MATHEMATICAL TRIPOS PART III (2017–18)

Algebraic Number Theory - Example Sheet 1 of 4 **C. Johansson**

1. In lectures, we defined valuations on fields. More generally, if A is a ring, a *valuation* on A is function $v : A \to \mathbb{R} \cup \{\infty\}$ satisfying the axioms for a valuation as given in lectures. Show that A is an integral domain, and that v extends uniquely to a valuation on the fraction field of A.

2. Let K be a field. An *absolute value* on K is a function $|-| : K \to \mathbb{R}$ satisfying the following properties:

   (i) $|x| = 0$ if and only if $x = 0$;

   (ii) $|xy| = |x||y|$ for all $x, y \in K$;

   (iii) *(Triangle inequality)* $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

   If v is a valuation on K and $c > 1$ is a real number, show that $|x| := c^{-v(x)}$ defines an absolute value on K (here we use the convention $c^{-\infty} = 0$). In fact, show that it satisfies the *strong triangle inequality*

   $$|x + y| \leq \max\{|x|, |y|\}$$

   for $x, y \in K$. Absolute values satisfying the strong triangle inequality are called *non-archimedean*. If $|-|$ is a non-archimedean absolute value on K, show that $w(x) := -\log_c |x|$ defines a valuation on K for any $c > 1$, with the convention $-\log_c(0) = \infty$.

3. Let $A \subseteq B$ be rings. Show that if $b_1, ..., b_n \in B$ are integral over A and $x \in B$ satisfies $x^n + b_1 x^{n-1} + ... + b_n = 0$, then x is integral over A. Show also that the integral closure $\widetilde{A}$ of A in B is a ring, and is integrally closed in B.

4. (The Chinese remainder theorem) Let A be a ring and let $I_1, \ldots, I_n$ be pairwise coprime ideals of A. We recall that two ideals I, J of A are said to be coprime if $I + J = A$.

   (i) Show that $\prod_{i=1}^n I_i = \bigcap_{i=1}^n I_i$.

   (ii) Show that the natural map $A \to \prod_{i=1}^n A/I_i$ is surjective. Deduce that there is an isomorphism $A/\prod_{i=1}^n I_i \cong \prod_{i=1}^n A/I_i$.

   (iii) Show that if $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are distinct maximal ideals of A and $e_1, dots, e_r \geq 1$ are integers, then the ideals $\mathfrak{m}_1^{e_1}, \ldots, \mathfrak{m}_r^{e_r}$ are pairwise coprime.

5. Let A be a Dedekind domain with field of fractions K, and let $\mathfrak{a} \neq 0$ be an ideal of A.

   (i) Define $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq A\}$ and show that it is a fractional ideal of A.

(ii) Show that the set of ideals $\mathfrak{b}$ of A containing $\mathfrak{a}$ satisfies the descending chain condition (*Hint: consider their inverses* $\mathfrak{b}^{-1}$ *inside* $\mathfrak{a}^{-1}$).

(iii) Deduce that there are only finitely many maximal ideals $\mathfrak{p}$ containing $\mathfrak{a}$.

6. Let A be a Dedekind domain. If $\mathfrak{p}$ be a maximal ideal of A and $\mathfrak{a} \neq 0$ is any ideal, recall that we defined $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}_{\geq 0}$ by the equality $\mathfrak{a}_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{v_{\mathfrak{p}}(\mathfrak{a})}$.

   (i) Show that $v_{\mathfrak{p}}(\mathfrak{a}) > 0$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$, and deduce from Question 5 that $v_{\mathfrak{p}} = 0$ for all but finitely many $\mathfrak{p}$.

   (ii) Show that $\mathfrak{a} = \bigcap_{\mathfrak{p}} \mathfrak{a}_{\mathfrak{p}}$, where the intersection takes place in Frac(A).

   (iii) If $(e_{\mathfrak{p}})_{\mathfrak{p}}$ is a collection of integers ≥ 0 such that $e_{\mathfrak{p}} = 0$ for all but finitely many $\mathfrak{p}$, show that, for any maximal ideal $\mathfrak{q}$ of A,

$$v_{\mathfrak{q}}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}\right) = e_{\mathfrak{q}}.$$

   Deduce unique factorization of ideals into maximal ideals (Proposition 25 from lectures).

7. By definition, a Dedekind domain is an integral domain which is (1) Noetherian, (2) integrally closed, and (3) every non-zero prime ideal is maximal, and there exist non-zero prime ideals. Find examples of integral domainds which satisfy (1) and (2), or (2) and (3), or (1) and (3), but which are not Dedekind domains.

8. If $c \in \mathbb{Z}_p$ satisfies $v_p(c) > 0$ show that $(1+c)^{-1} = 1 - c + c^2 - c^3 + \ldots$ Hence or otherwise find $a \in \mathbb{Z}$ such that $v_5(4a-1) \geq 10$.

9. Let $x = \sum_{n \geq N} a_n p^n \in \mathbb{Q}_p$, with $a_n \in \{0, 1, \ldots, p-1\}$, $N \in \mathbb{Z}$ and $a_N \neq 0$. Show that $x \in \mathbb{Q}$ if and only if the sequence $(a_n)_n$ is eventually periodic.

10. Show that the equation $x^3 - 3x + 4 = 0$ has a unique solution in $\mathbb{Z}_7$, but has no solutions in $\mathbb{Z}_5$ or in $\mathbb{Z}_3$. How many are there in $\mathbb{Z}_2$?

11. Consider the series

$$\text{“}\sqrt{1+15}\text{”} = 1 + \sum_{n=1}^{\infty} \binom{1/2}{n} 15^n$$

   where $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$. Show that the series converges to 4 in $\mathbb{Z}_3$, to -4 in $\mathbb{Z}_5$, and diverges with in $\mathbb{Z}_p$ for any $p \neq 2, 3, 5$.

12. Let $p > 2$ be a prime.

   (i) Show that $x \in \mathbb{Z}_p^{\times}$ is a square in $\mathbb{Z}_p$ if and only if its reduction modulo p is a square in $\mathbb{F}_p$. Deduce a description of the set of squares in $\mathbb{Q}_p^{\times}$.

   (ii) Show that there are exactly three non-isomorphic quadratic extensions of $\mathbb{Q}_p$.

   What happens if $p = 2$?

13. Show that any normalised valuation on $\mathbb{Q}$ is equal to v_p for some prime p. Can you find all normalised valuations on $\mathbb{F}_p(T) := \text{Frac}\,(\mathbb{F}_p[T])$?