May 3rd, 2013

Zahlentheorie II

Exercise sheet 8[1]

Exercise 1 (1 Point)**.** Let A be a Dedekind domain, K be its fraction field, and let I denote the multiplicative group of non-zero fractional ideals. Let $P \subseteq I$ be the subset principal ideals, i.e. P be the image of the map $K^* \to I$ sending $a \in K^* := K \setminus \{0\}$ to the fractional ideal generated by a. Show that P is a subgroup of K^* and that we have an exact sequence of groups

$$1 \to U \to K^* \to I \to H \to 1$$

where U is the group of invertible elements in A, $H := I/P$.

Exercise 2 (2 Points)**.** Let K be a number field with ring of integers O_K. A *modulus* is a finite formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu(\mathfrak{p})},\ \nu(\mathfrak{p}) > 0$$

where $\mathfrak{p}$ are maximal ideals of O_K (finite places) or imbeddings $K \hookrightarrow \mathbb{R}$ (real places). We say a prime $\mathfrak{p}$ *divides* $\mathfrak{m}$ or $\mathfrak{p}|\mathfrak{m}$ for some finite place $\mathfrak{p}$, if $\mathfrak{p}$ appears in the product. Let $I(\mathfrak{m})$ be the set of fractional ideals *relatively prime* to $\mathfrak{m}$, i.e. the primes ideals which appear in the factorization of the fractional ideal do not divide $\mathfrak{m}$. $P(\mathfrak{m}) := P \cap I(\mathfrak{m})$. Prove that the map

$$I(\mathfrak{m})/P(\mathfrak{m}) \to I/P$$

induced by the inclusion $I(\mathfrak{m}) \subseteq I$ is an isomorphism.

Exercise 3 (1 Point)**.** Let L/K be an abelian extension (i.e. a Galois extension whose Galois group is abelian) of number fields. Let $\mathfrak{p}$ be a prime of K which is unramified in L. Thus for any prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$ there is a unique element σ in the decomposition group $G_{\mathfrak{q}} \subseteq \mathrm{Gal}(L/K)$ having the effect

$$\sigma\alpha \equiv \alpha^q \pmod{\mathfrak{q}} \qquad \alpha \in O_L$$

where q is the cardinality of the residue field k of K at $\mathfrak{p}$. (See [Local Fields][Chapter I, §8, Page 23, first paragraph]) Show that $\sigma \in \mathrm{Gal}(L/K)$ is independent of the choice of the $\mathfrak{q}$. Thus we get a well defined symbol

$$(\mathfrak{p}, L/K) := \sigma$$

which is called the *Artin symbol* of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$.

Exercise 4 (3 points)**.** Notations being as in the previous exercise, we get a map ϕ from the set of unramified primes in K (i.e. all the primes in L lying above these primes in K are unramified) to $\mathrm{Gal}(L/K)$:

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K).$$

This map ϕ extends by linearity to a map from the set of all fractional ideals which do not contain ramified primes to $\mathrm{Gal}(L/K)$. Thus for any fractional ideal $\mathfrak{a}$ which does not contain a ramified ideal we still have the Artin symbol $(\mathfrak{a}, L/K)$. Show that the the Artin symbol $(\mathfrak{a}, L/K)$ satisfies the following properties:

[1]Please hand in your answers before June 19th.

(1) Let $L' \supseteq L \supseteq K$ be a bigger abelian extension. If $\mathfrak{a}$ is a fractional ideal in K which does not contain a ramified prime in L'/K, then

$$\mathrm{Res}_L(\mathfrak{a}, L'/K) = (\mathfrak{a}, L/K)$$

where Res_L is the restriction map $\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$.

(2) Let E/K be any finite extension, then LE/E is an abelian extension (You have to show this!). Let $\mathfrak{p}$ be a prime in K unramified in L and let $\mathfrak{q}$ be a prime of E lying above $\mathfrak{p}$. Then we have

$$\mathrm{Res}_L(\mathfrak{q}, LE/E) = (\mathfrak{p}, L/K)^f$$

where Res_L is the restriction map $\mathrm{Gal}(LE/E) \subseteq \mathrm{Gal}(LE/K) \to \mathrm{Gal}(L/K)$ and $f := [O_E/\mathfrak{q} : O_K/\mathfrak{p}]$ is the residue degree.

(3) Let E be as above, and let $\mathfrak{b}$ be a fractional ideal of E such that if $\mathfrak{q}$ occurs in the factorization of $\mathfrak{b}$ and $\mathfrak{q}|\mathfrak{p}$ with $\mathfrak{p}$ in K, then $\mathfrak{p}$ is unramified in L. Then

$$\mathrm{Res}_L(\mathfrak{b}, LE/E) = (N_K^E\mathfrak{b}, L/K)$$

where N_K^E is the *norm homomorphism* which is defined in the following way. Take any maximal ideal $\mathfrak{q}$ in O_E then $N_K^E(\mathfrak{q})$ is defined to be $\mathfrak{p}^{f_\mathfrak{q}}$, where $\mathfrak{p} := \mathfrak{q} \cap O_K$ and $f_\mathfrak{q}$ is the residue degree of E/K at $\mathfrak{q}/\mathfrak{p}$. Then we extend this map by linearity to a map from the set of fractional ideals in E to the set of fractional ideals in K. See also [Local Fields][Ch I, §5]. In particular, if $L \supseteq E \supseteq K$ then

$$(\mathfrak{b}, L/E) = (N_K^E\mathfrak{b}, L/K).$$

(4) Let $\mathfrak{m}$ be a modulus that is divisible by all ramified primes, show that ϕ extends to a group homomorphism

$$\omega : I(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

$$\mathfrak{a} \mapsto (\mathfrak{a}, L/K).$$

This map ω is called the *reciprocity law map* or the *Artin map*.

Exercise 5 (1 Point)**.** Let K be a number field, $\mathfrak{m}$ be a modulus. If $\alpha \in K^*$, we define

$$\alpha \equiv 1 \ (\mathrm{mod}^*\mathfrak{m})$$

to mean that α satisfies the following two conditions:

(1) If $\mathfrak{p}$ is a finite place (a maximal ideal in O_K) in $\mathfrak{m}$, then $\alpha \in (O_K)_\mathfrak{p}$, and

$$\alpha \equiv 1 \ (\mathrm{mod}\ (\mathfrak{p}O_K)_\mathfrak{p}^{\nu(\mathfrak{p})}).$$

(2) If $\mathfrak{p}$ is a real place (an imbedding from K to $\mathbb{R}$) in $\mathfrak{m}$. Let $\sigma_\mathfrak{p}$ be the corresponding imbedding of K into $\mathbb{R}$. Then $\sigma_\mathfrak{p}(\alpha) > 0$.

Let $K_\mathfrak{m}$ be the subset of K^* consisting of elements satisfying the above two conditions. Show that $K_\mathfrak{m}$ is a subgroup of K^* and that for any maximal ideal $\mathfrak{p}$ which divides $\mathfrak{m}$ the elements of $K_\mathfrak{m}$ are units in $(O_K)_\mathfrak{p}$.

Exercise 6 (3 Points)**.** Let L/K be an abelian extension. $\mathfrak{m}$ be a modulus on K which is divisible by all the ramified primes. Then the reciprocity law map $I(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ is surjective.

Hints. Let $H \subseteq \mathrm{Gal}(L/K)$ be the image of $I(\mathfrak{m})$, and F be the fixed field of H. If F is not k, take a non-trivial cyclic subextension (Galois extension whose Galois group is cyclic) F_0/K of F/K. Show that any $\mathfrak{p} \in I(\mathfrak{m})$ splits completely in F_0 (i.e. the ramification index $g_\mathfrak{p} = 1$ and the residue degree $f_\mathfrak{p}$=1). This contradicts to the fact (which you don't have to prove) that for any cyclic extension F_0/K of degree > 1 there are infinitely many primes in K which do not split completely F_0.

Exercise 7 (2 Points)**.** Let L/K be an abelian extension. $\mathfrak{m}$ be a modulus on K which is divisible by all the ramified primes. Let $P_\mathfrak{m}$ be the image of $K_\mathfrak{m} \subseteq K^* \to I$. We call $\mathfrak{m}$ a conductor if $P_\mathfrak{m}$ is contained in the kernel of the Artin map. Let $\mathfrak{N}(\mathfrak{m}) := \mathfrak{N}(\mathfrak{m}, L/K)$ denote the subgroup of $I(\mathfrak{m})$ consisting of all norms $N_K^L\mathfrak{U}$, where $\mathfrak{U}$ is a fractional ideal of L prime to $\mathfrak{m}$ (i.e. relatively prime to every prime ideal $\mathfrak{q}$ of L lying above some prime ideal $\mathfrak{p}|\mathfrak{m}$). Using the Universial Norm Index Inequality (which you don't have to prove):

$$(I(\mathfrak{m}) : P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})) \leq [L : K]$$

and Exercise 6, 4(3) to show that if there exists a conductor then the Artin map induces an isomorphism

$$I(\mathfrak{m})/P_\mathfrak{m}\mathfrak{N}(\mathfrak{m}) \to \mathrm{Gal}(L/K).$$

(In general, under our conditions, a conductor exists. But it takes more efforts to work out.)

Exercise 8 (3 Points)**.** Let $m \in \mathbb{N}$ and $m > 1$. Let $L = \mathbb{Q}(\xi_m)$ be the extension obtained by adjoint a primitive m-th root of unity ξ_m to $K = \mathbb{Q}$. L/K is an abelian extension, unramified away from the primes dividing m. The Galois group identifies canonically with $(\mathbb{Z}/m\mathbb{Z})^*$, by $\xi_m \mapsto \xi_m^a$ for $a \in (\mathbb{Z}/m\mathbb{Z})^*$. Let p be a prime which does not divide m.

(1) Show that $((p), L/K)$ has the effect $\xi_m \mapsto \xi_m^p$. (Hint: First from the correspondence $(\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(L/K)$, we know there is an element $\sigma \in \mathrm{Gal}(L/K)$ satisfying $\sigma(\xi_m) = \xi_m^p$. (You don't have to prove this.) You only have to show σ is a Frobenius element (Frobenius substitution). Since $O_L = \mathbb{Z}[\xi_m]$ we have $x = \sum_i a_i\xi_m^i$ for any $x \in O_L$. From this you can show that $\sigma(x) \equiv x^p \pmod p$.)

(2) Show that if $a \in \mathbb{Q}$ is any rational number prime to m (considering m as a modulus), and d be any positive integer satisfying $a \equiv d \pmod^* m$), then we have

$$((a), L/K) : \xi_m \mapsto \xi_m^d.$$

(3) Show that $((a), L/K) = 1$ if and only if $a \equiv 1 \pmod^* m$). So m is a conductor.

For questions, feel free to send emails to `l.zhang@fu-berlin.de` or come to Lei Zhang at A3 Zimmer 112A.

References

[Local Fields] Jean-Pierre Serre, Local Fields, Springer-Verlag, 1979.