MA 313 Algebraic Number Theory / January-April 2016

(Int PhD. and Ph. D. Programmes)

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

Lectures : Monday and Wednesday ; 15:30–17:00 **Venue:** MA LH-1 / LH-3 **(if LH-1 is not free)**

Midterms : Thursday, Feb 18, 2016, 10:00–11:30 **Seminars :** Fri April 15, Sat April 16, 2016, 15:00–17:00

Final Examination : Saturday, April 23, 2016, 14:00–17:00

Evaluation Weightage : Seminar : 20% **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

FINAL EXAMINATION

Saturday, April 23, 2016 **14:00 to 17:00** **Maximum Points :** 50 Points

• **Question F.6 is COMPULSARY. Attempt O N L Y F I V E Questions.**

F.1 Let A be a Dedekind domain and $\mathfrak{a} \neq 0$ an ideal in A.

(a) Show that all ideals in $A/\mathfrak{a}$ are principal ideals.
(**Hint :** Use the Chinese Remainder Theorem to assume that $\mathfrak{a} = \mathfrak{p}n$ with $\mathfrak{p} \in \operatorname{Spec} A$. Now, choose $a \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$, and prove $\mathfrak{p}^m = Aa^m + \mathfrak{p}^n$ for $1 \leq m \leq n$.) [5 Points]

(b) Show that the ideal $\mathfrak{a}$ is generated by two elements. Moreover, for any element $a \in \mathfrak{a}$, $a \neq 0$, there is an element $b \in \mathfrak{a}$ with $\mathfrak{a} = Aa + Ab$. (**Hint :** Apply part (a) to A/Aa.) [5 Points]

F.2 (a) (M i n k o w s k i ' s T h e o r e m o n L i n e a r F o r m s) Let $L \subseteq \mathbb{R}^n$ be a lattice and let $F_j := a_{1j}X_1 + \cdots + a_{nj}X_n \in \mathbb{R}[X]$, $j = 1, \ldots, n$ be linear forms with $\operatorname{Det}\left(a_{ij}\right) \neq 0$. Suppose that $c_1, \ldots, c_n \in \mathbb{R}^+$ be positive real numbers with $c_1 \cdots c_n \geq \left|\operatorname{Det}\left(a_{ij}\right)\right| \cdot \operatorname{Vol} L$. Show that there exists a non-zero $x = (x_1, \ldots, x_n) \in L$ such that

$$|F_1(x_1, \ldots, x_n)| \leq c_1 \quad \text{and} \quad |F_j(x_1, \ldots, x_n)| < c_j \quad \text{for all} \quad j = 2, \ldots, n. \qquad [6 \text{ Points}]$$

(**Hint :** Use Minkowski's Convex Body Theorem [1] to the convex, bounded and symmetric subset.

$$S := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \ |F_1(x_1, \ldots, x_n)| \leq c_1 + \varepsilon, \ 0 < \varepsilon < 1 \ \text{ and } \ |F_j(x_1, \ldots, x_n)| < c_j, \, j = 2, \ldots, n\}.$$

— If $v_1, \ldots, v_n \in L$ is a $\mathbb{Z}$-basis of L, then $\mathcal{P}(v_1, \ldots, v_n) := \{\sum_{i=1}^n r_i v_i \mid r_i \in \mathbb{R}, 0 \leq r_i \leq 1, \ i = 1, \ldots, n\}$ is a fundamental domain of L. The volume $\operatorname{Vol}(\mathcal{P}(v_1, \ldots, v_n)) = |\operatorname{Det}(v_1, \ldots, v_n)|$ is independent of the basis $v_1, \ldots, v_n$ which is called the v o l u m e of L and is denoted by $\operatorname{Vol} L$.)

(b) Let $r \in \mathbb{R}$ be a real number. For every natural number $m \in \mathbb{N}$, show that there exists a rational number $a/b \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, $b \neq 0$, with $\gcd(a, b) = 1$ such that

$$0 < b \leq m \qquad \text{and} \qquad \left| r - \frac{a}{b} \right| < \frac{1}{bm}.$$

(**Hint :** Apply the part (a) to the linear forms $F_1 = X_2$ vand $F_2 = -X_1 + rX_2$ with $c_1 = m, c_2 = 1/m$ and $L = \mathbb{Z}^2$. By setting $b := |x_2|$ and $a := \operatorname{sign}(x_2)x_1$, where $\operatorname{sign} x_2 = 1$ if $x_2 > 0$ and -1 if $x_2 < 0$.— This rational approximation of real numbers has implications in the theory of continued fractions and solutions of Pell's equation in elementary number theory.)

F.3 Let K be a number field and A be the ring of algebraic integers in K. For ideals $\mathfrak{a}$, $\mathfrak{b}$ in A, define $\gcd(\mathfrak{a}, \mathfrak{b}) := \mathfrak{a} + \mathfrak{b}$. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are r e l a t i v e l y p r i m e if $\gcd(\mathfrak{a}, \mathfrak{b}) = A$. (This is a generalization of the concept gcd of elements in $\mathbb{Z}$ to gcd of ideals in A).

---

[1] **Theorem** (M i n i k o w s k i ' s C o n v e x B o d y T h e o r e m) *Let L be a lattice in $\mathbb{R}^n$ with volume* $\operatorname{Vol} L := \operatorname{Vol}(\mathcal{P}(v_1, \ldots, v_n))$. *If $S \subseteq \mathbb{R}^n$ is a symmetric, convex subset with volume $\lambda^n(S) > 2^n \cdot \operatorname{Vol} L$, then there exists a non-zero element $x \in S \cap L$.*

Let $\mathfrak{a}$ be a non-zero ideal in A.

(a) Show that

$$\{\overline{a}\in A/\mathfrak{a} \mid Aa \text{ and } \mathfrak{a} \text{ are relatively prime }\}$$

is a subgroup of the multiplicative group of $A/\mathfrak{a}$ of order

$$\Phi(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})\prod_{\mathfrak{p}|\mathfrak{a}}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\right),$$

where the product runs over all distinct prime divisors of $\mathfrak{a}$ and $\mathrm{N}(-)$ denotes the norm.
(Note that for $a,b\in A$ with $\overline{a}=\overline{b}$ in $A/\mathfrak{a}$, $\gcd(Aa,\mathfrak{a})=\gcd(Ab,\mathfrak{a})$. Therefore having the same gcd with $\mathfrak{a}$ is an invariant of the residue class $\overline{a}\in A/\mathfrak{a}$.— **Hint :** Since the norm $\mathrm{N}(-)$ is multiplicative, one may assume that $\mathfrak{a}=\mathfrak{p}^m$ is a power of prime.)
Deduce that $\Phi(-)$ is multiplicative, i. e., if $\mathfrak{a}$ and $\mathfrak{b}$ are two relatively prime ideals in A, then

$$\Phi(\mathfrak{a}\mathfrak{b}) = \Phi(\mathfrak{a})\Phi(\mathfrak{b}).$$

(If $K=\mathbb{Q}$, then Φ is the ordinary Euler's totient function.) [5 Points]

(b) (Euler's Theorem for ideals) If $\mathfrak{a}\neq 0$ and $a\in A$ be relatively prime to $\mathfrak{a}$, then

$$a^{\Phi(\mathfrak{a})} \equiv 1 \,(\text{mod } \mathfrak{a}).$$

In particular, (Fermat's Little Theorem for ideals): if $\mathfrak{a}=\mathfrak{p}$ is a prime ideal in A, then $a^{\mathrm{N}(\mathfrak{p})-1}\equiv 1\,(\text{mod } \mathfrak{p})$. [3 Points]

(c) Let $\mathfrak{p}\neq 0$ be a prime ideal in A and $a\in A$. Show that there exists an integer $z\in\mathbb{Z}$ such that

$$a\equiv z\,(\text{mod } \mathfrak{p}) \qquad \text{if and only if} \qquad a^p\equiv a\,(\text{mod } \mathfrak{p}),$$

where $p\in\mathbb{P}$ is a prime number with $\mathbb{Z}p=\mathfrak{p}\cap\mathbb{Z}$. [3 Points]

F.4 **(a)** Let A_{-5} be the ring of algebraic integers in the quadratic number field $\mathbb{Q}[\sqrt{-5}]$. Show that $A_{-5}=\mathbb{Z}[\sqrt{-5}]$ and that it is not factorial. Further, show that the class group of $\mathbb{Q}[\sqrt{-5}]$ is cyclic of order 2. [5 Points]

(b) Show that the equation $X^2+5=Y^3$ has no solutions in $\mathbb{Z}^2$. (**Hint :** Use part (a).) [5 Points]

F.5 Let K be a number field and let A be the ring of integers in K. Let $p\in\mathbb{P}$ be a prime number, $\mathrm{V}(p):=\{\mathfrak{p}\in\operatorname{Spec}A \mid p\in\mathfrak{p}\}$ be the set of prime divisors in A and $Ap=\prod_{\mathfrak{p}\in\mathrm{V}(p)}\mathfrak{p}^{e_\mathfrak{p}}$ be the prime factorization of the ideal Ap in A. Show that

(a) For each $\mathfrak{p}\in\mathrm{V}(p)$, the norm $\mathrm{N}(\mathfrak{p})=p^{f_\mathfrak{p}}$ with $f_\mathfrak{p}\in\mathbb{N}^*$ and $\sum_{\mathfrak{p}\in\mathrm{V}(p)} e_\mathfrak{p}f_\mathfrak{p}=[K:\mathbb{Q}]$. [4 Points]

(b) The natural map $\operatorname{Gal}(K\,|\,Q)\times\operatorname{Spm}A\to\operatorname{Spm}A$, $\quad(\sigma,\mathfrak{p})\mapsto\sigma(\mathfrak{p})$, defines a natural operation of $\operatorname{Gal}(K\,|\,\mathbb{Q})$ on the maximal spectrum $\operatorname{Spm}A$ of A. Show that the orbits of this operation are precisely the subsets $\mathrm{V}(p)$, $p\in\mathbb{P}$ and that $e_\mathfrak{p}=e_\mathfrak{q}$ and $f_\mathfrak{p}=f_\mathfrak{q}$ for all $\mathfrak{p},\mathfrak{q}\in\mathrm{V}(p)$. What is the cardinality $|G_\mathfrak{p}|$ of the isotropy at $\mathfrak{p}\in\operatorname{Spm}A$? [6 Points]

*__F.6__ Let K be a number field with $[K:\mathbb{Q}]=n=r_1+2r_2$, where r_1 and r_2 is the number of real and non-real complex $\mathbb{Q}$-embeddings of K in $\mathbb{C}$, respectively and $M_K=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\operatorname{Disc}K|}$ be the Minkowski's bound for the norm of ideals in A.

(a) Show that the class group of K is generated by $\cup_{p\in\mathbb{P},\,p\leq M_K}\mathrm{V}(p)$. (See Question F.5 for notation. Use F.5, (a).) [5 Points]

(b) Compute the class group of the quadratic number field $K=\mathbb{Q}(\sqrt{-14})$. (**Hint :** Use part (a) and factorize the minimal polynomial $\mu_{\sqrt{-14},\mathbb{Q}}=X^2+14$ modulo primes 2 and 3.) [6 Points]

GOOD LUCK