Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 0

Exercise 1.

i) Let k be a finite field and $|\cdot|: k \to \mathbb{R}_{\geq 0}$ an absolute value. Prove that $|x| = 1$ for every $x \in k^\times$.

ii) Let k be a field of characteristic p. Show that there does not exist an archimedean absolute value on k.

iii) Give two non-equivalent archimedean absolute values on $\mathbb{Q}(\sqrt{2})$.

Exercise 2. Let k be a field with a non-archimedean absolute value $|\cdot|$. For $x, y \in k$, define $d(x, y) = |x - y|$.

i) Show that if $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.

ii) For $a \in k$ and $r \in \mathbb{R}_{>0}$, let $D(a, r) = \{x \in k \mid d(x, a) \leq r\}$ be the "closed" disc of center a and radius r. Show that $D(a, r)$ is open and closed in k.

iii) Show that two discs D and D' are either disjoint or concentric (that is, there exists $a \in k$ and $r, r' \in \mathbb{R}_{>0}$ such that $D = D(a, r)$ and $D' = D(a, r')$).

iv) Show that every triangle is isosceles: if for $x, y, z \in k$ one has $d(x, z) < d(y, z)$, then $d(y, z) = d(x, y)$.

Exercise 3. Write the 5-adic expansions of $\frac{2}{3}$, $-\frac{2}{3}$ as elements of $\mathbb{Z}_5$.

Solution:

$$\frac{2}{3} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \dots.$$

$$-\frac{2}{3} = 1 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \dots.$$

Exercise 4. Write the first 4 digits in the 7-adic expansion of a root of the polynomial $x^2 - 2 \in \mathbb{Z}_7[x]$.

Solution:

$$3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3.$$

Exercise 5. The only field automorphism of $\mathbb{Q}_p$ is the identity.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 1

Due date: 26/4/2016

Exercise 1.

1. Let E/K be a Galois extension and let M/K be a Galois subextension of E/K. Let $\mathfrak{p}$ be a nonzero prime ideal of K, let $\mathfrak{P}$ be a prime ideal of L lying over $\mathfrak{p}$, and write $\mathfrak{p}_M = \mathfrak{p} \cap M$. Then $e_{M/K}(\mathfrak{p}_M) = f_{M/K}(\mathfrak{p}_M) = 1$ if and only if the decomposition group $D_{E/K}(\mathfrak{P}) \subseteq \mathrm{Gal}(E/M)$.

2. Let $\mathfrak{p}$ be a nonzero prime ideal of a number field K. Let L/K and L'/K be finite Galois extensions. Show that $\mathfrak{p}$ is split in LL'/K if and only if it is split in L/K and L'/K.

Exercise 2. Show that the polynomial $x^3 - 3x^2 + 2x + 3 \in \mathbb{Z}_3[x]$ decomposes into linear factors over $\mathbb{Q}_3$.

Exercise 3. Let $K/\mathbb{Q}_p$ be a finite extension, and denote by $\mathfrak{p}$ the maximal ideal of the valuation ring of K. Write $p\mathcal{O}_K = \mathfrak{p}^e$. Write $U^{(n)} = 1 + \mathfrak{p}^n$ for $n \geq 1$.

i) Show that for $1 + x \in U^{(1)}$, the following series converges

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

ii) Show that for $x \in \mathfrak{p}^n$ with $n > \frac{e}{p-1}$, the following series converges

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Hint: Let v_p be the p-adic valuation of $\mathbb{Q}_p$. Show that if $\nu = \sum_{i=0}^r a_i p^i$, with $0 \leq a_i < p$, then $v_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^r a_i(p^i - 1)$.

iii) For $n > \frac{e}{p-1}$ show that log maps $U^{(n)}$ into $\mathfrak{p}^n$ and exp maps $\mathfrak{p}^n$ into $U^{(n)}$.

Hint: Show that if $v_\mathfrak{p}$ denotes the normalized valuation of K, then $v_\mathfrak{p}(\log(1+x)) = v_\mathfrak{p}(x)$ and $v_\mathfrak{p}(\exp(x) - 1) = v_\mathfrak{p}(x)$ for $v_\mathfrak{p}(x) > \frac{e}{p-1}$.

iv) Deduce that for $n > \frac{e}{p-1}$, $\log\colon U^{(n)} \to \mathfrak{p}^n$ and $\exp\colon \mathfrak{p}^n \to U^{(n)}$ are mutually inverse isomorphisms.

Hint: Simply invoke the following identities of formal power series:

$$\log((1+X)(1+Y)) = \log(1+X) + \log(1+Y), \quad \exp(X+Y) = \exp(X)\exp(Y),$$

$$\exp(\log(1+X)) = 1 + X, \qquad \log(\exp(X)) = X\,.$$

Exercise 4. Let $((X_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ be an inverse system of topological spaces X_i and continuous maps $f_{ij}\colon X_j \to X_i$. The inverse limit $X = \varprojlim X_i$ is endowed with projection maps

$$p_i\colon X \to X_i\,.$$

Equip X with the following topology: $U \subseteq X$ is an open set if and only if U is a union of subsets of the form $p_{i_1}^{-1}(U_{i_1}) \cap \cdots \cap p_{i_n}^{-1}(U_{i_n})$ for $i_\nu \in I$ and $U_{i_\nu} \subseteq X_{i_\nu}$ open.

i) Show that this is the coarsest topology such that all maps p_i are continuous.

ii) Show that if Y is a topological space and $g_i\colon Y \to X_i$ are continuous maps such that $g_i = f_{ij} \circ g_j$, then there exists a unique continuous map $u\colon Y \to X$ such that $g_i = p_i \circ u$.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 2

Due date: 3/5/2016

Exercise 1. A *topological group* G is a topological space endowed with a group structure such that the operations of product

$$G \times G \to G\,, \qquad (x, y) \mapsto xy$$

and taking inverses

$$G \to G\,, \qquad x \mapsto x^{-1}$$

are continuous maps. Let G and G' be topological groups.

i) Show that a subgroup $H \subseteq G$ is open if and only if it contains an open neighbourhood of the identity element $1 \in G$.

ii) Show that a group homomorphism $f\colon G \to G'$ is continuous if and only if there is a basis of open neighbourhoods $\mathcal{B}$ of the identity $1 \in G'$ such that $f^{-1}(B)$ is open for every $B \in \mathcal{B}$.

iii) Show that every open subgroup of G is also closed.

iv) Give an example of a closed and non-open subgroup in a topological group.

Exercise 2. Let K be a field with a non-trivial non-archimedean absolute value $|\cdot|$. Suppose that K is locally compact with the topology induced by $|\cdot|$. Prove that then K is complete, $|\cdot|$ is discrete, and the residue field is finite.

Exercise 3. Let K be a local field. Prove that:

i) If $\mathrm{Char}(K) = 0$, then $(K^\times)^n$ is an open subgroup of $K^\times$ for every $n \geq 1$.

ii) If $\mathrm{Char}(K) = p$, then $(K^\times)^n$ is an open subgroup of $K^\times$ if and only if $p \nmid n$.

Hint: Use the "p-adic Newton method" in the form that given $f \in \mathcal{O}_K[X]$ and $a \in \mathcal{O}_K$ with $|f(a)| < |f'(a)|^2$ there exists a zero b of f in $\mathcal{O}_K$.

Exercise 4. Let K be a complete non-archimedean field and let $\overline{K}$ denote an algebraic closure. Let $\alpha, \beta \in \overline{K}$, assume that α is separable over $K(\beta)$, and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the Galois conjugates of α over K. Prove that if

$$|\alpha - \beta| < |\alpha - \alpha_i|$$

for $2 \leq i \leq n$, then $K(\alpha) \subseteq K(\beta)$.

Hint: Note that it is enough to show that $\tau(\alpha) = \alpha$ for all $\tau \in \mathrm{Hom}_{K(\beta)}(K(\alpha, \beta), \overline{K})$.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 3

Due date: 10/5/2016

Exercise 1. Give an example of a field K, complete with respect to a non-archimedean absolute value and with perfect residue class field, and two totally ramified extensions L_1/K and L_2/K such that their compositum L_1L_2/K is not totally ramified.

Exercise 2.

i) Prove that there exists a sequence $\{a_n\}_{n\in\mathbb{N}} \subseteq \mathbb{Z}$ satisfying

$$a_n \equiv a_m \pmod{m}$$

whenever $m|n$, but such that there is no $a \in \mathbb{Z}$ such that $a_n \equiv a \pmod{n}$ for every $n \in \mathbb{N}$.

ii) Now let $\mathbb{F}_q$ be a finite field, q some prime power. Deduce from part i) that $\mathrm{Frob}_q^{\mathbb{Z}} \subsetneq \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Exercise 3. Let G be a profinite group and let G' be the closure of its commutator group $[G, G]$. Show that $G^{\mathrm{ab}} = G/G'$ is a profinite group and that every continuous homomorphism $G \to A$, where A is an abelian profinite group, factors through G^{ab}.

Exercise 4.

i) Let K be a local field of characteristic 0. Show that every subgroup of $K^\times$ of finite index is open.

ii) Let K be the extension field of $\mathbb{Q}$ generated by all $\sqrt{p}$ where p is a prime number. Show that $G := \mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$. Via this identification, let $H = \bigoplus_{\mathbb{N}} \mathbb{Z}/2\mathbb{Z} \subset G$. Show that H is dense in G. Prove that there exists a subgroup $H \subset H' \subset G$ such that G/H' is finite but non-trivial (choose a basis of the $\mathbb{F}_2$-vector space G/H in order to find such a H'). Conclude that G has normal subgroups of finite index which are not open. (*Remark.* It is easy to deduce that also $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has normal subgroups of finite index which are not open.)

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 4

Due date: 17/5/2016

Exercise 1. Let E/K be a finite Galois extension of local fields. Prove that $\mathrm{Gal}(E/K)$ is solvable.

Exercise 2. Let L/K be an unramified extension of non-archimedean local fields. Let $f = [L : K]$, let $\pi \in K$ be a uniformizer, and let κ and λ be the residue fields of K and L.

i) Let $n = |\lambda| - 1$ and $m = |\kappa| - 1$. The mth (resp. nth) roots of unity are contained in K (resp. L). Prove that for every mth root of unity ζ in K there is an nth root of unity ξ in L such that $N_{L/K}(\xi) = \zeta$.

   Hint: It is enough to show that if ξ is a primitive nth root of unity, then

$$N_{L/K}(\xi) = \xi^{1+|\kappa|+|\kappa|^2 \cdots + |\kappa|^{f-1}}$$

   is a primitive mth root of unity.

ii) Prove that $N_{L/K}(L^\times) = \langle \pi^f \rangle \times \mathcal{O}^\times$, where $\mathcal{O}$ denotes the ring of integers of K.

   Hint: The difficulty is showing that $\mathcal{O}^\times$ is contained in $N_{L/K}(L^\times)$. Let $\overline{\gamma}$ be a generator of $\lambda^\times$ and let $\overline{\alpha} = N_{\lambda/\kappa}(\overline{\gamma})$ be a generator of $\kappa^\times$. By i), it is enough to show that for every $\alpha \in \mathcal{O}^\times$ such that $\alpha \equiv \overline{\alpha} \pmod{\pi}$ there exists $\gamma \in L^\times$ such that $N_{L/K}(\gamma) = \alpha$. Let $f(T) \in \kappa[T]$ be the minimal polynomial of $\overline{\gamma}$ over κ. Show that you can obtain such a γ as a root of a lift of $f(T)$ in $K[T]$, whose constant term is $(-1)^f\alpha$.

Exercise 3. Let K be a non-archimedean local field, and denote by π a uniformizer of K. Let K^{un} and K^{tr} be its maximal unramified and maximal tamely ramified extensions. Denote by $I^{\mathrm{tr}} = \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}})$ the tame inertia group. Recall from the course that there is a canonical isomorphism

$$t_0 \colon I^{\mathrm{tr}} \xrightarrow{\cong} \varprojlim_{p \nmid e} \mu_e(K^{\mathrm{un}})$$

induced by the isomorphisms $\mathrm{Gal}(K(\sqrt[e]{\pi})/K) \cong \mu_e(K^{\mathrm{un}})$, $\sigma \mapsto \sigma(\sqrt[e]{\pi})/\sqrt[e]{\pi}$ (where $\sqrt[e]{\pi}$ denotes a fixed zero of $X^e - \pi$).

1. Let $\varphi \in \mathrm{Gal}(K^{\mathrm{un}}/K)$ be the Frobenius automorphism. Then φ acts on I^{tr} by conjugation (i.e., every lift of φ to an element of $\mathrm{Gal}(K^{\mathrm{tr}}/K)$ acts on the normal subgroup I^{tr} by conjugation, and the action is independent of the lift). Show that

$$t_0(\varphi\sigma\varphi^{-1}) = t_0(\sigma)^q.$$

2. Conclude that the extension K^{tr}/K is not abelian.

Exercise 4.

i) Give an example of a group G and an exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

such that

$$0 \to A^G \to B^G \to C^G \to 0$$

is not exact.

ii) Give an example of a group G and G-modules A and B such that the map

$$A^G \otimes B^G \to (A \otimes B)^G$$

is neither injective nor surjective.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 5

Due date: 24/5/2016

Exercise 1. Let

$$\cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{d_0} C_{-1} \to \dots$$

be a sequence of abelian groups such that for every $q \in \mathbb{Z}$ there exists a group homomorphism $h_q \colon C_q \to C_{q+1}$ such that $h_{q-1} \circ d_q + d_{q+1} \circ h_q = \mathrm{id}_{C_q}$. Show that $C_\bullet$ is exact if one of the following conditions is satisfied:

1. The sequence $C_\bullet$ is a complex, i.e., $d_q \circ d_{q+1} = 0$ for all q.
2. We have $C_q = 0$ for all $q < -1$ and $d_0 \circ d_1 = 0$ and that h_q is surjective for all q.

Exercise 2. Let G be a group and A a G-module. A map $\varphi \colon G \to A$ is called a 1-*cocycle* if for every $\sigma, \tau \in G$ one has

$$\varphi(\sigma\tau) = \varphi(\sigma) + \sigma\varphi(\tau).$$

Let $Z^1(G, A)$ denote the group of 1-cocycles (with addition induced by the addition on A). A map $\varphi \colon G \to A$ of the form $\varphi(\sigma) = \sigma(b) - b$ (for some fixed $b \in A$) is called a 1-*coboundary*. Let $B^1(G, A)$ denote the group of 1-coboundaries; check that this is a subgroup of $Z^1(G, A)$. The first cohomology group of A is then defined as the quotient

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)\,.$$

i) Let $G = \mathbb{Z}/2Z = \{1, -1\}$ act on $A = \mathbb{Z}$ in the following way: the nontrivial element -1 satisfies $-1 \cdot a = -a$ for every $a \in \mathbb{Z}$. Compute $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$.

ii) Let $G = (\mathbb{Z}/4\mathbb{Z})^\times$ act on $A = \mathbb{Z}/4\mathbb{Z}$ by multiplication. Determine the group $H^1((\mathbb{Z}/4\mathbb{Z})^\times, \mathbb{Z}/4\mathbb{Z})$.

iii) If p is a prime and the action on $\mathbb{Z}/p\mathbb{Z}$ is the natural one by multiplication, what is $H^1((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{Z}/p\mathbb{Z})$?

Exercise 3. Let L be a finite Galois extension of the field K, and let $G = \mathrm{Gal}(L/K)$.

i) Prove that $H^1(G, L^\times) = 1$.

Hint: Given a 1-cocycle $\varphi \colon G \to L^\times$, construct a 1-coboundary from the element

$$b = \sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma(a)$$

for $a \in L^\times$ chosen such that $b \neq 0$. To show that there exists $a \in L^\times$ such that $b \neq 0$, use Dedekind's theorem on the independence of characters.

ii) Suppose that G is cyclic and that σ is a generator of G. Show that if $a \in L^\times$ is such that $N_{L/K}(a) = 1$, then there exists $b \in L^\times$ such that $a = b/\sigma(b)$.

Hint: Show that if $a \in L^\times$ is such that $N_{L/K}(a) = 1$, then there is a 1-cocycle $\varphi\colon G \to L^\times$ uniquely characterized by the condition $\varphi(\sigma) = a$.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 6

Due date: 31/5/2016

Exercise 1. Let G be a group and A an abelian group. (In this exercise and Exercise 2 we write all groups multiplicatively.) A *group extension of G by A* is a short exact sequence of groups

$$0 \to A \to E \xrightarrow{\pi} G \to 1\,.$$

An extension is said to split if there exists a group homomorphism $\sigma\colon G \to E$ such that $\pi \circ \sigma = \mathrm{id}$.

i) Show that in an extension of G by A, the abelian group A has a G-module structure with action defined by ${}^g a = g' a g'^{-1}$ for $a \in A$ and $g \in G$, and $g' \in E$ any lift of g.

ii) The semidirect product $A \rtimes G$ of a group G and a G-module A is a group with underlying set $A \times G$ and multiplication given by the formula

$$(a, g) \cdot (b, h) = (a \cdot {}^g b, gh)\,.$$

Show that $A \rtimes G$ is indeed a group.

iii) Prove that the group extension $0 \to A \to E \to G \to 1$ splits if and only if E is isomorphic to $A \rtimes G$, where G acts on A as in i).

Exercise 2. Let G be a group and A a G-module. We will be interested in extensions ξ of G by A such that the given G-module structure on A coincides with that induced by ξ as in Exercise 1 ii). Say that two such group extensions $\xi_i\colon 0 \to A \to E_i \to G \to 1$ of G by A with $i = 1, 2$ are equivalent if there exists a group isomorphism $\varphi\colon E_1 \simeq E_2$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

is commutative. Let $\mathrm{EXT}(G, A)$ denote the set of equivalence classes of extensions of G by A inducing the given G-module structure on A. Given a group extension $\xi\colon 0 \to A \to E \xrightarrow{\pi} G \to 1$, define

$$c_\xi(g, h) = \sigma(g)\sigma(h)\sigma(gh)^{-1} \in A\,,$$

where $\sigma\colon G \to E$ is a map such that $\pi \circ \sigma = \mathrm{id}$.

i) Prove that c_ξ lies in $Z^2(G, A)$, that its cohomology class γ_ξ only depends on the equivalence class $[\xi]$ of ξ, and that the association $[\xi] \mapsto \gamma_\xi$ gives a bijection between $\mathrm{EXT}(G, A)$ and $H^2(G, A)$.

ii) Let $m, n \in \mathbb{Z}_{>1}$, and let $\mathbb{Z}/m\mathbb{Z}$ act trivially on $\mathbb{Z}/n\mathbb{Z}$. We will see later in the course that

$$H^2(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/(n, m)\mathbb{Z}.$$

Prove this for $(m, n) = (2, 2), (2, 3), (3, 3)$.

Hint: Prove that every extension E of a cyclic group G by an abelian group A contained in the center of E is again an abelian group, and then use i).

Exercise 3. For a cyclic field extension L/K, show that $H^1(\mathrm{Gal}(L/K), L) = 0$.

Exercise 4. For a finite group G, we define the *character group* $G^\vee := \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of G. Prove that the natural map $G \to G^{\vee\vee}$ induces an isomorphism $G^{\vee\vee} = G^{\mathrm{ab}}$.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 7

Due date: 7/6/2016

Exercise 1. Let G be a finite group and A a G-module.

i) Show that $\mathrm{Ord}(G) \cdot H_T^q(G, A) = 0$ for all $q \in \mathbb{Z}$.

   Hint: Use dimension shift.

ii) Show that if the multiplication map

$$A \to A\,, \qquad a \mapsto \mathrm{Ord}(G)a$$

   is an isomorphism, then $H_T^q(G, A) = 0$.

Exercise 2. Prove that $H^2(G, \mathbb{Z}) = G^\vee$.

Hint: Consider the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ *and apply the previous exercise.*

Exercise 3. Let G be a finite group and A a finite abelian group of order coprime to the order of G. Prove that any extension

$$1 \to A \to E \to G \to 1$$

is split.

Hint: Use Exercise 1 and Exercise 2 of PS6.
Remark: More generally, the Theorem of Schur and Zassenhaus says that the condition that A be abelian can be dropped.

Exercise 4. Let $m \geq 1$ be an integer, and let k be a field whose characteristic is coprime to m. Let $\overline{k}$ be a separable closure of k, and let $G = \mathrm{Gal}(\overline{k}/k)$. Denote by $\mu_m \subseteq \overline{k}^\times$ the subgroup of $m-$th roots of unity.

i) Show that $k^\times/(k^\times)^m \simeq H^1(G, \mu_m)$.

ii) Assume that $\mu_m \subseteq k^\times$, so that the first part yields an isomorphism

$$\psi \colon k^\times/(k^\times)^m \xrightarrow{\sim} \mathrm{Hom}(G, \mu_m).$$

   Prove that the maps

$$k' \mapsto \psi^{-1}(\mathrm{Hom}(\mathrm{Gal}(k'/k), \mu_m)),$$
$$B \mapsto k(\sqrt[m]{b};\, b \in B)$$

   define a bijection between the finite abelian extensions k'/k inside $\overline{k}$ whose Galois group is annihilated by m and finite subgroups of $k^\times/(k^\times)^m$.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 8

Due date: 14/6/2016

Exercise 1. Let G be a finite group and let A be a G-module. Denote by $H^q_T(G,A)_p$ the *p-primary part* of $H^q_T(G,A)$, that is, the group of all elements whose order is a power of p. Let G_p denote a p-Sylow subgroup of G. Prove that:

i) $\mathrm{res}_q\colon H^q_T(G,A)_p \to H^q_T(G_p,A)$ is injective.

ii) $\mathrm{cor}_q\colon H^q_T(G_p,A) \to H^q_T(G,A)_p$ is surjective.

Exercise 2. Let G be a finite group and $H \subseteq G$ a subgroup. For each coset $\xi \in H\backslash G$, choose a representative $\sigma(\xi)$, i.e.,

$$G = \bigcup_{\xi \in H\backslash G} H\sigma(\xi) \quad \text{(disjoint union)}.$$

For a G-module C and $c \in {}_{N_G}C$, define

$$N'_{G/H}(c) = \sum_{\xi} \sigma(\xi)\cdot c \in {}_{N_H}C\,.$$

i) Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of G-modules. Show that the diagram

$$\begin{array}{ccc} H_T^{-1}(G,C) & \xrightarrow{\ \delta\ } & H_T^{0}(G,A) \\ \Big\downarrow{\scriptstyle N'} & & \Big\downarrow{\scriptstyle \mathrm{res}_0} \\ H_T^{-1}(H,C) & \xrightarrow{\ \delta\ } & H_T^{0}(H,A) \end{array}$$

is commutative. Here, we define $N'(c + I_GC) = N'_{G/H}(c) + I_HC$. Recall that we know from the lecture that $\mathrm{res}_0(a + N_GA) = a + N_HA$.

ii) Deduce that $N' = \mathrm{res}_{-1}$.

iii) Let $\tau \in G$. Show that

$$\sigma(\xi)\cdot\tau\cdot\sigma(\xi\tau)^{-1} \in H \quad \text{for all } \xi \in H\backslash G.$$

Show that the transfer map $\mathrm{ver}\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is given by the formula

$$\mathrm{ver}(\tau G') = \left(\prod_{\xi\in H\backslash G} \sigma(\xi)\tau\sigma(\xi\tau)^{-1}\right) H'\,.$$

Hint: Use the identification $G^{\mathrm{ab}} = I_G/I_G^2$ *(and similarly for* H*), and that by part ii) the restriction map* $I_G/I_G^2 = H_T^{-1}(G, I_G) \to H_T^{-1}(H, I_G) = I_G/I_H I_G$ *is given by* N'.

Exercise 3. Let $G = \mathbb{Z}/6\mathbb{Z}$ act on $A = \mathbb{Z}/3\mathbb{Z}$ in the following way: the action of a generator of G is given by the formula $a \mapsto -a$. Show that:

i) $H_T^q(G, A) = 0$ for $q = 0, -1$. (We will see soon that this implies $H_T^q(G, A) = 0$ for every $q \in \mathbb{Z}$ since G is cyclic.)

ii) The G-module A is, however, not *cohomologically trivial*, that is, there exists $H \subseteq G$ and $q \in \mathbb{Z}$ such that $H_T^q(H, A) \neq 0$.

Exercise 4. Let $G = \mathbb{Z}/2\mathbb{Z}$ act on $A = \mathbb{Z}/8\mathbb{Z}$ in the following way: the action of the non-trivial element of G is given by the formula $a \mapsto 3a$.

i) Show that $H_T^q(G, A) = 0$ for $q = 0, -1$. (By the remark in Ex. 3 i) this implies that the G-module A is cohomologically trivial.)

ii) Let $B = \mathbb{Z}/2$ with trivial G-action. Prove that the G-module $A \otimes B$ is not cohomologically trivial.

Hint: Recall from PS6 Exercise 2 part ii) that $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ *when* $\mathbb{Z}/2\mathbb{Z}$ *acts trivially on* $\mathbb{Z}/2\mathbb{Z}$.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 9

Due date: 21/6/2016

Exercise 1. Let M be an abelian group and f, g endomorphisms of M such that $f \circ g = g \circ f = 0$. The Herbrand quotient is defined as

$$q_{f,g}(M) = \frac{[\mathrm{Ker}(f) : \mathrm{Im}(g)]}{[\mathrm{Ker}(g) : \mathrm{Im}(f)]} \in \mathbb{Q}\,,$$

provided that $[\mathrm{Ker}(f) : \mathrm{Im}(g)]$ and $[\mathrm{Ker}(g) : \mathrm{Im}(f)]$ are finite.

i) Show that if M is finite, then $q_{f,g}(M) = 1$.

ii) Suppose that G is cyclic and that M is a G-module such that the cohomology groups $H^1(G, M), H^2(G, M)$ are finite. If σ is a generator of G, we write $h(M) = q_{\sigma-1,N_G}(M)$. Check that

$$h(M) = \frac{\#H^2(G, M)}{\#H^1(G, M)}\,.$$

iii) Compute $h(\mathbb{Z})$, where G acts trivially on $\mathbb{Z}$.

Exercise 2. Let G be a finite cyclic group. Show that if

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of G-modules, then $h(M) = h(M')h(M'')$, in the sense that whenever two of the three Herbrand quotients are defined, then so is the third one, and that in this case equality holds.

Exercise 3. Let L/K be a finite unramified extension of local fields with Galois group G, and let $U_L = \mathcal{O}_L^\times$. Show that $H^r_T(G, U_L) = 0$ for all $r \in \mathbb{Z}$.

Hint: Show that that there is an isomorphism $L^\times \simeq U_L \times \mathbb{Z}$ of G-modules, where we let G act trivially on $\mathbb{Z}$. Then use Ex. 3 of PS5 and Ex. 2 of PS4.

Exercise 4. Let G be a topological group and let M be a G-module. Show that the following are equivalent:

i) The map $G \times M \to M$ defined by $(g, m) \mapsto {}^g m$ is continuous, where M carries the discrete topology and $G \times M$ is endowed with the product topology.

ii) The stabilizer in G of any element $m \in M$ is open.

iii) $M = \bigcup_H M^H$, where H runs through all the open subgroups of G.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 10

Due date: 28/6/2016

Exercise 1. Let G be a group and A a (not necessarily commutative) group on which G operates by group isomorphisms. We write A multiplicatively, and by abuse of notation call A a non-commutative G-module. A map $\varphi\colon G \mapsto A$ is called a 1-*cocycle* if $\varphi(\sigma\tau) = \varphi(\sigma)\cdot\sigma(\varphi(\tau))$ for every $\sigma, \tau \in G$. We denote by $Z^1(G, A)$ the set of all 1-cocycles. Say that two 1-cocycles φ, ψ are cohomologous, and write $\varphi \sim \psi$, if there exists $a \in A$ such that $\psi(\sigma) = a^{-1}\cdot\phi(\sigma)\cdot\sigma(a)$ for every $\sigma \in G$. Show that $\sim$ is an equivalence relation. The first cohomology group of A is the set of cohomology classes

$$H^1(G, A) = Z^1(G, A)/\sim\ .$$

Note that $H^1(G, A)$ has the structure of a "pointed set", that is, a set with a distinguished element corresponding to the trivial 1-cocycle satisfying $\varphi(\sigma) = 1$ for every $\sigma \in G$.

Remark: Note that if A is abelian, $H^1(G, A)$ coincides with the group defined in Ex. 2 of PS5.

Exercise 2. Let

$$1 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 1$$

be a sequence of non-commutative G-modules.

i) Given $c \in C^G$, define

$$\delta(c)\colon G \to A\,, \qquad \delta(c)(\sigma) = i^{-1}(b^{-1}\cdot\sigma(b))\,,$$

where $b \in B$ is such that $\pi(b) = c$. Show that $\delta(c) \in Z^1(G, A)$ and that its cohomology class is independent of the choice of b.

ii) Show that the sequence of pointed sets

$$1 \to A^G \xrightarrow{i_0} B^G \xrightarrow{\pi_0} C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{i_1} H^1(G, B) \xrightarrow{\pi_1} H^1(G, C)$$

is exact.

Remark: By the kernel of a morphism of pointed sets we mean the preimage of the distinguished element of the target set. One can see any group as a pointed set by considering the set underlying the group together with the neutral element. Above, i_0, i_1, (resp. π_0, π_1) are the maps induced by i (resp. π).

Exercise 3. Let L/K be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(L/K)$. Consider the natural action of G on $\mathrm{GL}_n(L)$.

i) Show that $H^1(G, \mathrm{GL}_n(L)) = 1$.

Hint: Imitate the procedure of PS 5, Ex. 3. To show that given a 1*-cocycle* $\varphi\colon G \to \mathrm{GL}_n(L)$*, there exists* $C \in \mathrm{GL}_n(L)$ *such that* $B = \sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma(C)$ *is invertible, show first that a linear form* $L^n \to L$ *which vanishes on the image of the map*

$$b\colon L^n \to L^n\,, \qquad b(x) := \sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma(x)$$

must be zero on all of L^n*. In other words, the image of* b *generates* L^n *over* L*. Then, if* $x_1, \ldots, x_n \in L^n$ *are such that the* $y_i = b(x_i)$ *generate* L^n*, take* C *to be the matrix of the linear map that sends the canonical basis* e_i *to* x_i*.*

ii) Deduce that $H^1(G, \mathrm{SL}_n(L)) = 1$.

Exercise 4. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. For $n \geq 1$, let G act naturally on L^n and by

$$\sigma(\psi)(x) = \sigma(\psi(\sigma^{-1}(x))) \qquad \text{for all } \psi \in \mathrm{Aut}(L^n),\ x \in L^n$$

on $\mathrm{Aut}(L^n)$.

i) Show that giving $\phi \in Z^1(G, \mathrm{GL}_n(L))$ is equivalent to giving a family of K-vector space isomorphisms $\psi_\sigma\colon L^n \to L^n$ satisfying

$$\psi_\sigma \psi_\tau = \psi_{\sigma\tau} \qquad \text{for all } \sigma, \tau \in G$$

and

$$\psi_\sigma(\alpha x) = \sigma(\alpha)\psi_\sigma(x) \qquad \text{for all } \alpha \in L,\ x \in L^n.$$

Hint: To construct the family of ϕ_σ *from the* 1*-cocycle* ϕ*, set* $\psi_\sigma := \phi(\sigma) \circ \sigma(\cdot)$*.*

ii) Note that we can endow L^n with a new action of G by letting $\sigma \in G$ send $x \in L^n$ to $\psi_\sigma(x) \in L^n$. Write V to denote L^n with this new G-module structure. Show that

$$V^G = \{v \in V \mid \psi_\sigma(v) = v \text{ for all } \sigma \in G\}$$

satisfies $\dim_K(V^G) = n$ (and hence the natural map $V^G \otimes_K L \to V$ is an isomorphism).

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 11

Due date: 5/7/2016

Exercise 1. *Algebraic independence of characters*
Let K be an infinite field, L/K be a finite Galois extension, and $\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n$ the Galois automorphisms of L/K. Let $f \in K[X_1, \dots, X_n]$ be such that

$$f(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) = 0$$

for all $\alpha \in L$. Prove that $f = 0$.

Hint: Fix a basis of L as a K-vector space, and do a suitable change of coordinates so that you can use the following fact (which you may use without proof): Let E be an infinite field, and let $g \in E[X_1, \dots, X_r]$ with $g(x_1, \dots, x_r) = 0$ for all $x_i \in E$. Then $g = 0$.

Exercise 2. Apply algebraic independence of characters to give another proof of PS 10, Ex. 3 i) in the case that K is infinite.

Hint: With the notation introduced in the hint of that exercise, let $C = cE_n$, $c \in L^\times$, be a scalar matrix and consider $\det(B)$.

Exercise 3. *Normal basis theorem*
Prove that if L/K is a finite Galois extension with K an infinite field (and notation as in Exercise 1), there exists $\alpha \in L^\times$ such that $\sigma_i(\alpha)$ is a basis of L as a K-vector space.

Hint: Consider the matrix $A = (a_{i,j}) \in M_n(K[X_1, \dots, X_n])$, where $a_{i,j} = X_k$ if $\sigma_i \circ \sigma_j = \sigma_k$. Show that $\det(A) \neq 0$ and use algebraic independence of characters to prove the existence of $\alpha \in L^\times$ such that $\det(B) \neq 0$, where $B = (\sigma_i \circ \sigma_j(\alpha)) \in M_n(L)$.

Remark: The statement is also true for finite fields.

Exercise 4.

i) Let A be a discrete $\widehat{\mathbb{Z}}$-module. Show that $H^2(\widehat{\mathbb{Z}}, A) = 0$, if A is torsion (i.e., for all $a \in A$, there exists $n \in \mathbb{Z} \setminus \{0\}$ with $na = 0$).

   Hint: Writing A as an inductive limit of finite $\widehat{Z}$-modules reduces to the case that A is finite. Denote by N_n the norm of $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} (\cong \mathbb{Z}/n\mathbb{Z})$. Now apply the fact below to identify $\varinjlim H^2(\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}}, A^{n\widehat{\mathbb{Z}}}) = \varinjlim A^{\widehat{\mathbb{Z}}}/N_n A$, with transition maps $A^{\widehat{\mathbb{Z}}}/N_m A \to A^{\widehat{\mathbb{Z}}}/N_{mn} A$ given by multiplication by n.

   Fact. Let G be a cyclic group of order n, let $\sigma \in G$ be a generator, and let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be defined by $\chi(\sigma) = 1/n$. Let $\theta = \delta(\chi) \in H^2(G, \mathbb{Z})$, where δ is the connecting homomorphism for the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Let A be a G-module. Show that

$$H^0_T(G, A) \longrightarrow H^2_T(G, A), \qquad a \mapsto a \cup \theta,$$

is an isomorphism.

ii) Deduce that $H^2(\widehat{\mathbb{Z}}, A) = 0$ if A is divisible (i.e., multiplication by n is a surjection $A \to A$ for all $n \in \mathbb{Z} \setminus \{0\}$).

iii) Let K be a perfect field with absolute Galois group $\mathrm{Gal}(\overline{K}/K) \cong \widehat{\mathbb{Z}}$. Show that the *Brauer group* $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$ is trivial.

iv) Let K be a perfect field with absolute Galois group $\mathrm{Gal}(\overline{K}/K) \cong \widehat{\mathbb{Z}}$. Show that for each finite extension L/K, the norm map $N_{L/K}$ is surjective.

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 12

Due date: 12/7/2016

Exercise 1. Let $\zeta_1, \zeta_2 \in \overline{\mathbb{Q}}_p$ be roots of unity such that $\mathbb{Q}_p(\zeta_1)/\mathbb{Q}_p$ is unramified of degree f and ζ_2 has order p^m. Show that

$$N_{\mathbb{Q}_p(\zeta_1\zeta_2)/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_1\zeta_2)^\times) = \langle p^f \rangle \times U^{(m)}\,.$$

Exercise 2. *Local Kronecker-Weber*
Show that every finite abelian extension $K/\mathbb{Q}_p$ is contained in a field of the form $\mathbb{Q}_p(\zeta)$, where $\zeta \in \overline{\mathbb{Q}}_p$ is a root of unity.

Exercise 3. *Artin-Schreier theory*
Let k be a field of characteristic $p > 0$, $\overline{k}$ a separable closure of k, and $G = \mathrm{Gal}(\overline{k}/k)$. Prove that there is an exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k \xrightarrow{\wp} k \to H^1(G, \mathbb{Z}/p\mathbb{Z}) \to 0\,,$$

where $\wp(x) = x^p - x$ and G acts trivially on $\mathbb{Z}/p\mathbb{Z}$.

Exercise 4. Let $K/\mathbb{Q}_p$ be a finite extension containing all mth roots of unity ($m \geq 1$). For $a \in K^\times$, set $L_a = K(\sqrt[m]{a})$, and let $L = K(\sqrt[m]{a};\ a \in K)$ be the compositum of all L_a. Prove that

$$(K^\times)^m = \bigcap_{a \in K^\times} N_{L_a/K}(L_a^\times) = N_{L/K} L^\times\,.$$

Hint: Use Kummer theory (PS 7, Ex. 4).

Prof. Dr. U. Görtz
Dr. F. Fité

Sommersemester 2016

ALGEBRAIC NUMBER THEORY II

Problem Set 13

Due date: 19/7/2016

Exercise 1. Let L/K be a finite abelian extension of $\mathfrak{p}$-adic number fields. Show that the norm residue symbol

$$(\, , L/K) \colon K^\times \to \mathrm{Gal}(L/K)$$

maps the group of units U_K onto the inertia group $I_{L/K}$ and the the group of principal units $U_K^{(1)}$ onto the wild ramification group $P_{L/K}$.

Hint: Recall that $U_K^{(1)}/U_K^{(n)}$ (resp. $P_{L/K}$) are the unique p-Sylow subgroups of $U_K/U_K^{(n)}$ (resp. $I_{L/K}$).

Exercise 2. Let K be a number field, and let $\mathbb{I}_K$ be its group of ideles. Consider the content map $c \colon \mathbb{I}_K \to \mathbb{R}_{>0}$, $(\alpha_v)_v \mapsto \prod_v |\alpha_v|_v$.

i) Show that c is a continuous and surjective group homomorphism.

ii) Let $\mathbb{I}^1$ be the kernel of c. Show that the image of $K^\times$ in $\mathbb{I}_K$ under the diagonal embedding is contained in $\mathbb{I}^1$.

iii) Using, without proof, the fact that the quotient $\mathbb{I}^1/K^\times$ is compact, show that the ideal class group of K is finite.

Exercise 3. Let $K/\mathbb{Q}$ be a number field. Show that $K \subseteq \mathbb{A}_K$ is discrete, that $\mathbb{A}_K/K$ is compact, and that $K^\times \subseteq \mathbb{I}_K$ is discrete.

Hint: Reduce when necessary to the case $K = \mathbb{Q}$.

Exercise 4. Let K be a number field, and let S be a finite set of places of K. Show that $\mathbb{I}_K^S K^\times$ is dense in $\mathbb{I}_K$.

Hint: Use the weak approximation theorem.