L-functions and applications
4. Exercise Sheet

TECHNISCHE UNIVERSITÄT DARMSTADT

Department of Mathematics
Dr. Jolanta Marzec, Dr. Michael Neururer

SS 2019
07.06.2019

Groupwork

Exercise G1 (Prime splitting in towers of extensions)

(a) Let $K \subset L \subset M$ be extensions of number fields and $\mathfrak{p}$ a prime in $\mathcal{O}_K$. If $\mathfrak{P} \triangleleft \mathcal{O}_L$ lies above $\mathfrak{p}$ and $\mathfrak{s} \triangleleft \mathcal{O}_M$ lies above $\mathfrak{q}$

$$e_{\mathfrak{s}/\mathfrak{p}} = e_{\mathfrak{s}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} \quad \text{and} \quad f_{\mathfrak{s}/\mathfrak{p}} = f_{\mathfrak{s}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}$$

(b) Describe how 7 decomposes in $K = \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{11})$, i.e., find the ramification, inertia degree and the number of primes above 7 in K.

Exercise G2 (Prime splitting in cyclotomic fields)
The aim of this exercise is to prove the following proposition which describes splitting behaviour of primes in **cyclotomic fields**, i.e., in $\mathbb{Q}(\mu_m)$, where μ_m is a primitive m-th root of unity. The consecutive steps of the proof may be illustrated with use of SageMath.

Proposition *Let $m = \prod_p p^{\nu_p}$ be the prime factorization of m and, for every $p \in \mathbb{P}$, let f_p be the smallest positive integer such that $p^{f_p} \equiv 1 \bmod \frac{n}{p^{\nu_p}}$. Then one has in $K = \mathbb{Q}(\mu_m)$ the factorization*

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p^{\nu_p})},$$

where $\mathfrak{p}_1 \dots \mathfrak{p}_r$ are distinct prime ideals, all of degree f_p, and ϕ denotes the Euler function.

(a) Let $K = \mathbb{Q}(\mu)$, μ a primitive m-th root of unity. Assume that m is a power of some prime number p. Use a minimal polynomial of μ and its decomposition into irreducible factors over K to prove that

$$p\mathcal{O}_K = (1-\mu)^{\phi(m)}\mathcal{O}_K .$$

Use the fundamental equality (see cheatsheet II) to deduce that

$$\mathcal{O}_K/(1-\mu)\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z} .$$

SAGE: Consider cyclotomic fields for $m = 4, 27, 5$. Find their degree over $\mathbb{Q}$ and defining polynomials; factor these polynomials over $\mathbb{Q}(\mu)$; find decomposition of $p = 2, 3, 5$ in corresponding cyclotomic fields. It may be helpful to use the following code and the code from exercise G4:

```
m =
K.<zetam> = CyclotomicField(m) #zetam is a primitive m-th root of unity
zetam.minpoly() #minimal polynomial of zetam
```

(b) Under assumptions from (a), compute the discriminant of the basis $1, \mu, \dots, \mu^{\phi(m)-1}$ of $K/\mathbb{Q}$.
SAGE: Compute the discriminant of the ideal generated by the above basis for K as in (a). Use the functions `absolute_norm()` and `discriminant()`.

(c) Deduce from (a) that $\mathcal{O}_K = \mathbb{Z}[\mu] + (1-\mu)^t\mathcal{O}_K$ for any $t \geq 1$. Use this and the fact that $\operatorname{disc}(1, \mu, \dots, \mu^{\phi(m)-1})\mathcal{O}_K \subseteq \mathbb{Z}[\mu]$ to prove that $O_K = \mathbb{Z}[\mu]$.
SAGE: Verify the statement $O_K = \mathbb{Z}[\mu]$ for K as in (a).

(d) Now let m be an arbitrary positive integer. Prove that $O_K = \mathbb{Z}[\mu]$.
SAGE: Verify this statement for $K = \mathbb{Q}(\mu_m)$ with $m = 4 \cdot 9 \cdot 5$.

(e) Use Kummer-Dedekind theorem (see cheatsheet II) to prove the above Proposition.
SAGE: Factor first twenty prime numbers in $\mathcal{O}_K$ for K as in (d) to verify this statement.

Hints:
(b): Let Φ_m be the minimal polynomial of μ. Relate $\mathrm{disc}(1, \mu, \ldots, \mu^{\phi(m)-1})$ to $\Phi_m'(\mu)$. Then differentiate the equation $(X^{m/p} - 1)\Phi_m(X) = X^m - 1$ at $X = \mu$.
(d): You may use the following basic fact: Let L and L' be two Galois extensions of $\mathbb{Q}$ of degree n, resp. n', such that $L \cap L' = \mathbb{Q}$. Let $\omega_1, \ldots, \omega_n$, resp. $\omega_1', \ldots, \omega_n'$ be an integral basis of $L/\mathbb{Q}$, resp. $L'/\mathbb{Q}$, with discriminant d, resp. d'. If d and d' are coprime, then $\{\omega_i \omega_j' : i = 1, \ldots, n; j = 1, \ldots, n'\}$ is an integral basis of LL', of discriminant $d^{n'} d'^{n}$.
(e): First show that for $m = p^\nu M$, $p \nmid M$, the minimal polynomial $\Phi_m(X)$ of primitive m-th root of unity satisfies $\Phi_m(X) \equiv \Phi_M(X)^{\phi(p^\nu)}$ mod p. Then reduce to the case $p \nmid m$ and show that $\Phi_m(X)$ doesn't have multiple roots mod p as a divisor of $X^m - 1$. Observe that $\mathbb{F}_{p^{f_p}}$ is the splitting field of the polynomial Φ_m mod p.

Exercise G3
Let L/K be a Galois extension such that $\mathrm{Gal}(L/K)$ is not cyclic. Show that no prime $\mathfrak{p}$ of K is inert, i.e. $\mathfrak{p}\mathcal{O}_L$ is never a prime ideal in L.

Hint: Show that if p is inert, the decomposition group of p, $\mathrm{Gal}(L/K)$, is isomorphic to the Galois group of a finite field extension. These are all cyclic.

Exercise G4 (A cubic extension)
Let $L = \mathbb{Q}(\alpha)$ be the cubic extension of $\mathbb{Q}$ generated by α with minimal polynomial $P(X) = X^3 - X - 1$. In this exercise you should use SageMath to help with the calculations. Here is a code snipped to get you started.

```
Pol.<x> = PolynomialRing(ZZ) #Defines a polynomial ring
P = x^3-x-1
L.<a> = NumberField(P) #Defines the number field generated by a root of P
OL = L.ring_of_integers()
OL.basis()
L.disc()
L.factor(5) #Gives the prime factorisation of (5) in L
P.factor_mod(5) #Factors P modulo 5. This is closely connected to L.factor(5).
```

(a) Let H be the splitting field of P and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of P in $\mathbb{C}$. Show that $\sqrt{\mathrm{disc}(L)} \in H$ and conclude that L is not a Galois extension of $\mathbb{Q}$.

(b) Show that a prime p can split in L in the following ways:

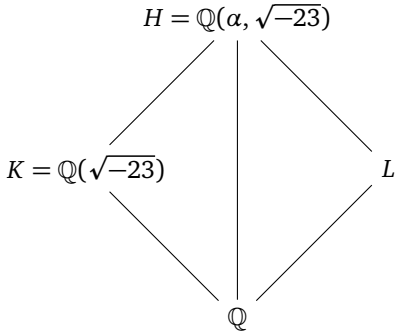
$$p\mathcal{O}_L = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 & \text{with } e_{\mathfrak{p}_i/p} = f_{\mathfrak{p}_i/p} = 1, \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{with } e_{\mathfrak{p}_i/p} = f_{\mathfrak{p}_1/p} = 1,\ f_{\mathfrak{p}_2/p} = 2, \\ \mathfrak{p} & \text{with } e_{\mathfrak{p}/p} = 1,\ f_{\mathfrak{p}/p} = 3 \\ \mathfrak{p}_1\mathfrak{p}_2^2, & \text{if } p = 23, \text{with } e_{\mathfrak{p}_1/p} = f_{\mathfrak{p}_i/p} = 1, e_{\mathfrak{p}_2/p} = 2. \end{cases}$$

Find examples for all of these cases. Consider the Euler product

$$\zeta_L(s) = \prod_p \zeta_{L,p}(s),$$

and write down what $\zeta_{L,p}(s)$ is, depending on the splitting behaviour of p. Show that $L(s) = \zeta_L(s)\zeta(s)^{-1}$ is meromorphic on $\mathbb{C}$ and holomorphic in $\mathrm{Re}\, s \geq 1$ and write down an Euler product of this L-function.

(c) Consider the following diagram of extensions:



Which of the extensions you see are Galois? Write down the corresponding Galois groups.

(d) Show that p is inert in K, i.e., $p\mathcal{O}_K$ is a prime ideal, if and only if $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$.

(e) Show that

$$\zeta_H(s) = L(s)^2\zeta_K(s),$$

by comparing local Euler factors.

☠ Show that $L(s)$ extends to a holomorphic function on $\mathbb{C}$ or, in other words, every zero of $\zeta(s)$ is also a zero of $\zeta_L(s)$.