NUMBER THEORY III – WINTERSEMESTER 2016/17

PROBLEM SET 2

HÉLÈNE ESNAULT, LARS KINDLER

Exercise 1. Let Ω/F be a Galois extension and $E, L \subseteq \Omega$ two subextensions. Prove the following statements.

(a) If E/F is Galois, then EL/L and $E/L \cap E$ are Galois and the map

$$\mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/L \cap E), \sigma \mapsto \sigma|_E$$

is an isomorphism of topological groups.

(b) If E, L are Galois over F, then so is EL.

(c) If E, L are Galois, and $\sigma \in \mathrm{Gal}(E/F), \tau \in \mathrm{Gal}(L/F)$ are such that $\sigma|_{E\cap L} = \tau|_{E\cap L}$, then there exists $\alpha \in \mathrm{Gal}(EL/F)$ such that $\alpha|_E = \sigma$, $\alpha|_L = \tau$.

(d) If E, L are Galois over F, then $\mathrm{Gal}(EL/F)$ can be identified with the subgroup

$$\{ (\tau, \tau') \in \mathrm{Gal}(E/F) \times \mathrm{Gal}(L/F) \big| \, \tau|_{E\cap L} = \tau'|_{E\cap L} \} \subseteq \mathrm{Gal}(E/F) \times \mathrm{Gal}(L/F)$$

Exercise 2. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. We show that in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ there exist finite index subgroups which are neither open nor closed.

(a) Let p be a prime number. Show that $E^{(p)} := \mathbb{Q}[\sqrt{-1}, \sqrt{\ell} | \ell \text{ prime} \leq p]/\mathbb{Q}$ is a Galois extension with Galois group

$$\mathrm{Gal}(E^{(p)}/\mathbb{Q}) \cong \prod_{\{-1\}\cup\{\text{primes } \leq p\}} \mathbb{Z}/2\mathbb{Z}.$$

(b) Write $E := \mathbb{Q}[\sqrt{-1}, \sqrt{p} \mid p \text{ prime}] = \bigcup_p E^{(p)} \subseteq \overline{\mathbb{Q}}$. Show that $E/\mathbb{Q}$ is a Galois extension with Galois group

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \prod_{\{-1\}\cup\{\text{prime numbers}\}} \mathbb{Z}/2\mathbb{Z}.$$

(c) Define $H \subseteq \mathrm{Gal}(E/\mathbb{Q})$ as

$$H := \left\{ (a_i) \in \prod_{\{-1\}\cup\{\text{prime numbers}\}} \mathbb{Z}/2\mathbb{Z} \mid a_i = 0 \text{ for all but finitely many indices } i \right\}.$$

Show that H is a dense subgroup of $\mathrm{Gal}(E/\mathbb{Q})$.

(d) Lemma: Let k be a field and V an infinite dimensional k-vector space. For all $n \geq 1$, there exists a subspace $V_n \subseteq V$, such that V/V_n has dimension n.

(e) Conclude that for every $n \in \mathbb{N}$ there exists a subgroup $G_n \subseteq \mathrm{Gal}(E/\mathbb{Q})$ of index 2^n, such that $H \subseteq G_n$. Show that G_n is neither open nor closed.

(f) Finally, show that the preimage of G_n under the canonical surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(E/\mathbb{Q})$ is not open.

If you want your solutions to be corrected, please hand them in just before the lecture on November 1, 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. Let I be a directed set, let $(G_i, p_i^j)_{i \leq j \in I}$ be an inverse system of finite groups and write

$$G := \varprojlim_{i \in I} G_i.$$

Write $\mathrm{pr}_i : G \to G_i$ for the projections.

(a) Show that there always is a projective system $(G'_i, p'^j_i)_{i \leq j \in I}$, such that $G \cong \varprojlim_i G'_j$ and such that the projections $\mathrm{pr}_i : G \to G'_i$ are surjective.

(b) Show that there always is a projective system $(G'_i, p'^j_i)_{i \leq j \in I}$, such that $G \cong \varprojlim_i G'_j$ and such that the transition maps $p_i^j : G'_j \to G'_i$ are surjective.

(c) Show that there always is a projective system $(G'_i, p'^j_i)_{i \leq j \in I}$, such that $G \cong \varprojlim_i G'_j$ and such that the projection maps pr_i and the transition maps p_i^j are surjective.

(d) Show that G admits a basis of neighborhoods of 1 consisting of open, normal subgroups.

Exercise 4. Let I be a directed partially ordered set, let $\mathcal{G}' := (G'_i, p'^j_i)$, $\mathcal{G} := (G_i, p_i^j)$ be inverse systems of groups. For our purposes, a *morphism* $f : \mathcal{G}' \to \mathcal{G}$ is a sequence of morphisms $f_i : G'_i \to G_i$, such that the diagram

$$\begin{array}{ccc} G'_j & \xrightarrow{f_j} & G_j \\ \downarrow{\scriptstyle p'^j_i} & & \downarrow{\scriptstyle p_i^j} \\ G'_i & \xrightarrow{f_i} & G_i \end{array}$$

commutes whenever $i \leq j$.

(a) Show that the morphism f gives rise to a morphism

$$\varprojlim_{i \in I} f_i : \varprojlim_{i \in I} G'_i \to \varprojlim_{i \in I} G_i.$$

If $\mathcal{G}'' := (G''_i, p''^j_i)$ is a third inverse system, then we say that a sequence

$$1 \to \mathcal{G}' \xrightarrow{f} \mathcal{G} \xrightarrow{h} \mathcal{G}'' \to 1 \qquad (\star)$$

is a *short exact sequence of inverse systems of groups*, if for every $i \in I$ the associated sequence $1 \to G'_i \xrightarrow{f_i} G_i \xrightarrow{h_i} G''_i \to 1$ is a short exact sequence of groups.

(b) Show that it is always true that

$$1 \longrightarrow \varprojlim_{i \in I} G'_i \xrightarrow{\varprojlim_{i \in I} f_i} \varprojlim_{i \in I} G_i \xrightarrow{\varprojlim_{i \in I} h_i} \varprojlim_{i \in I} G''_i$$

is exact.

In general it is not true that $(\star)$ gives rise to a short exact sequence of topological groups

$$1 \longrightarrow \varprojlim_{i \in I} G'_i \xrightarrow{\varprojlim_{i \in I} f_i} \varprojlim_{i \in I} G_i \xrightarrow{\varprojlim_{i \in I} h_i} \varprojlim_{i \in I} G''_i \longrightarrow 1. \qquad (\star\star)$$

(c) Let $(I, \leq)$ be $\mathbb{N}$ with the usual ordering. Fix a prime number $p \in \mathbb{Z}$. We define $\mathcal{G}', \mathcal{G}, \mathcal{G}''$ as follows.

(i) For $i \in \mathbb{N}$, let $G'_i = p^i\mathbb{Z}$, with transition morphisms the inclusion $p^j\mathbb{Z} \to p^i\mathbb{Z}$ if $i \leq j$.

(ii) For $i \in \mathbb{N}$, let $G_i = \mathbb{Z}$, and let every transition morphisms be $\mathrm{id}_{\mathbb{Z}}$. $\mathcal{G}$ is called *constant inverse system* for the group $\mathbb{Z}$.

(iii) For $i \in \mathbb{N}$, let $G''_i = \mathbb{Z}/p^i\mathbb{Z}$, with transition morphisms given by the reduction $\mathbb{Z}/p^j \twoheadrightarrow \mathbb{Z}/p^i$ for $i \leq j$.

The short exact sequences

$$0 \to p^i\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z} \to 0$$

produce a short exact sequence $(\star)$. Compute the limits and show that the associated sequence $(\star\star)$ is not short exact.

On the other hand, if the G'_i, G_i and G''_i are finite for all $i \in I$, then $(\star\star)$ is always short exact:

(d) Prove the following lemma: If $(X_i, \varphi_i^j)_{i \leq j \in I}$ is a projective system of nonempty, compact, Hausdorff topological spaces, then $\varprojlim_{i \in I} X_i$ is nonempty. (*Hint: Use the fact that if* $\{Y_\lambda | \lambda \in J\}$ *is a set of subspaces of a a compact topological space indexed by some index set* J*, such that for any* finite *subset* $J' \subseteq J$*,* $\bigcap_{j \in J'} Y_j \neq \emptyset$*, then* $\bigcap_{j \in J} Y_j \neq \emptyset$*.*)

(e) Conclude that if $h : \mathcal{G} \to \mathcal{G}''$ is a morphism of inverse systems of finite groups such that $h_i : G_i \to G''_i$ is surjective for every i, then

$$\varprojlim_{i \in I} h_i : \varprojlim_{i \in I} G_i \to \varprojlim_{i \in I} G''_i$$

is surjective.