' = Ax_m$, it is a free A-module by induction hypothesis. Further, by Exercise 5.10 the last exact sequence splits and hence $U \cong f(U) \oplus (V' \cap U)$. Moreover, $V' \cap U$ is a finite A-module, since it is a direct summand of a finite A-module U and by induction hypothesis $V' \cap U$ is an A-submodule of a free A-module V' with basis $x_1, \ldots, x_{m-1}$. Altogether, this proves that U is a free A-module. •)

(b) Every finite torsion-free A-module is free. (**Hint :** Every finite torsion-free module over an integral domain is a submodule of a finite free A-module. for a proof see solution of Ecxersie 2.9 (c).)

(c) Every finite submodule of an A-module of finite presentation[3] is itself of finite presentation.

5.12 Let $f : V \to W$ be an A-module homomorphism of A-modules over a commutative ring A, where W is a *free* A-module. Further, let $\mathfrak{a} \subseteq A$ be an ideal in A.

(a) If $\mathfrak{a}$ is *nilpotent* and if f induces an isomorphism $\overline{f} : V/\mathfrak{a}V \xrightarrow{\sim} W/\mathfrak{a}W$, then f itself is an isomorphism.

(b) If $\mathfrak{a} \subseteq \mathfrak{m}_A$ (=the Jacobson-radical of A), and if V and W are finite A-modules and if f induces an isomorphism $\overline{f} : V/\mathfrak{a}V \xrightarrow{\sim} W/\mathfrak{a}W$, then f itself is an isomorphism.

(**Hint :** First show that f is surjective and then consider the split exact sequence, see Footnote No. 1

$$0 \to \operatorname{Ker} f \to V \xrightarrow{f} W \to 0.$$

— **Remark :** The assertions in the parts (a) and (b) holds also even if W is only *projective* A-module. — Recall that an A-module P is called p r o j e c t i v e over A if it is isomorphic to direct summand of a free A-module. Equivalently, every short exact sequence $0 \to V' \xrightarrow{f'} V \xrightarrow{f} P \to 0$ of A-modules splits, see Footnote No. 1.)

5.13 An A-module V over a commutative ring A is isomorphic to the dual of an A-module of finite presentation if and only if V is isomorphic to the kernel $\operatorname{Ker} f$ of an A-module homomorphism $f : F \to G$ where F and G are finite free A-modules.

5.14 Let A be a noetherian commutative ring. then every torsion-less finite A-module is isomorphic to submodule of a finite free A-module. (**Hint :** Recall the concept of a torsion-less modules from the solution of the Exercise 2.9 (c).)

R **5.15** Let x_i, $i \in I$, be a family of n-tuples from $\mathbb{Z}^n$. For a prime number p, let $\mathbb{F}_p$ 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 $\mathbb{F}_p^n$, are linearly independent over $\mathbb{F}_p$.

(iv) For almost all prime numbers p, the images of x_i, $i \in I$, in $\mathbb{F}_p^n$, are linearly independent over $\mathbb{F}_p$.

---

[3] **Finitely presented modules** Recall that an A-module V is of f i n i t e p r e s e n t a t i o n if there exists a finite generating system x_i, $i \in I$ (finite indexed set), such that the corresponding relation-module $\operatorname{rel}_A(x_i \mid i \in I)$ is also finite. Equivalently, if there exist natural numbers $m, n \in \mathbb{N}$ such that the sequence of A-modules

$$A^m \to A^n \to V \to 0$$

is exact. Note that : *Finitely generated modules over a noetherian ring A are finitely presented.*

Exercise Let V be an A-module of finite presentation and let W be a finite A-modue, $\pi : W \to V$ be a *surjective* A-module homomorphism Then $\operatorname{Ker} \pi$ is also finite A-module.

Moreover, if I is finite with $|I| = n$, then the above statements are further equivalent to the following statement

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

(**Hint :** All four conditions (i) to iv) imply that $|I| \leq n$. Consider the case $|I| = n$.)

5.16 Let x_i, $i \in I$, be a family of n–tuples from $\mathbb{Z}^n$. For every prime number p let $\mathbb{F}_p$ 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 $\mathbb{F}_p^n$, generate the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. (**Hint :** (ii) $\Rightarrow$ (i) : Let $U := \sum_{i\in I} \mathbb{Z}x_i$. Note that by the above Exercise 5.9, 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 $U = \mathbb{Z}^n$.)