Zahlenentheorie

Exercise Sheet 2

Exercise 2.1

Let K be a field, let $|.| : K \to \mathbb{R}_{\geq 0}$ be an absolute value on K. A *K-vector space norm* on a finite dimensional K-vector space V is a map $||.|| : V \to \mathbb{R}_{\geq 0}$ satisfying the following conditions:

(i) $||v|| = 0$ if and only if $v = 0$

(ii) $||v + w|| \leq ||v|| + ||w||$ for all $v, w \in V$

(iii) $||av|| = |a| \cdot ||v||$ for all $a \in K$ and $v \in V$

Two K-vector space norms on V are said to be *equivalent* if and only if they define the same topology on V. Show the following:

(a) If $e = \{e_i\}_i$ is a K-basis of the finite dimensional K-vector space V, then

$$|| \sum_i a_i e_i ||_e := \max_i |a_i| \qquad \text{for } a_i \in K$$

defines a K-vector space norm on V.

(b) Two K-vector space norms $||.||_1$, $||.||_2$ on a finite dimensional K-vector space V are equivalent if and only if there are constants $C_1, C_2 \in \mathbb{R}_{>0}$ with $C_1||v||_1 \leq ||v||_2 \leq C_2||v||_1$ for all $v \in V$.

(c) If K complete then all K-vector space norms on a finite dimensional K-vector space V are equivalent. For any such norm, V is complete (i.e. each Cauchy sequence converges).

Exercise 2.2

Let $|.|_1$ and $|.|_2$ be non trivial absolute values on a field K. Show the equivalence of the following statements:

(a) $|.|_1$ and $|.|_2$ are *equivalent*, i.e. they define the same topology on K.

(b) There is some $s \in \mathbb{R}_{>0}$ with $|x|_1 = |x|_2^s$ for all $x \in K$.

(c) For all $x \in K$ with $|x|_1 < 1$ we have $|x|_2 < 1$.

Ansatz: In order to see (c)$\Rightarrow$(b) try to show first that $|x|_1 < 1$ for all $x \in K$ with $|x|_2 < 1$. Then fix some $a \in K$ with $0 < |a|_1 < 1$. For each $x \in K^\times$ we then find $\alpha_1, \alpha_2 \in \mathbb{R}$ with $|x|_1 = |a|_1^{\alpha_1}$ and $|x|_2 = |a|_2^{\alpha_2}$. Show that $\alpha_1 = \alpha_2$.

Exercise 2.3

(a) Every sequence in $\mathbb{Z}_p$ has a convergent subsequence. In particular, $\mathbb{Z}_p$ is compact.

(b) Given $f(X) \in \mathbb{Z}[X_1, \ldots, X_s]$ (for some $s \in \mathbb{N}$), one may ask for the solutions $(x_1, \ldots, x_s) \in \mathbb{Z}^s$ of the *diophantine equation* $f(X) = 0$. As an (easier) approximation, one may ask for the $x = (x_1, \ldots, x_s) \in \mathbb{Z}^s$ satisfying $f(x) \equiv 0 \mod m\mathbb{Z}$, for a given $m \in \mathbb{N}$. The Chinese Remainder Theorem tells us that it will be enough to answer this latter question for all m's which are powers of prime numbers, i.e. to find the $x = (x_1, \ldots, x_s) \in \mathbb{Z}^s$ satisfying $f(x) \equiv 0 \mod p^n\mathbb{Z}$, for all prime numbers p and all $n \in \mathbb{N}$. Fixing p, working with the p-adic numbers $\mathbb{Z}_p$ provides a conceptual approach towards the solution set of $f(x) \equiv 0$ modulo $p^n\mathbb{Z}$ *for all n simultaneously.* This is the upshot of the following problem.

Let p be a prime number. A polynomial $f(X) \in \mathbb{Z}[X_1, \ldots, X_s]$ has a zero $(x_1, \ldots, x_s)$ in $\mathbb{Z}_p^s$ if and only if it has a zero in $(\mathbb{Z}/p^n\mathbb{Z})^s$ for each $n \in \mathbb{N}$.

Exercise 1.4

Let p be a prime number, let $n \in \mathbb{N}$. Prove the following formula for $v_p(n!)$: If we write $n = a_0 + a_1p + \ldots + a_kp^k$ with $a_i \in \{0, \ldots, p-1\}$ and put $s_n = a_0 + a_1 + \ldots + a_k$, then

$$v_p(n!) = \frac{n - s_n}{p - 1}.$$