MA 315 Galois Theory / January-April 2013

(Int. PhD, ME, MSc, PhD Programmes)

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** dppatil@csa.iisc.ernet.in / patil@math.iisc.ernet.in

Lectures : Monday and Wednesday ; 11:00–12:30 **Venue:** MA Lecture Hall I

1-st Midterm : Monday, February 18, 2013; 11:00 -13:00 **2-nd Midterm :** Saturday, March 16, 2013; 10:30 -12:30
Final Examination : ???, April ??, 2013, 09:00 -12:00

Evaluation Weightage : Midterms (Two) : 50% **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

1. Zeros of Polynomials

Monday, January 23, 2013

1.1 Let k be a field and let $f := a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in k[X]$ be a polynomial. Further, let $f_0 := a_0 + a_2X + a_4X^2 + \cdots$ and $f_1 := a_1 + a_3X + a_5X^2 + \cdots$. Show that $X^2 - a$ divides f in $k[X]$ if and only if $f_0(a) = f_1(a) = 0$. (**Hint :** Divide f by $X^2 - a$.)

1.2 Let A be an infinite integral domain and let $f, g, h \in A[X_1, \ldots, X_n]$, $h \neq 0$ be polynomials such that $f(a) = g(a)$ for all $a \in A^n$ whenever $h(a) \neq 0$. Show that $f = g$. (**Hint :** Use the following well-known: **Identity Theorem for Polynomials:** *Let A be an integral domain and let $f, g \in A[X_1, \ldots, X_n]$ be two polynomials such that the partial degrees $\deg_{X_i} f$ and $\deg_{X_i} g$ with respect to the indeterminate X_i is $\leq r_i \in \mathbb{N} \cup \{-\infty\}$ for all $i = 1, \ldots, n$. Further, assume that there are subsets $N_1, \ldots, N_n$ of A such that $\# N_i > r_i$ for all $i = 1, \ldots, n$. If $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ for all $(a_1, \ldots, a_n) \in N_1 \times \cdots \times N_n$, then $f = g$.*)

1.3 Let A be a non-zero commutative ring. Show that the canonical map $\Phi : A[X] \to A^A$, defined by $f \mapsto (A \to A, a \mapsto f(a))$ is surjective if and only if A is a finite field. Moreover, in this case, prove that the kernel $\operatorname{Ker} \Phi$ is generated by the monic polynomial $X^q - X$. (**Hint :** Use Division with remainder and the Identity Theorem given in the Hint of Exercise 1.2.)

1.4 Let k be an infinite field and let $K|k$ be a field extension of k, $f \in k[X_1, \ldots, X_n]$ be a polynomial and let

$$\mathscr{E} \; : \quad a_{i1}x_1 + \cdots + a_{in}x_n = b_i\,, \qquad i = 1, \ldots, m\,,$$

be a system of linear equations with coefficients $a_{ij}, b_i \in k$. Suppose that the system $\mathscr{E}$ has a solution $(x_1, \ldots, x_n) \in K^n$ with $f(x_1, \ldots, x_n) \neq 0$. Then show that the system $\mathscr{E}$ also has a solution $(y_1, \ldots, y_n) \in k^n$ with $f(y_1, \ldots, y_n) \neq 0$. (**Hint :** Let $n - r$ be the rank of the system $\mathscr{E}$. The entire solution spaces $L_k(\mathscr{E})$ (over k) and $L_K(\mathscr{E})$ (over K) of the system $\mathscr{E}$ are determined by a solution $x = (x_1, \ldots, x_n) \in k^n$ and solutions $x^{(\rho)} = (x_1^{(\rho)}, \ldots, x_n^{(\rho)}) \in k^n$, $\rho = 1, \ldots, r$, which generate the solution spaces $L_k(\mathscr{E}_0)$ and $L_K(\mathscr{E}_0)$ of the corresponding homogenous system $\mathscr{E}_0$ over k as well as over K. Substitute this resulting parametrization of the solution space $L_K(\mathscr{E})$ in the polynomial f and use the Identity Theorem.)

1.5 Let A be a commutative ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise comaximal ideals in A and $\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Suppose that the polynomial $f \in A[X]$ has a zero in every quotient ring $A/\mathfrak{a}_i$, $i = 1 \ldots, n$. Show that f has also a zero in the quotient ring $A/\mathfrak{a}$. (**Hint :** – Recall that two ideal $\mathfrak{a}, \mathfrak{b}$ in a (commutative) ring A are said to c o m a x i m a l if the sum ideal $\mathfrak{a} + \mathfrak{b} = A$. For example, the ideals $\mathbb{Z}n$ and $\mathbb{Z}m$ in the ring $\mathbb{Z}$ are comaximal if and only if m and n are relatively prime. Use the following well-known **Chinese Remainder Theorem**: *The canonical ring homomorphism $\pi : A \to \prod_{i=1}^n A/\mathfrak{a}_i$ defined by $a \mapsto (\pi_1(a), \ldots, \pi_n(a))$, where $\pi_i : A \to A/\mathfrak{a}_i$, $i = 1, \ldots, n$ are the canonical projections, is surjective and moreover, the kernel $\operatorname{Ker} \pi$ of π is the intersection $\cap_{i=1}^n \mathfrak{a}_i$. In particular, π induces the isomorphism $A/\cap_{i=1}^n \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^n A/\mathfrak{a}_i$.*)

1.6 Let $f \in \mathbb{Z}[X]$ be a polynomial of positive degree. Show that there are infinitely many prime numbers p such that the polynomial f has a zero in $\mathbb{Z}/\mathbb{Z}p$. (**Hint :** Show by using Taylor's formula the values $f(x) \neq 0$ for $x \in \mathbb{N}^*$ have altogether have infinitely many prime divisors: For $x \in \mathbb{N}^*$, there exists an integer $y \in \mathbb{Z}$ such that $f\left(x + f(x)^2\right) = f(x) + f(x)^2 y = f(x)\,(a + f(x)y)$. But not all $|f(x)|$, $x \in \mathbb{N}^*$ are prime numbers.)

Below one can see auxiliary results and (simple) Test-Exercises.

Auxiliary Results/Test-Exercises

To understand and appreciate the Test-Exercises which are marked with the symbol † one may possibly require more mathematical maturity than one has! These are steps towards applications to various other branches of mathematics, especially to Analysis, Number Theory and Algebraic Geometry.

T1.1 **(a)** How many zeros the polynomial X^2+X in $\mathbb{Z}_6$?

(b) The polynomial $X^3+X^2+X+1 \in \mathbb{Z}_4[X]$ is a multiple of both $X+1$ and $X+3$, but not of the product $(X+1)(X+3)$.

(c) Give an example of a commutative ring A such that the polynomial X^2-X has infinitely many zeros in A.

(d) Compute the zeros and the two top coefficients of the polynomial over Z defined by the following determinant:

$$\operatorname{Det}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & X+1 & 1 & \cdots & 1 \\ 1 & 1 & X+2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & X+n \end{pmatrix}$$

(e) For which prime numbers p, the polynomial $X^5+6X-20$ is divisible by X^2+2 in the polynomial ring $k[X]$ in one indeterminate over a field k of charateristic p ?

(f) Let $f_1,\ldots,f_n \in A[X]$ be polynomials in one indeterminate over a commutative ring A of degrees $\leq n-2$ and let $a_1,\ldots,a_n \in A$ be arbitrary elements. Show that :

$$\operatorname{Det}\big(f_i(a_j)\big)_{1\leq i,j\leq n} = 0\,.$$

T1.2 Let $K|k$ be a field extension and let $f,g \in k[X] \subseteq L[X]$. Show that g divides f in the ring $k[X]$ if and only if g divides f in the ring $K[X]$.

T1.3 Let $a,b,c \in \mathbb{N}$ be natural numbers. Show that $X^{3a+2}+X^{3b+1}+X^{3c} \in \mathbb{Z}[X]$ is divisible by X^2+X+1.

T1.4 Let A be an infinite integral domain and let $f \in A[X_1,\ldots,X_n]$. Show that f is homogeneous of degree r if and only if $f(aX_1,\ldots,aX_n) = a^r f(X_1,\ldots,X_n)$.

†**T1.5** Show that the polynomials

$$f := (X^2-2)(X^2+7)(X^2+14) \quad \text{and} \quad g := (X^2-2)(X^2-17)(X^2-34)$$

have zeros in every proper quotient ring $\mathbb{Z}/\mathbb{Z}n$ of the ring of integers $\mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, but have no zeroes in the field $\mathbb{Q}$ of rational numbers. (**Hint :** Use the following Exercise from Elementary Number Theory: *Let a and b be relatively prime integers. Suppose that every prime divisor p of a (respectively, of b), b (respectively, a) is a quadratic residue modulo p. Further assume that one of the numbers a, b, ab is congruent modulo* 1 *modulo* 8*. Then show that for every* $m \in \mathbb{N}^*$, *the equation* $(x^2-a)(x^2-b)(x^2-ab) \equiv 0 \,(\mathrm{mod}\, m)$ *has a solution.* For the solution of this Exercise one might need to use the elementary facts about the unit group $\mathbb{Z}_m^\times$ and quadratic residues.)

T1.6 (Taylor's Formula) Let I be any indexed set (for example, $I=\{1,2,\ldots,n\}, n\in\mathbb{N}$) and let A be an arbitrary commutative ring. Let $f \in A[X_i \mid i \in I]$ and let $a=(a_i)_{i\in I} \in A^I$. The coefficients $b_\nu \in A$, $\nu \in \mathbb{N}^{(I)}$, in the Taylor's expansion

$$f = \sum_{\nu\in\mathbb{N}^{(I)}} b_\nu (X-a)^\nu$$

are determined by the following equations:

$$\nu\,!\,b_\nu = (\partial_\nu f)\,(a)\,, \quad \nu \in \mathbb{N}^{(I)}\,.$$

Moreover, if $m = m \cdot 1_A$ are all units in A for all $m \in \mathbb{N}^*$ (for example, $A = \mathbb{Q}$ or $A = k$ is any field of characteristic 0), then the above formula can be represented as:

$$f = \sum_{\nu \in \mathbb{N}^{(I)}} \frac{(\partial_\nu f)(a)}{\nu\,!} (X - a)^\nu$$

and is called the Taylor's expansion of $f \in A[X_i \mid i \in I]$ at the point $a \in A^I$.

(**Remarks:** Note that above we have used the standard notation from the Calculus of severable variables: For each $j \in I$, $\partial_j := \partial / \partial X_j$ is the j-th partial derivatives of $A[X_i \mid i \in I]$; $\partial_j : A[X_i \mid i \in I] \to A[X_i \mid i \in I]$ is an A-linear endomorphism of $A[X_i \mid i \in I]$ which also satisfy the product-rule: $\partial_j(fg) = f\partial_j(g) + g\partial_j(f)$ for all $f, g \in A[X_i \mid i \in I]$. This means that ∂_j is a A-derivation of the polynomial ring $A[X_i \mid i \in I]$. Moreover, ∂_j, $j \in I$, are pairwise commutative, i. e. $\partial_j \partial_k = \partial_k \partial_j$ for all $j, k \in I$ (this is immediate from the fact that ∂_j is uniquely determined by its values $\partial_j(X_i)$ on the indeterminates X_i, $i \in I$).

Therefore, for arbitrary $\nu = (\nu_i) \in \mathbb{N}^{(I)}$, $\partial_\nu := \dfrac{\partial^{|\nu|}}{\partial X^\nu} = \prod_{i \in I} \partial_i^{\nu_i}$ is a well-defined A-linear endomorphism of $A[X_i \mid i \in I]$. In case of one variable, i. e. $I = \{1\}$ and $X = X_1$; it is $\dfrac{\mathrm{d}}{\mathrm{d}X^\nu}$ and instead of $\dfrac{\mathrm{d}f}{\mathrm{d}X^\nu}$ one can also use the short notation $f^{(\nu)}$ (called the ν-th derivative of f). For multi-index $\nu = (\nu_i) \in \mathbb{N}^{(I)}$, we have used the short notation: $|\nu| = \sum_{i \in I} \nu_i$, $\nu = \prod_{i \in I} \nu_i\,!$, $X^\nu = \prod_{i \in I} X_i^{\nu_i}$.)

(a) Let A be an integral domain, $a \in A$ and let $f \in A[X]$, $f \neq 0$. For $i \in \mathbb{N}$, let $f^{(i)} := \dfrac{\mathrm{d}f}{\mathrm{d}X^i}$ be the i-th derivative of f. then:

(1) If a is a zero of f with multiplicity ν, then $f^{(i)}(a) = 0$ for all $i = 0, \ldots, \nu - 1$. Moreover, if $\nu\,!$ is not a zero divisor in A, then $f^{(\nu)}(a) \neq 0$.

(2) (Converse of (1)) If $\nu\,!$ is not a zero divisor in A and if $f^{(i)}(a) = 0$ for all $i = 0, \ldots, \nu - 1$ and $f^{(\nu)}(a) \neq 0$, then ν is the multiplicity of the zero a of f.

In particular, if the characteristic $\operatorname{Char} A = 0$, then the multiplicity of f at $a \in A$ is the smallest natural number $\nu \in \mathbb{N}$ with $f^{(\nu)}(a) \neq 0$. (**Hint :** Use Taylor's Formula $f = \sum_{i \in \mathbb{N}} b_i (X - a)^i$, where $i\,! b_i = f^{(i)}(a)$.)

(b) (Polynomial Theorem) Let A be a commutative ring and let $a_1, \ldots, a_r \in A$ be arbitrary elements. Then for every $n \in \mathbb{N}$, we have the formula:

$$(a_1 + \cdots + a_r)^n = \sum_{\nu = (\nu_1, \ldots, \nu_r) \in \mathbb{N}^r,\ |\nu| = n} \frac{n\,!}{\nu\,!} a^\nu .$$

(**Hint :** For a proof use the Kronecker's method of indeterminates. For this, let $\Phi : \mathbb{Z}[X_1, \ldots, X_r] \to A$ be the substitution homomorphism $X_i \mapsto a_i$, $i = 1, \ldots, r$. Clearly, the formula for $X_1, \ldots, X_r$ implies the formula for $a_1, \ldots, a_r$. We therefore restrict to calculate g^n for $g := X_1 + \cdots + X_r$. By the Taylor's formula $g^n = \sum_{|\nu| = n} a_\nu X^\nu$ where $\nu\,! a_\nu = (\partial_\nu g^n)(0)$.)

(c) Let k be a field of characteristic 0. Show that all zeroes of the n-th truncated exponential polynomial $E_n := 1 + X + X^2/2\,! + \cdots + X^n/n\,!$, $n \in \mathbb{N}^*$, are simple, i.e. of multiplicity one. (**Hint :** Note that $\frac{\mathrm{d}}{\mathrm{d}X}(E_n) = E_n' = E_{n-1}$ for every $n \in \mathbb{N}^*$.)

T1.7 Let $f \in \mathbb{R}[X]$ be a non-constant polynomial which has only real zeroes. Show that:

(a) If a is a zero of the derivative f' of f, then a is also a zero of f. (**Hint :** Use Rolle's theorem.)

(b) $(f'(a))^2 \geq f(a) f''(a)$ for all $a \in \mathbb{R}$. (**Hint :** Let $a_1, \ldots, a_n \in \mathbb{R}$ be all zeroes (may be repeated!) of f. Then $f'(x) = \sum_{i=1}^n \frac{f(x)}{(X - a_i)}$ for all $x \notin \{a_1, \ldots, a_n\}$. The product rule of differentiation yields $\frac{f'(x)}{f(x)} = \sum_{i=1}^n \frac{1}{(X - a_i)}$. Differentiate this equation again.)

T1.8 We recall here some consequences of the Intermediate Value theorem for real polynomials. These can be directly proved without going back to Analysis.

(a) (Rolle's Theorem) Let $f \in \mathbb{R}[X]$ be a polynomial and let $a, b \in \mathbb{R}$ be two zeroes of f with $a < b$. Then there exists $c \in (a, b)$ such that $f'(c) = 0$.

(b) (Mean-Value Theorem) Let $f \in \mathbb{R}[X]$ be a polynomial and let $a, b \in \mathbb{R}$ with $a < b$. Then there exists $c \in (a, b)$ such that $\dfrac{f(b) - f(a)}{b - a} = f'(c)$, where f' denote the derivative of f.
(**Hint :** Apply Rolle's theorem to the polynomial $g := f - f(a) - \frac{f(b)-f(a)}{b-a}(X - a)$.)

(c) Let $f \in \mathbb{R}[X]$ be a polynomial and let $a, b \in \mathbb{R}$ with $a < b$. Suppose that $f'(x) > 0$ (respectively, $f'(x) < 0$) for all $x \in (a, b)$ (respectively, $x \in (a, b)$), then show that $f(a) < f(b)$ (respectively, $f(a) > f(b)$).

T1.9 Let $f \in \mathbb{R}[X]$ be a polynomial and let $a, b \in \mathbb{R}$ with $a < b$.

(a) If $f(a) \cdot f(b) < 0$ (respectively, $f(a) \cdot f(b) > 0$), then show that the number of zeros (either every zero counted with multiplicities or otherwise every zero counted only once) of f in (a, b) is odd (respectively, even). (**Hint :** Use induction on the degree of f.)

(b) If f has no zeroes in (a, b), then show that the number of zeros (either every zero counted with multiplicities or as simple zero) of f' in (a, b) is odd.

T1.10 Let $n \in \mathbb{N}^*$ and let $L_n := \sum_{\nu=0}^{n-1} (-1)^\nu X^\nu / (\nu + 1)$ be the n-th truncated logarithm polynomial (the expansion of $\log(1 + X)$ at the point 0). Show that if n is odd (respectively, even), then L_n has no (respectively, exactly one simple zero) real zero other than 0.

T1.11 (a) Let $f \in \mathbb{R}[X]$, $f \neq 0$, and let $a \in \mathbb{R}$. Show that the polynomial $F := f + af'$ has at least as many as real zeros as f; Moreover, this assertion is also true even if one counts each zero with multiplicities. (**Hint :** Assume $a \neq 0$. If $x, y \in \mathbb{R}$, $x < y$ are zeroes of f such that f has no zeroes in (x, y), then F has odd number of zeroes counted with multiplicities in (x, y). Further, note that $\deg F = \deg f$.)

(b) Let $g \in \mathbb{R}[X]$ be a polynomial of degree $n \in \mathbb{N}$ and let $a \in \mathbb{R}$. Show that the polynomial $f := g + ag' + \cdots + a^n g^{(n)}$ have at most as many real zeroes as g (whether each zero is counted with multiplicities or as simple). (**Hint :** Use $g = f - af'$.)

(c) Let $n \in \mathbb{N}$. Show that the n-th truncated exponential polynomial $E_n := \sum_{\nu=0}^{n} X^\nu / \nu!$ has exactly one (simple) (respectively, no) real zero if n is odd (respectively, even). (**Hint :** Apply part (b) to $g := X^n / n!$ and $a := 1$.)

T1.12 (Polynomial-Interpolation) Let A be an integral domain and let $m \in \mathbb{N}$. *Whether there is a polynomial $f \in A[X]$ of degree m which takes $m+1$ given values at $m+1$ places and how does one explicit find it*, is known as Interpoltaion - Problem. Over fields the existence of f is trivial: If k is a field, $a_1, \ldots, a_{m+1} \in k$ are distinct (places) elements in k and if $b_1, \ldots, b_m \in k$ are given values in k, then (Lagrange's Interpolation-Formula):

$$f := \sum_{i=0}^{m} \frac{b_i}{c_i} \prod_{j \neq i} (X - a_j), \quad \text{where} \quad c_i := \prod_{j \neq i} (a_i - a_j), \quad i = 0, \ldots, m,$$

is the unique polynomial of degree $\leq m$ with $f(a_i) = b_i$ for $i = 0, \ldots, m$.

(Newton's interpolation) One can also proceed as follows: Since $f_j(a_j) \neq 0$, the coefficients $\alpha_0, \ldots, \alpha_m \in k$, in

$$\left(\sum_{j=0}^{r} \alpha_j f_j \right)(a_r) = b_r, \quad r = 0, \ldots, m,$$

can be recursively determined, where $f_0 := 1$, $f_1 := X - a_0$, $f_2 := (X - a_0)(X - a_1), \ldots, f_m := (X - a_0) \cdots (X - a_{m-1})$. Moreover, the polynomials $\sum_{j=0}^{r} \alpha_j f_j$ are of degree $\leq r$ and takes the values b_i at the places a_i for all $i = 0, \ldots, r$.

(Hermite-Interpolation) Let k be a field, $a_1, \ldots, a_r \in k$ be distinct elements and let $m_1, \ldots, m_r \in \mathbb{N}$ be such that $m_1! \cdots m_r!$ is not zero in k. Further, let $m := (m_1 + 1) + \cdots + (m_r + 1)$.

For given elements $b_i^{(\mu_i)}$ in k, $0 \leq \mu_i \leq m_i$, $1 \leq i \leq n$, show that there exists a unique polynomial $f \in k[X]$ of degree $< m$ such that

$$\frac{\mathrm{d}^{\mu_i} f}{\mathrm{d}X^{\mu_i}}(a_i) = b_i^{(\mu_i)}, \quad 0 \leq \mu_i \leq m_i, \quad 1 \leq i \leq n.$$

(**Hint :** The k-linear map $f \mapsto \left(\frac{\mathrm{d}^{\mu_i} f}{\mathrm{d}X^{\mu_i}}(a_i) \right)$ from the k-vector space $k[X]_m$ of polynomials of degree $< m$ into the k-vector space k^m is injective and hence bijective, since $\mathrm{Dim}_k k[X] = m = \mathrm{Dim}_k k^m$.)