ALGEBRAIC NUMBER THEORY - MIDSEMESTRAL TEST

17TH FEB, 2017, 10:00AM – 1:00PM

Instructions:

(i) *This exam is an open sheet exam – you can keep one A4 sized sheet with you as a cheat sheet (with anything written on it) for your reference.*
(ii) *The questions in section 1 are to be answered in True/False, no explanation need be given. All questions are compulsory. Each question carries 1 point.*
(iii) *In section 2 and section 3, answer any two questions out of the three. Each question carries 5 points.*

1.

Q 1. Answer in True/False, no explanation needed. Each question carries 1 point.

(1) Let $S \subset R$ be a multiplicative set (that is $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$). Then the ideals of $S^{-1}R$ are in bijective correspondece with ideals of R which do not have an intersection with S.
(2) Let L be a subfield of $\mathbb{C}$ which is algebraic, finite dimensional over $\mathbb{Q}$. Then for any $x \in L$, the norm $N_{L/\mathbb{Q}}(x) = |x|$ where $|\cdot|$ denotes the usual norm in $\mathbb{C}$.
(3) Let $L/\mathbb{Q}$ be a number field of degree n. Then there are n distinct embeddings $\sigma : L \hookrightarrow \mathbb{C}$.
(4) Discriminant of a number field $L/\mathbb{Q}$ is always positive.
(5) Let $(K, |\cdot|)$ be a valued field and V/K be a finite dimensional vector space with basis $a_1, a_2, .., a_r$. Let $\|\cdot\|$ be a K-norm on V (that is a norm on V such that $\|\lambda v\| = |\lambda|\|v\| \forall \lambda \in K, \forall v \in V$). Let $v_n = \lambda_n^{(1)} a_1 + ... + \lambda_n^{(r)} a_r$ be such that $\|v_n\| \to 0$ as $n \to \infty$. Then $|\lambda_n^{(i)}| \to 0$ as $n \to \infty$, for all i.

2.

Answer any two questions from Q 2 – Q 4. Each question carries 5 points.

Q 2. Show that:

(1) Let R be a Dedekind domain and $I \subset R$ be a nonzero ideal. If $0 \neq a \in I$, then there is some $b \in I$ such that $I = (a, b)$.
(2) Let K be a number field, R it's ring of integers and $p \in \mathbb{Z}$ be a prime. Assume that $pR = \mathfrak{q}_1^{e_1} ... \mathfrak{q}_r^{e_r}$ where $\mathfrak{q}_1, ..., \mathfrak{q}_r$ are prime ideals of R. Then for a prime ideal $\mathfrak{q} \subset R$,

$$\mathfrak{q} \cap \mathbb{Z} = (p) \Leftrightarrow \mathfrak{q} \in \{\mathfrak{q}_1, ..., \mathfrak{q}_r\}.$$

Q 3. Show that discriminant of a number field L is 0 or 1 (mod 4).

Q 4. Find all integer solutions X, Y satisfying $X^2 - 7Y^2 = 1$.

3.

Answer any two questions from Q 5 – Q 7. Each question carries 5 points.

Q 5. Compute the class group of $K = \mathbb{Q}[\sqrt{-14}]$ as follows:

(1) Use Minkowski bound to show that primes $\mathfrak{p}$ that lie over (2) and (3) generate the class group.

(2) Show that the ring of integers in K is $\mathbb{Z}[\sqrt{-14}]$ and show that

$$(2) = \mathfrak{p}_2^2 \text{ and } (3) = \mathfrak{p}_3\mathfrak{p}_3'$$

with $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$ not principal.

(3) Compute the class group of K by computing the factorization of the principal ideal $(2+\sqrt{-14})$.
Hint: $N_{K/\mathbb{Q}}(2+\sqrt{-14}) = 2 \cdot 3^2$ and show that $(3) = \mathfrak{p}_3\mathfrak{p}_3' \nmid (2+\sqrt{-14})$.

Remark (Minkowski Bound)**.** *For any fractional ideal $I \subset K$, there is an integral ideal $J \in [I]$ (where $[I]$ denotes the class of I in the class group) such that:*

$$N_{K/\mathbb{Q}}(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta(K/\mathbb{Q})|}$$

where n is the degree of $K/\mathbb{Q}$, there are $2s$ complex embeddings of K in $\mathbb{C}$, and $\Delta(K/\mathbb{Q})$ is the discriminant of K.

Q 6. Let L/K be a finite extension of degree n where K is complete with respect to a non-Archimedean discrete valuation $|\cdot|$. Then:

(1) Show that there exists a unique extension of $|\cdot|$ to a valuation on L.

(2) This extension is given by

$$|y| := |N_{L/K}(y)|^{1/n} \text{ for any } y \in L.$$

Q 7. Show that there is a unique function $\log : \mathbb{Q}_p^\times \to \mathbb{Q}_p$ characterized by the following properties:

(1) $\log(xy) = \log(x) + \log(y)$ for all $x, y \in \mathbb{Q}_p^\times$.

(2) $\log(p) = 0$.

(3) $\log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \ldots$ whenever the right hand side converges.

Remark. *You can assume the following (well known) relation in the ring of formal power series $\mathbb{Q}[[X,Y]]$*

$$\log(1-X) + \log(1-Y) = \log(1-(X+Y-XY))$$

where the logarithm is defined by:

$$\log(1-P(X,Y)) := -P(X,Y) - \frac{P(X,Y)^2}{2} - \frac{P(X,Y)^3}{3} - \ldots$$

for any $P(X,Y)$ lying in the ideal generated by $\{X,Y\}$.

Remark. *$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for the p-adic exponential valuation ($v_p(\cdot)$ with $v_p(p) = 1$).*