NUMBER THEORY III – WINTERSEMESTER 2016/17

PROBLEM SET 6

HÉLÈNE ESNAULT, LARS KINDLER

Exercise 1. Let $(K, |\cdot|)$ be a complete discretely valued field with residue field k.

(a) Show that $\mathrm{char}(K) = \mathrm{char}(k)$ or $\mathrm{char}(K) = 0$.

Now assume that k is a field and define $K := k(\!(X)\!)$. Recall that $k(\!(X)\!)$ is the field of *Laurent series with coefficients in* k. It can be described as

$$k(\!(X)\!) = \left\{ \sum_{i=-\infty}^{\infty} a_n X^n \,\middle|\, a_n \in k, a_n = 0 \text{ for } n \ll 0 \right\},$$

and it is the completion of the field of rational functions $k(X)$ with respect to the absolute value defined for $f(X), g(X) \in k[X]$, $g(X) \neq 0$, as

$$\left| \frac{f(X)}{g(X)} \right| = \exp(-(\mathrm{ord}(f(X)) - \mathrm{ord}(g(X)))),$$

where $\mathrm{ord}(f(X)) := \max\{n \in \mathbb{N} | f(X) \in X^n k[X]\}$.

The field K is a complete, discretely valued field with residue field k and its valuation ring is the ring of formal power series

$$k[\![X]\!] = \varprojlim_{n\in\mathbb{N}} k[X]/(X^n) := \left\{ \sum_{n=0}^{\infty} a_n T^n \,\middle|\, a_n \in k \right\}$$

(b) Show that for $n \in \mathbb{N}$ the polynomial $f(T) := T^n - X \in K[T]$ is irreducible and that the extension $K \subseteq K[T]/(f(T))$ is totally and tamely ramified or inseparable.

(c) Let $\mathrm{char}(K) = p > 0$. Show that for $n \in \mathbb{N}$ the polynomial $g(T) := T^p - T - 1/X \in K[T]$ is irreducible and that the extension $K[T]/(g(T))$ is totally and wildly ramified with Galois group $G = \mathbb{Z}/p\mathbb{Z}$. Compute the ramification filtration of G. (*Hint: It can be helpful to compute the minimal polynomial of* $T^{-1} \in K[T]/(g(t))$)

Exercise 2. Let k be a field and let G be a finite group. We write $|G|$ for the order of G. Define the *group algebra* $k[G]$ *of* G as follows. As a k-vector space, $k[G]$ has dimension $|G|$ and it is spanned by the basis $\{g|g \in G\}$. Multiplication on $k[G]$ is defined via the group structure of G: For $g, h \in G$, we define $g \cdot h := gh$ in $k[G]$. More explicitly, typical elements of $k[G]$ are of the shape

$$\sum_{g\in G} \lambda_g g, \sum_{g\in G} \mu_g g, \quad \lambda_g, \mu_g \in k,$$

If you want your solutions to be corrected, please hand them in just before the lecture on November 29, 2016. If you have any questions concerning these exercises you can contact Lars Kindler via `kindler@math.fu-berlin.de` or come to Arnimallee 3, Office 109.

and their product is

$$\left(\sum_{g\in G}\lambda_g g\right)\left(\sum_{g\in G}\mu_g g\right)=\sum_{g\in G}\left(\sum_{\substack{r,s\in G\\ rs=g}}\lambda_r\mu_s\right)g.$$

(a) Convince yourself that the map $k\to k[G]$, $\lambda\mapsto\lambda\cdot e$, ($e$ the neutral element of G) makes $k[G]$ into a k-algebra.

(b) For a left-$k[G]$-module V, let $V^G:=\{v\in V|\text{for all } g\in G, gv=v\}$; this is called the submodule of *G-invariants of V*. Show that V^G is a left-sub-$k[G]$-module of V, and compute that

$$k[G]^G=\left\{\sum_{g\in G}\lambda g\,\middle|\,\lambda\in k\right\},$$

where we consider $k[G]$ as a left-$k[G]$-module.

(c) If $\mathrm{char}(k)=p>0$ and if G is a p-group, show that $V^G\neq 0$ for every finitely generated nonzero left-$k[G]$-module V. (*Hint: First show that without loss of generality, you can assume that $k=\mathbb{F}_p$ by finding a G-stable finite dimensional sub-$\mathbb{F}_p$-vector space of V. Then use your knowledge about p-groups acting on finite sets to finish.*)

(d) Conclude that the only simple left-$k[G]$-module is k equipped with the G-action given by $g\cdot\lambda=\lambda$ for all $g\in G$, $\lambda\in k$.

(e) If $\mathrm{char}(k)=p>0$ and if G is a p-group, show that $k[G]$ is indecomposable, that is, show that whenever $V,W\subseteq k[G]$ are sub-left-$k[G]$-modules such that $k[G]=V\oplus W$, then $V=k[G]$ or $W=k[G]$.

Exercise 3. (a) Consider k as a left-$k[G]$-module by defining $g\cdot\lambda=\lambda$ for all $g\in G,\lambda\in k$. Let I_G be the left-ideal of $k[G]$ generated by $\{(g-1)|g\in G\}$. Show that there is a short exact sequence of left-$k[G]$-modules

$$0\to I_G\to k[G]\xrightarrow{\varphi}k\to 0,\qquad(\star)$$

where φ is defined by $\varphi(\sum_{g\in G}\lambda_g g):=\sum_{g\in G}\lambda_g$

(b) Recall that a splitting of $(\star)$ is a morphism of left-$k[G]$-modules $\psi:k\to k[G]$, such that $\varphi\circ\psi=\mathrm{id}_k$. Show that any splitting has image contained in $k[G]^G$.

(c) Show that there exists a splitting of the short exact sequence $(\star)$, if and only if the order $|G|$ of G is invertible in k.

(d) *(Maschke's theorem)* If $|G|$ is invertible in k, show that every finitely generated left-$k[G]$-module is semi-simple. (*Hint: If $\varphi:V\twoheadrightarrow W$ is a surjection of left-$k[G]$-modules, let $\psi_0:W\to V$ be a homomorphism of k-vector spaces such that $\varphi\circ\psi_0=\mathrm{id}_W$. Modify ψ_0 to make it $k[G]$-linear.*)