NUMBER THEORY III – WINTERSEMESTER 2016/17

PROBLEM SET 1

HÉLÈNE ESNAULT, LARS KINDLER

Exercise 1. Let p be a prime number and fix an algebraic closure $\overline{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$. Write $G := \mathrm{Gal}(\overline{\mathbb{F}}_p)/\mathbb{F}_p)$. Denote by $\varphi \in G$ the Frobenius automorphism, i.e, the $\mathbb{F}_p$-linear automorphism of $\overline{\mathbb{F}}_p$ given by $\varphi(a) = a^p$, $a \in \overline{\mathbb{F}}_p$.

(a) Show that the fixed field of the cyclic subgroup $\langle\varphi\rangle \subseteq G$ is $\mathbb{F}_p$.

(b) Let $a := (a_n)_{n\in\mathbb{N}}$ be a sequence of integers such that $a_n \equiv a_m \mod m$ whenever $m|n$. Show that there exists an element $\psi_a \in G$, such that $\psi_a|_{\mathbb{F}_{p^n}} = \varphi^{a_n}$ for all $n \in \mathbb{N}$.

(c) We now construct a sequence $a := (a_n)_{n\in\mathbb{N}}$ as above, such that $\psi_a \notin \langle\varphi\rangle$. For $n \in \mathbb{N}$, write $n = n'p^{v_p(n)}$ with $(p, n') = 1$, and pick $x_n, y_n \in \mathbb{Z}$ such that $n'x_n + p^{v_p(n)}y_n = 1$. Define $a_n := n'x_n$ and show that $(a_n)_{n\in\mathbb{N}}$ is a sequence of integers such that $a_n \equiv a_m \mod m$ whenever $m|n$, but such that there is no $a \in \mathbb{Z}$ with $a \equiv a_n \mod n$ for all n. Conclude that $\psi_a \notin \langle\varphi\rangle \subseteq G$.

This shows that the classical Galois correspondence does not extend to the case of infinite extensions.

Exercise 2.

(a) Show that $\mathbb{Z}$ can be made into a topological group in which the set of subsets $\{n\mathbb{Z}|\, n \in \mathbb{N}\}$ forms a basis of open neighborhoods of 0.

Define a Cauchy sequence in $\mathbb{Z}$ to be a sequence $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ such that for all $n \in \mathbb{N}$ there exists $N > 1$ such that $a_i \equiv a_j \mod n$ for all $i, j > N$. A Cauchy sequence is called *trivial* if for all $n \in \mathbb{N}$ there exists an N such that $a_i \equiv 0 \mod n$ for all $i > N$.

(b) Show that the group structure of $\mathbb{Z}$ induces an abelian group structure on the set of Cauchy sequences in $\mathbb{Z}$, and that the set of trivial Cauchy sequences is a subgroup. Denote by $\widehat{\mathbb{Z}}$ the quotient of the group of Cauchy sequences by the subgroup of trivial sequences.

Equip $\widehat{\mathbb{Z}}$ with the topology defined by requiring that the sets

$$U_n := \left\{ x \in \widehat{\mathbb{Z}} \middle| \text{for every Cauchy sequence } (a_r)_r \text{ representing } x, a_i \in n\mathbb{Z} \text{ for } i \gg 0 \right\}$$

form a basis of open neighborhoods of 0.

(c) Show that this makes $\widehat{\mathbb{Z}}$ into a topological group with a basis of neighborhoods of 0 given by $\{n\widehat{\mathbb{Z}} \mid n \in \mathbb{N}\}$.

(d) Show that mapping an integer $n \in \mathbb{N}$ to the constant sequence $(n, n, n, \ldots)$ gives rise to a continuous homomorphism $\mathbb{Z} \to \widehat{\mathbb{Z}}$.

If you want your solutions to be corrected, please hand them in just before the lecture on October 25, 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.

Exercise 3. (a) We continue with the setup of Exercise 1. Let $a := (a_n)_{n\in\mathbb{N}}$ be a Cauchy sequence of integers in the sense just defined. Prove that for any $n > 0$, there exists $i_n \gg 0$ such that $(\varphi|_{\mathbb{F}_{p^n}})^{a_{i_n}} = (\varphi|_{\mathbb{F}_{p^n}})^{a_j}$ for all $j \geq i_n$. Check that this implies that setting

$$(\varphi^a)|_{\mathbb{F}_{p^n}} := (\varphi|_{\mathbb{F}_{p^n}})^{a_{i_n}},$$

defines an automorphism $\varphi^a \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

(b) Prove that this construction produces a homeomorphism $\widehat{\mathbb{Z}} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.(*Hint for surjectivity: Consider* $\psi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ *and write* $\psi|_{\mathbb{F}_{p^{n!}}} = (\varphi|_{\mathbb{F}_p^{n!}})^{a_n}$ *with* $a_n \in \{0, \ldots, n!-1\}$. *Show that* $(a_n)_n$ *is Cauchy and that* $\varphi^a = \psi$.)