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

Evaluation Weightage : Assignments : 20% **Seminars :** 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

	Grade A$^+$	Grade A	Grade B$^+$	Grade B	Grade C	Grade D	Grade F
Marks-Range	> 90	81 — 90	71 — 80	61 — 70	51 — 60	40 — 50	< 40

5. Finite algebras over a field — Hilbert's Nullstennensatz

Submit a solutions of $*$**-Exercises ONLY.** **Due Date : Wednesday, 13-09-2017**

5.1 Show that each of the following set is an algebraic set and find generators for the ideals of algebraic sets in (a), (c) and (d).

(a) Finite subsets of $\mathbb{A}^n_K$, $\in \mathbb{N}^+$. **(b)** $\{(\cos t, \sin t) \in \mathbb{A}^2_{\mathbb{R}}) \mid t \in \mathbb{R}\}$.

(c) (Twisted cubic curve) $\{(t,t^2,t^3) \in \mathbb{A}^3_K \mid t \in K\}$.

(d) $\{(t^p,t^q) \in \mathbb{A}^2_{\mathbb{C}} \mid t \in \mathbb{C}\}$, where p, q are relatively prime positive integers.

5.2 Let K be an arbitrary field and $m, n \in \mathbb{N}^+$.

(a) If we identify $\mathbb{A}^2_K$ with $\mathbb{A}^1_K \times \mathbb{A}^1_K$ in a natural way, show that the Zariski topology on $\mathbb{A}^2_K$ is not the product of the Zariski topologies on the two copies of $\mathbb{A}^1_K$. Compare these two topologies.

(b) Show that the Zariski topology on $\mathbb{A}^n_K$ is Hausdroff if and only if K is finite.

(c) Show that the Zariski topology of $\mathbb{A}^n_{\mathbb{R}}$ (resp. $\mathbb{A}^n_{\mathbb{C}}$) is weaker than the usual topology on $\mathbb{A}^n_{\mathbb{R}}$ (resp. $\mathbb{A}^n_{\mathbb{C}}$).

(d) If $m \leq n$ and we identify $\mathbb{A}^m_K$ as a subset of $\mathbb{A}^n_K$ via the natural inclusion $\varphi : \mathbb{A}^m_K \to \mathbb{A}^n_K$ given by $\varphi(a_1,\ldots,a_m) \mapsto (a_1,\ldots,a_m,0,\ldots,0)$. Then show that the Zariski topology on $\mathbb{A}^m_K$ is the relative topology from the Zariski topology on $\mathbb{A}^n_K$. Moreover, if W is an algebraic set in $\mathbb{A}^m_K$ then $\varphi(W)$ is an algebraic set in $\mathbb{A}^n_K$. What is the relation between the ideals $I_K(W)$ and $I_K(\varphi(W))$?

(e) Give an example to show that the image of an algebraic set under the natural projection map $\mathbb{A}^2_K \to \mathbb{A}^1_K$ need not be an algebraic set.

5.3 Let L be a line, $H = \mathrm{V}(f)$ be a hypersurface and V be an algebraic set in $\mathbb{A}^n_K$. Show that

(a) Either $\mathrm{L} \subseteq H$ or $\mathrm{L} \cap H$ is a finite set of at most $d = \deg f$ points.

(b) Either $\mathrm{L} \subseteq V$ or $\mathrm{L} \cap V$ is a finite set of points. (How many!)

(c) Let $\mathcal{C} = \mathrm{V}(f)$ and $\mathcal{C}' = \mathrm{V}(f')$ be two plane curves in $\mathbb{A}^2_K$. If f and f' are relatively prime in $K[X_1,X_2]$ then show that $\mathcal{C} \cap \mathcal{C}'$ is a finite set of at most $d \cdot d'$ points , where $d = \deg f$ and $d' = \deg f'$. (**Hint :** Reduce to the case $f \in K[X_1]$ and $f' \in K[X_2]$ and then use (a).)

S5.1 Show that each of the following set is *not* an algebraic set

(1) $\{(x,y) \in \mathbb{A}^2_{\mathbb{R}} \mid y = \sin x\}$. (2) $\{(x,y) \in \mathbb{A}^2_{\mathbb{R}} \mid y = \cos x\}$. (3) $\{(x,y) \in \mathbb{A}^2_{\mathbb{R}} \mid y = e^x\}$.

(4) $\{(z,w) \in \mathbb{A}^2_{\mathbb{C}} \mid |z|^2 + |w|^2 = 1\}$. (5) $\{(\cos t, \sin t, t) \in \mathbb{A}^3_{\mathbb{R}} \mid t \in \mathbb{R}\}$. (6) $\bigcup_{m \in \mathbb{N}} \mathrm{L}_m$, where L_m is the line $\mathrm{V}(Y - mX)$. (This shows that arbitrary (in fact, even countable) union of algebraic sets need not be an algebraic set. — **Hint :** Use the exercise (1.5)(b).)

5.4 Let K be an arbitrary field.

(a) If K is infinite then show that $\mathrm{I}_K(\mathbb{A}^n_K) = 0$. In particular, if K is infinite, then $\mathbb{A}^n_K$ is irreducible.

(b) If K is finite then find a set of generators for $\mathrm{I}_K(\mathbb{A}^n_K) = 0$. Deduce that if K is finite, then $\mathbb{A}^n_K$ is not irreducible.

5.5 Let $L \mid K$ be a field extension with L infinite. For $f_1,\ldots,f_n \in K[T_1,\ldots,T_m]$, put

$$V_0 := \{(f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m)) \in \mathbb{A}^n_L \mid (t_1,\ldots,t_m) \in \mathbb{A}^m_L\}.$$

(a) Show by an example that V_0 need not be an K-algebraic set.

(b) Show that the closure V in $\mathbb{A}^n_L$ (in the Zariski topology) of the set V_0 is an irreducible K-algebraic set. (**Hint :** In fact $V = \mathrm{V}(\mathfrak{a})$, where $\mathfrak{a}$ is the kernel of the K-algebra homomorphism $K[X_1,\ldots,X_n] \to K[T_1,\ldots,T_m]$, defined by $X_i \mapsto f_i$ for every $i = 1, \ldots, n$. — In this situation one says that V is given by a polynomial parametrization with parameters $T_1, \ldots, T_m$. If $m = 1$ and $f_i = T^{d_i}$, $i = 1, \ldots, n$, for some positive integers $d_1, \ldots, d_n$ then we say that V is a monomial curve given by the sequence $d_1, \ldots, d_n$ of positive integers.)

(c) Assume that $K = L$ is algebraically closed and $K[T_1, \ldots, T_m]$ is integral over $K[f_1, \ldots, f_n]$, then show that V_0 is closed, that is, $V_0 = V$.

5.6 **(a)** A finite commutative reduced $\mathbb{C}$-algebra $\neq 0$ is isomorphic to a product algebra $\mathbb{C}^n$, $n \in \mathbb{N}$, where n is determined uniquely by the isomorphism type of the algebra. Every such a $\mathbb{C}$-algebra is cyclic.

(b) A finite commutative $\mathbb{R}$-algebra $\neq 0$ is isomorphic to a product algebra $\mathbb{R}^m \times \mathbb{C}^n$, $m, n \in \mathbb{N}$,where the natural numbers m, n are determined uniquely by the isomorphism type of the algebra. Every such $\mathbb{R}$-algebra is cyclic.

5.7 Let K be a field. If the unit group $K^\times$ of K is finitely generated, then K is finite. (One can generalise this result to commutative rings which has only finitely many maximal ideals. — Such rings are called semilocal. See "Bemerkungen über die Einheitengruppen semilokaler Ringe", Math. Phys. Semesterberichte **17**, 168-181(1970).)

5.8 Let K be a field. If K is finite type over $\mathbb{Z}$, then K is finite. (**Hint:** If $\operatorname{Char} K = 0$, then show that $\mathbb{Q}$ is finite type over $\mathbb{Z}$-algbera.)

5.9 The Hilbert's Nullstellensatz (HNS3) can be easily proved for uncountable fields (for example, for $\mathbb{R}$ and $\mathbb{C}$) as follows:

Let K be a countable field and L be a field which is finite type over K, $L = K[x_1, \ldots, x_n]$. If $x \in L$ is not algebraic over K, then the elements $(x - a)^{-1}$, $a \in K$, are K-linearly independent On the other hand $\operatorname{Dim}_K L$ is countable. (**Remark:** Analogously one proves: Let K be a uncountable field and L be a field. If L is generated as an K-algebra by x_i, $i \in I$, with $\operatorname{Card} I < \operatorname{Card} K$. Then every $x \in L$ is algebraic over K.)

5.10 Let K be a field, $P := K[X_1, \ldots, X_n]$ and $\mathfrak{m}$ be a maximal ideal in P. Then there exists a generating system $f_1, \ldots, f_n$ of the ideal $\mathfrak{m}$ of the form $f_i \in K[X_1, \ldots, X_i]$, $1 \leq i \leq n$. (**Hint:** Induction on n. Let $A := K[X_1, \ldots, X_{n-1}]$, $\mathfrak{n} := \mathfrak{m} \cap A$. Show that $\mathfrak{m}/\mathfrak{n}P$ is a principal ideal in $P/\mathfrak{n}P \cong (A/\mathfrak{n})[X_n]$.)

5.11 Let K be a field. A commutative K-algebra of finite type in aritinian if and only if it is finite over K. (**Hint:** Use HNS3.)

5.12 Let K be a field which is *not* algebraically closed.

(a) For every $m \in \mathbb{N}_+$, there exists a non-constant polynomial $f_m \in K[X_1, \ldots, X_m]$ whose zero-set in K^m is singleton $\{0 = (0, \ldots, 0)\}$, i.e. $\mathrm{V}_K(f) = \{(0, \ldots, 0)\}$. (**Hint:** Induction on m. For $m \geq 2$, put $f_{m+1} = f_2(f_m, X_{m+1})$.)

(b) Every K-algebraic set $V \subseteq K^n$,$n \geq 1$, is a hypersurface in K^n, i.e. it is the zero-set of a single polynomial, in sympols: $V = \mathrm{V}_K(f)$ with $f \in K[X_1, \ldots, X_n]$. (**Hint:** Use (a).)

5.13 (Generalisation of HNS1) Let K be an arbitrary field, S be the set of all polynomials in $K[X_1, \ldots, X_n]$ that have no zeros in K^n, i.e. $S := \{f \in K[X_1, \ldots, X_n] \mid \mathrm{V}_K(f) = \emptyset\}$ and let $\mathfrak{a}$ be an ideal in $K[X_1, \ldots, X_n]$. If $S \cap \mathfrak{a} = \emptyset$, then $\mathrm{V}_K(\mathfrak{a}) \neq \emptyset$. (**Hint:** Use the Exercise ???.)

5.14 (HNS4) Let K be an algebraically closed field. Then the map $K^n \to \operatorname{Spm} K[X_1, \ldots, X_n]$, $a \mapsto \mathfrak{m}_a = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ is bijective. Moreover, for any ideal $\mathfrak{a} \in \mathfrak{I}(K[X_1, \ldots, X_n]$, $a \in \mathrm{V}_K(\mathfrak{a})$ if and only if $\mathfrak{a} \subseteq \mathfrak{m}_a$.

5.15 Let $E \,|\, K$ be an arbitrary field extension and $\mathfrak{a} \subsetneq K[X_1, \ldots, X_n]$ be a non-unit ideal. Then the extended ideal $\mathfrak{a}E[X_1, \ldots, X_n] \subsetneq E[X_1, \ldots, X_n]$ is also a non-unit ideal. (**Hint:** Apply HNS1 to the field extension $\overline{E} \,|\, K$, where $\overline{E}$ denote an algebraic closure of E.)

5.16 Prove the equivalence of HNS4 and HNS1. (**Hint:** Use the above Exercise.)

S5.1 In this exercise we want to collect the fundamental properties of the product algebras K^I, where K is a field and I is *finite* set. K^I is the K-algebra of all functions $I \to K$. Any map $f : I \to J$ of finite sets induces a K-algebra homomorphism $f^* : K^J \to K^I$, $\psi \mapsto \psi f$.

(a) Let $\mathrm{Idp}(K^I)$ be the set of all idempotent elements in K^I. As for any commutative ring, this set is a Boolean ring with addition $e \rhd f := (e-f)^2$ and with multiplication of the given ring. Let $e_i := (\delta_{ij})_{j\in I} \in K^I$, $i \in I$. Show that the map $J \mapsto e_J := \sum_{j\in J} e_j$ is an isomorphism $\mathfrak{P}(I) \to \mathrm{Idp}(K^I)$ of Boolean rings, where the power set $\mathfrak{P}(I) = \mathbb{F}_2^I$ carries the canonical Boolean ring structure. In particular, $e_i, i \in I$ are the principal idempotents of K^I which are, by definition, the atoms in the Boolean ring $\mathrm{Idp}(K^I)$. (Remember that in any Boolean ring B, $a \le b$ if and only if $ab = a$, is the canonical order on B.)

(b) Let $\mathcal{R}$ be the set of all equivalence relations on (the finite set) I with $|I| = n$. The cardinality $|\mathcal{R}|$ is, by definition, the n-th Bell number. For $R \in \mathcal{R}$, we denote by π_R the canonical projection $I \to I/R$. Show that the map $R \mapsto C_R := \mathrm{Im}\,(\pi_R^*)$ is an order reversing bijection of $\mathcal{R}$ onto the set of all K-subalgebras of K^I. The inverse map is given by $C \mapsto R_C$, where for a K-subalgebra $C \subseteq K^I$, $R_C \in \mathcal{R}$ is the equivalence relation

$$i \equiv_C i' \quad \text{if and only if} \quad \varphi(i) = \varphi(i') \quad \text{for all } \varphi \in C.$$

In particular, the set of K-subalgebras of K^I is finite of cardinality β_n, and any K-subalgebra of K^I is again isomorphic to a product K-algebra K^J, more precisely, $C_R \cong K^{I/R}$ for all $R \in \mathcal{R}$. With the notation of the part a), the principal idempotents of C_R are $e_X \in K^I$, $X \in I/R$. — For an element $x = (x_i)_{i\in I} \in K^I$, the subalgebra $K[x]$ generated by x is C_R where R is the equivalence relation

$$i \equiv_x i' \quad \text{if and only if} \quad x_i = x_{i'}\,.$$

In particular, $K[x] = K^I$ if and only if the components of x are pairwise distinct. The K-algebra K^I has a primitive element if and only if $|K| \ge n = |I|$. (Remember that, in general, a primitive element of an algebra is a generating element of the given algebra.)

(c) The map $J \mapsto \mathfrak{a}_J := K^I e_J$ is an order preserving bijection from $\mathfrak{P}(I)$ onto the set of all ideals in K^I. The inverse map is given by $\mathfrak{a} \mapsto \mathrm{D}(\mathfrak{a}) := I \setminus \mathrm{V}(\mathfrak{a})$, where

$$\mathrm{V}(\mathfrak{a}) := \{i \in I \mid \varphi(i) = 0 \ \text{ for all } \ \varphi \in \mathfrak{a}\}\,.$$

($\mathfrak{a} \mapsto \mathrm{V}(\mathfrak{a})$ is an order reversing bijection.) The quotient algebra $K^I/\mathfrak{a}_J$ is isomorphic to $K^{I\setminus J} = K^{\mathrm{V}(\mathfrak{a}_J)}$. In particular, the map $i \mapsto \mathfrak{m}_i := \{\varphi \in K^I \mid \varphi(i) = 0\} = \mathfrak{a}_{I\setminus\{i\}}$ is a bijection of I onto $K\text{-}\mathrm{Spec}\,K^I = \mathrm{Spm}\,K^I = \mathrm{Spec}\,K^I$. For an arbitrary ideal $\mathfrak{a} \subseteq K^I$, one has $\mathfrak{a} = \bigcap_{i\in \mathrm{V}(\mathfrak{a})} \mathfrak{m}_i$.

S5.2 Let K be a field. Two elements x, y in a K-algebra A are said to be conjugate over K if they are algebraic over K and if they have the same minimal polynomial over K.

(a) Let $L|K$ be a normal field extension. Show that $x, y \in L$ are conjugate over K if and only if there exists a K-algebra automorphism $\psi : L \to L$ such that $\psi(x) = y$.

(b) Let $L|K$ be a normal field extension and let L_1 be an intermediary field such that every polynomial in $K[X]$ which has a zero in L has a zero in L_1. Then show that $L = L_1$. (**Hint:** One can easily reduce to the case that L is finite over K. If K is finite, then the assertion easily from that fact that L has a primitive element. Now, if K is infinite and if $\varphi_1, \ldots, \varphi_r$ are all K-automorphisms of L, then $L = \bigcup_{i=1}^r \varphi_i(L_1)$ by the part a) and hence $L = L_1$.)

S5.3 Let K be a field, A be a K-algebra, $a_1, \ldots, a_n \in K$ be distinct elements and let $x \in A$ be such that $x - a_1, \ldots, x - a_n$ are units in A. Then $1, x, \ldots, x^{n-1}$ are linearly independent over K if and only if the elements $(x-a_1)^{-1}, \ldots, (x-a_n)^{-1}$ are linearly independent over K. (**Proof:** Put $y_i = (x-a_i)^{-1}$ and $y := \prod_{i=1}^n (x-a_i)$. Then $y \in A^\times$ and if $y_1, \ldots, y_n$ are linearly independent over K, then $yy_1, \ldots, yy_n$ linearly independent over K in $K + Kx + \cdots Kx^{n-1}$. Conversely, if $1, x, \ldots, x^{n-1}$ are linearly independent over K and if $b_1y_1 + \cdots + b_ny_n = 0$ with $b_i \in K$, then multiply by y and compute the co-efficient of x^{n-1} to get $b_1 + \cdots + b_n = 0$. Therefore $0 = \sum_{i=1}^n b_i(y_i - y_n) = \sum_{i=1}^{n-1} b_i(a_i - a_n)y_iy_n$ and so $y_1, \ldots, y_n$ are linearly independent over K by induction on n. •)

S5.4 Let K be a *finite* field and $f \in K[X_1, \ldots, X_n]$.

(a) (Chevalley's Theorem) If $0 \in \mathrm{V}_K(f)$ and $n > \deg(f)$, then $\mathbf{V}(f)$ has a non-trivial K-rational point $a \in K^n$, $a \ne 0$. (**Proof:** Suppose on the contrary that $\mathrm{V}_K(f) = \{0\}$. — Use the following simple Lemma **??**. Put $F = 1 - f^{q-1}$. Then $R(F) = \prod_{i=1}^n (1 - X_i^{q-1})$. (check this equality by evaluating both sides on every $a \in K^n$ and using (2.a), (2.d) and (1) in the Lemma **??**). Now, use (2.b) to get $(q-1)\cdot\deg(f) = \deg(F) \ge \deg(R(F)) = \deg(\prod_{i=1}^n (1 - X_i^{q-1})) = (q-1)\cdot n$ and so $\deg(f) \ge n$. a contradiction. •

5.S.1 Lemma *Let K be a finite field with q elements and $f, g \in K[X_1, \ldots, X_n]$. Then*
(1) *If $\deg_{X_i}(f) \le q-1$ for every $i = 1, \ldots, n$ and $f(a) = 0$ for every $a \in K^n$ then $f = 0$.*
(2) *There exists a unique polynomial $R(f) \in K[X_1, \ldots, X_n]$ such that:* **(2.a)** $\deg_{X_i}(R(f)) \le q-1$ *for all $i = 1, \ldots n$.* **(2.b)** $\deg(R(f)) \le \deg(f)$. **(2.c)** $R(f+g) = R(f) + R(g)$. **(2.d)** *The polynomial function $f - R(f) : K^n \to K$ is the zero function, that is, $f(a) = R(f)(a)$ for every $a \in K^n$.*)

(b) If f is homogeneous of degree 2 and $n \geq 3$, then $\mathrm{V}_K(f)$ has a non-trivial K-rational point. (**Hint:** Use Chevalley's Theorem in (a).)

S5.5 Let $L\,|\,K$ be a field extension. A K-algebraic set $V \subseteq L^n$ is called a K-cone (with vertex at the origin) if $V = \mathrm{V}_L(F_1,\ldots,F_r)$ for some homogeneous polynomials $F_1,\ldots,F_r \in K[X_1,\ldots,X_n]$. For an algebraic set $V \subseteq K^n$, show that V is a cone if and only if for each $a \in V$, $a \neq 0$, the line $\mathrm{L}(a,0)$ joining a and 0 is contained in V.

S5.6 Let $L\,|\,K$ be a *normal* field extension. Two points $a = (a_1,\ldots,a_n)$ and $b = (b_1,\ldots,b_n) \in L^n$ are called K-conjugates if there exists a K-automorphism σ of L such that $\sigma(b_i) = a_i$ for every $i = 1,\ldots n$.

(a) Let $V \subseteq L^n$ be an K-algebraic set . If $a \in V$, then V contains all K-conjugates of a.

(b) Let $V \subseteq L^n$ be a finite set of points with the property that : if $a \in V$ then V contains all K-conjugates of a. Then show that V is a K-algebraic set. (**Hint:** If $a \in L^n$, then there exist an ideal $\mathfrak{a} \subseteq K[X_1,\ldots,X_n]$ and a K-algebra isomorphism $K[a_1,\ldots,a_n] \cong K[X_1,\ldots,X_n]/\mathfrak{a}$.)

S5.7 Let $L\,|\,K$ be a field extension and $V \subseteq L^n$ be an L-algebraic set. Then the set $V_K := V \cap K^n$ of all K-rational points of V is an K-algebraic set in K^n.

S5.8 Let $\mathbb{Z}^n := \{(a_1,\ldots,a_n) \mid a_i \in \mathbb{Z} \text{ for every } i = 1,\ldots,n\}$ be the set of lattice points. If V is an algebraic set in $\mathbb{C}^n$ with $\mathbb{Z}^n \subseteq V$, then show that $V = \mathbb{C}^n$.