May 23th, 2013

Zahlentheorie II

Exercise sheet 7[1]

Exercise 1 (5 Points)**.** Let R be a local ring with residue field k. In the lecture you proved that in some cases R contains a field K, such that the canonical map $R \twoheadrightarrow k$ maps K isomorphically to k. Such a field K is called *coefficient field* of R. A subfield K of R is called *maximal*, if for any subfield L of R with $L \supset K$ it follows that $L = K$.

(a) Show that any coefficient field of R is a maximal subfield.
(b) Show that every local ring which contains a field also contains a maximal subfield. (Hint: Zorn's Lemma)
(c) Show that if R is a complete local ring containing a field of characteristic 0, then every maximal subfield is a coefficient field. (**Hint:** Use Hensel's Lemma as presented in the lecture or in Serre's Local Fields, Chap. II, Prop. 7)
(d) Let k be a field of characteristic $p > 0$, and $R := k(t)[\![x]\!]$. Show that $k(t^p + x)$ is a maximal subfield of R but not a coefficient field of R.

Exercise 2 (3 Points)**.** Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial.

(a) Show that the local ring $R := \mathbb{Q}[x]_{(f)}$ does not contain a coefficient field, if $\deg f > 1$.
(b) Show that the completion $\hat{R} := \varprojlim_n R/(fR)^n$ contains a *unique* coefficient field (**Hint:** Use Hensel's Lemma as presented in the lecture or in Serre's Local Fields, Chap. II, Prop. 7).

Exercise 3 (6 Points)**.** Let R be a commutative ring. For $n \in \mathbb{N}$, an element $\xi \in R$ is called *n-th root of unity*, if $\xi^n = 1$. The set of n-th roots of unity in R is denoted by $\mu_n(R)$, and it is a subgroup of $R^\times$.

Let $p \in \mathbb{Z}$ be a prime number, and $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ the p-adic integers. From the lecture you know that if $\mathbb{Q}_p$ denotes the completion of $\mathbb{Q}$ with respect to the p-adic absolute value, then $\mathbb{Z}_p$ can be identified with the valuation ring of $\mathbb{Q}_p$.

(a) Show that for every $n \in \mathbb{N}$ the group $\mu_n(\mathbb{Z}_p)$ is cyclic.
(b) For $n \in \mathbb{N}$ compute the order of $\mu_n(\mathbb{Z}_p)$ whenever n is prime to p (**Hint:** Think about roots of unity in $\mathbb{F}_p$ and then use Hensel's Lemma).
(c) If we write $\mu'(\mathbb{Z}_p)$ for the group of elements $\xi \in \mathbb{Z}_p$ such that $\xi^n = 1$ for some n prime to p, then show that $\mu'(\mathbb{Z}_p)$ is finite and compute its order.

Exercise 4 (8 Points)**.** Again let $p \in \mathbb{Z}$ be a prime number. Write $U := 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$. Clearly U is a subgroup of $\mathbb{Z}_p^\times$. **In the rest of this exercise, assume that $p > 2$.**

(a) Consider the ideal $p\mathbb{Z}_p$ as a subgroup of the additive group of $\mathbb{Z}_p$. For an element $a \in p\mathbb{Z}_p$, show that the exponential series

$$\exp(a) := \sum_{n=0}^{\infty} \frac{a^n}{n!}$$

converges in $\mathbb{Z}_p$, and that exp induces a homomorphism of groups $p\mathbb{Z}_p \to U$.

[1] For questions or remarks, feel free to come to A3.112A or to write to `kindler@math.fu-berlin.de`. At the latest, hand in your solutions on **June 5**.

(b) For an element $1 + b \in U$, show that the series

$$\log(1+b) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{b^n}{n} = b - \frac{b^2}{2} + \frac{b^3}{3} - \dots$$

converges in $\mathbb{Z}_p$, and that log induces a homomorphism of groups $U \to p\mathbb{Z}_p$.

(c) Show that exp and log are mutually inverse, and hence $U \cong p\mathbb{Z}_p \cong \mathbb{Z}_p$ as abelian groups. Actually this is a homeomorphism of *topological* groups, but you do not need to prove this.

(d) Show that there is a split short exact sequence of abelian groups

$$0 \to \mathbb{Z}_p \xrightarrow{\exp(p\cdot)} \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to 0,$$

and hence that $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times$. (**Hint:** Use Exercise 3 to show that the sequence is split)

(e) Finally compute the order of $\mu_n(\mathbb{Z}_p)$ for $(n,p) > 1$, conclude that $\mathbb{Z}_p$ only contains finitely many roots of unity. How many are there?

Hints.

- Recall that since the p-adic absolute value is non-archimedian, a series $\sum_{n\geq 0} a_n$ with $a_n \in \mathbb{Z}_p$ converges if and only if the sequence $(a_n)_{n\geq 0}$ converges to 0. Hence, to show that, e.g., $\exp(a)$ converges, it would suffice to show that $v_p(\frac{a^n}{n!})$ gets larger and larger.
- To check relations like

$$\log((1+a)(1+b)) = \log(1+a) + \log(1+b), \tag{1}$$

you may use the following facts: If a formal power series $F(X,Y) \in \mathbb{Q}[\![X,Y]\!]$ vanishes on a nonempty open subset of $\mathbb{R}^2$, then $F(X,Y) = 0$ as an element of $\mathbb{Q}[\![X,Y]\!]$. Next, if the formal power series $F(X,Y)$ converges on an open subset of $\mathbb{Q}_p$, then one may rearrange its summands without changing the limit.

This allows you to use your knowledge about the real logarithm and exponential function to prove, e.g., (1).

To check that exp and log are mutually inverse, you can use the same reasoning for formal power series in one variable.