HOMEWORK ASSIGNMENT 3

MATH-GA 2210.001 ELEMENTARY NUMBER THEORY

Each problem will be marked out of 5 points.

Exercise 1 ([1, II.3.1]). Show that

$$|z| = (z\overline{z})^{1/2}$$

is the only valuation of $\mathbb{C}$ which extends the absolute value $|\ |$ of $\mathbb{R}$.

`Solution.` Let $|\ |$ be a valuation on $\mathbb{C}$ that extends the absolute value $|\ |$ of $\mathbb{R}$. Then $|-1| = 1$ by assumption. Moreover, we have $|i| = 1$ as well, because

$$1 = |-1| = |i \times i| = |i| \times |i|$$

and $|i| > 0$. Thus, we have

$$\left|e^{2\pi i\theta}\right| = |\cos(\theta) + i\sin(\theta| \leqslant |\cos(\theta)| + |i\sin(\theta| = |\cos(\theta)| + |i||\sin(\theta| \leqslant 2$$

for every $\theta \in \mathbb{R}$. If $|e^{2\pi i\theta}| > 1$, then

$$\left|e^{2\pi i\theta n}\right| = \left|e^{2\pi i\theta}\right|^n > 2$$

for some $n \in \mathbb{N}$. Thus, $|e^{2\pi i\theta}| \leqslant 1$ for every $\theta \in \mathbb{R}$. Similarly, if $|e^{2\pi i\theta}| < 1$, then

$$\left|e^{-2\pi i\theta n}\right| = \frac{1}{\left|e^{2\pi i\theta}\right|^n} > 2$$

for some $n \in \mathbb{N}$. This shows that $|e^{2\pi i\theta}| = 1$ for every $\theta \in \mathbb{R}$. Since, every non-zero complex number z can be written as

$$z = re^{2\pi i\theta}$$

for some $r \in \mathbb{R}_{>0}$ and $\theta \in \mathbb{R}$, we see that

$$|z| = \left|re^{2\pi i\theta}\right| = \left|r\right|\left|e^{2\pi i\theta}\right| = r = (z\overline{z})^{1/2}$$

for every $z \in \mathbb{C}$.

Exercise 2 ([1, II.3.2]). What is the relation between the Chinese remainder theorem and the approximation theorem [1, Theorem II.3.4]?

`Solution.` The Chinese Remainder Theorem says that if $n_1, \ldots, n_k$ are pairwise coprime integers, and $a_1, \ldots, a_k$ are some integers, then there is an integer x such that

$$x \equiv a_i \bmod n_i.$$

for every $i \in \{1, \ldots, k\}$. Taking prime decomposition of each n_i and applying [1, Theorem II.3.4], we can find a *rational* number

$$q = \frac{s}{t}$$

such that

$$s \equiv ta_i \bmod n_i.$$

If such q was always an integer, i.e. $t = 1$, this would give us the Chinese Remainder Theorem. However, [1, Theorem II.3.4] does not claim that q is an integer. So, the Chinese Remainder Theorem is somewhat stronger statement.

This assignment is due on Wednesday 18 February 2015.

Exercise 3 ([1, II.3.3])**.** Let k be a field and $K = k(t)$ be the function field in one variable. Show that the valuations $v_{\mathfrak{p}}$ associated to the prime ideals

$$\mathfrak{p} = \big(p(t)\big)$$

of $k[t]$, together with the degree valuation v_∞, are the only non-trivial valuations of K that are trivial on k, up to equivalence. What are the residue class fields?

`Solution.` Let v be a valuation of K. Since V is trivial on k, it must be a nonarchimedian valuation (see [1, Definition II.3.5]). Thus, it follows from [1, Proposition II.3.4] that

$$v(a+b) \geqslant \min\{v(a), v(b)\}$$

for every a and b in K (strict triangle inequality). Recall that the valuation ring of v is

$$\mathcal{O} = \{x \in K \mid v(x) \geqslant 0\}.$$

The ring $\mathcal{O}$ has a unique maximal ideal

$$\mathfrak{I} = \{x \in K \mid v(x) > 0\}$$

by [1, Proposition II.3.8].

Suppose that $v(t) \geqslant 0$. Let us show that v is equivalent to $v_{\mathfrak{p}}$ for some non-trivial ideal $\mathfrak{p}$ in $k[t]$ that is generated by a non-zero irreducible polynomial $p(t) \in k[t]$. To see that this is true, note that for any polynomial $f(t) \in k[t]$, if

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n,$$

we have

$$v\big(f(t)\big) \geqslant \min\{v(a_l) + l \cdot v(t) | l = 0, 1, \ldots, n\}.$$

Since $v(a_i) = 0$ and $v(t) \geqslant 0$, this means that $v(f(t)) \geq 0$. So $k[t]$ is a subset of the valuation ring $\mathcal{O}$. Put $\mathfrak{p} = \mathfrak{I} \cap k[t]$. Then $\mathfrak{p}$ is an ideal in $k[t]$ (and it is nontrivial because $1 \notin \mathfrak{I}$). So, since $k[t]$ is a principal ideal domain (it's a polynomial ring over a field), the ideal $\mathfrak{p}$ is generated by a single element $p(t) \in k[t]$. Moreover, because $\mathfrak{I}$ is prime, so is $\mathfrak{p}$. Thus, $p(t)$ is irreducible. We claim that

$$v(h(t)) = v_{\mathfrak{p}}(h(t)) \times v\big(p(t)\big)$$

for every $h(t) \in K$. Indeed, let $h(t) \in K$, and write it as

$$h(t) = p(t)^m \frac{q(t)}{r(t)}$$

where $q(t)$ and $r(t)$ are polynomials in $k[t]$ such that $p(t)$ does not divide either $q(t)$ or $r(t)$. Then neither $q(t)$ nor $r(t)$ is in $\mathfrak{p}$, so they are no in $\mathfrak{I}$. Then

$$v\big(q(t)\big) = v\big(r(t)\big) = 0.$$

On the other hand, we have

$$m = v_{\mathfrak{p}}(h(t)$$

by definition. Thus, we have

$$v\big(h(t)\big) = m \times v\big(p(t)\big) = v_{\mathfrak{p}}(h(t)) \times v\big(p(t)\big).$$

So, v is equivalent to $v_{\mathfrak{p}}$.

Suppose now that $v(t) < 0$. Let us show that v is equivalent to the degree valuation. Put $x = \frac{1}{t}$. Then

$$v\big(x\big) > 0,$$

which implies that $x \in \mathfrak{I}$. Arguing as in the case $v(t) \geqslant 0$, we see that $k[x]$ is a subset of the valuation ring $\mathcal{O}$, and $\mathfrak{p} \cap k[x]$ is a non-trivial prime ideal. Since, x is an irreducible polynomial and $x \in \mathfrak{p}$, we see that $\mathfrak{p} \cap k[x]$ is generated by x. Arguing as in the case $v(t) \geqslant 0$, we see that

$$v\big(f(t)\big) = v(t) \times v_\infty\big(f(t)\big)$$

for every $f(t) \in k(t)$, so that v is equivalent to v_∞. Indeed, it is enough to check the latter equality for polynomials in $k[t]$. Let

$$f(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + a_n t^n$$

be a polynomial of degree n in $k[t]$, where $a_n \neq 0$. Then we can factor out a power of t^n so that

$$f(t) = t^n \Big(a_n + a_{n-1} t^{-1} + \cdots + a_1 t^{1-n} + a_0 t^{-n} \Big).$$

Then the strict triangle inequality gives

$$v\Big(a_n + a_{n-1} t^{-1} + \cdots + a_1 t^{1-n} + a_0 t^{-n} \Big) = v(a_n) = 0.$$

Thus, we have

$$v\big(f(t)\big) = n \times v(t) = v(t) \times v_\infty\big(f(t)\big).$$

The residue class fields for the $p(t)$-adic valuations are

$$k[t]/(p(t)),$$

and that the residue class field for v_∞ is just k. Indeed, in the former case, the ring $\mathcal{O}$ is just a localization of the ring $k[t]$ in the ideal generated by $p(x)$, which implies that

$$\mathcal{O}/\mathfrak{I} \cong k[t]/(p(t)).$$

In the latter case, $\mathcal{O}$ is the localization of the ring $k[x]$ in the ideal generated by x, where $x = \frac{1}{t}$ as above. Thus, the residue class field for v_∞ is

$$\mathcal{O}/\mathfrak{I} \cong k[x]/(x) \cong k.$$

References

[1] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.