Humboldt-Universität zu Berlin
Institut für Mathematik
Dr. D. Agostini, M. Sc. L. Lerer
L. Mädje

Zahlentheorie

SoSe 2019

Exercise Sheet 11

These exercises will not be corrected, but some of them will be discussed in class.

This exercise lists some essential concepts that you *must* know in order to pass the course.

Exercise 11.1

a) Let K be a field and $K \subset L$ a field extension. Define the trace $Tr_{L/K} : L \to K$ and the norm $N_{L/K} : L^\times \to K^\times$.

b) Write one possible definition of discrete valuation ring.

c) Write one possible definition of Dedekind domain.

d) Write the definition of prime element and irreducible element in a ring.

e) Let K be a number field, L a finite extension of K, $\mathfrak{P} \subset \mathcal{O}_L$ a nonzero prime ideal and $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ the prime ideal lying under $\mathfrak{P}$. Write the definition of ramification index $e(\mathfrak{P}|\mathfrak{p})$ and of inertia degree $f(\mathfrak{P}|\mathfrak{p})$.

f) Write the definition of fractional ideal.

g) Let K be a number field and $I, J \subset K$ be fractional ideals. Write the definition of $I \cdot J$ and prove that it is again a fractional ideal.

This exercise is a collection of small tasks that you should be able to answer in order to successfully pass the exam.

Exercise 11.2

a) Let $m > 0$ be an integer. Is it true that there are only finitely many algebraic integers α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq m$? Prove it or give a counterexample.

b) List all the ideals of $\mathbb{Z}[\sqrt{-7}]$ containing 10.

c) Let K be a number field and $M > 0$ an integer. Is it true that there are only finitely many $\alpha \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha)| < M$? Prove it or give a counterexample.

d) Let $R \subset S$ be two principal ideal domains and let $a, b \in R$. Show that $\gcd_R(a, b) = 1$ if and only if $\gcd_S(a, b) = 1$.

e) Prove that $\mathbb{Z}[\sqrt{-10}]$ is not a UFD.

f) Let p be a prime number and ζ_p a primitive p-th root of unity. Compute $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p)$.

Many of the next exercises are somehow longer and harder than those that will appear in the exam, but because of this, they are an even better preparation. Note that when trying to solve a particular point, you can assume the validity of the previous ones, even if you did not solve them.

Exercise 11.3 In this exercise we conclude the proof of the first case of Fermat's Last Theorem for regular primes. So, let $p > 5$ be a regular prime number, $K = \mathbb{Q}(\zeta_p)$ the corresponding cyclotomic field and $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Suppose that there is a solution to the equation

$$X^p + Y^p = Z^p$$

such that $p \nmid XYZ$. Then, we have proven in class that in the ring $\mathcal{O}_K$ we have

$$X + \zeta_p Y = (-\zeta_p)^m \cdot v \cdot \alpha^p$$

for certain $m \in \mathbb{Z}$,$v \in U_{K^+}$ and $\alpha \in \mathcal{O}_K$. We want to derive a contradiction.

a) Let $\beta = b_0 + b_1\zeta_p + \cdots + b_{p-1}\zeta_p^{p-1}$ with $b_i \in \mathbb{Z}$ and at least one $b_i = 0$. Let also $n \in \mathbb{Z}$. Show that if $\beta \equiv 0 \mod n\mathcal{O}_K$ then $b_i \equiv 0 \mod n\mathcal{O}_K$ for each i.

b) Show that there is $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \mod p\mathcal{O}_K$.

c) Show that $X + \zeta Y \equiv (-\zeta)^m va \mod p\mathcal{O}_K$ and $X + \overline{\zeta} Y \equiv (-\zeta)^{-m} va \mod p\mathcal{O}_K$. Conclude that $X + \zeta Y - \zeta^{2m} X - \zeta^{2m-1} Y \equiv 0 \mod p\mathcal{O}_K$.

d) Use point (a) to get a contradiction.

Exercise 11.4 Let $K = \mathbb{Q}(\alpha)$ be a number field with α integral and let $n = [K : \mathbb{Q}]$.

a) Let $d = \mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Prove that $d\mathcal{O}_K \subseteq \mathbb{Z}[\alpha]$.

Now consider the polynomial $f(X) = X^3 - 3X + 1$.

b) Show that $f(X)$ is irreducible over $\mathbb{Q}$ with three real roots.

c) Let α be any root of $f(X)$ and $K = \mathbb{Q}(\alpha)$. Prove that the ideal $(\alpha + 1)$ is prime in $\mathcal{O}_K$ and conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha] + (\alpha + 1)\mathcal{O}_K$. [*Hint*: for the second assertion, it is enough to prove that the natural map $\mathbb{Z}[\alpha] \to \mathcal{O}_K/(\alpha + 1)$ is surjective].

d) Show that $3^4 \cdot \mathcal{O}_K \subseteq \mathbb{Z}[\alpha]$.

e) Show that $(\alpha + 1)^3 = 3\alpha(\alpha + 2)$ and that $\alpha, \alpha + 2 \in U_K$. Conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. [*Hint*: multiply the relation $\mathcal{O}_K = \mathbb{Z}[\alpha] + (\alpha + 1)\mathcal{O}_K$ by $\alpha + 1$ on both sides].

f) Show that $\mathcal{O}_K$ is an UFD.

Exercise 11.5 Let K^+ be a totally real number field: this means that every embedding $K^+ \hookrightarrow \mathbb{C}$ is a real embedding. Let also $K \supseteq K^+$ be a finite extension such that $[K^+ : K] = 2$ and K^+ is totally imaginary. This means that every embedding $K \hookrightarrow \mathbb{C}$ is nonreal.

a) Let U_{K^+} and U_K be the two groups of units. Show that they have the same rank as $\mathbb{Z}$-modules.

b) Show that the conjugation $z \mapsto \overline{z}$ induces an automorphism $K \to K$ that fixes K^+. Show also that this is the unique nontrivial automorphism of K that fixes K^+. Furthermore, prove that for every embedding $\sigma\colon K \hookrightarrow \mathbb{C}$ we have $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}$. Conclude that if $u \in U_K$, then $\frac{\overline{u}}{u} \in \mu_K$.

c) Consider the map

$$\phi\colon U_K \longrightarrow \mu_K/\mu_K^2 \qquad u \mapsto \text{class of } \frac{\overline{u}}{u}$$

Show that ϕ is an homomorphism of groups and compute its kernel.

d) Prove that the quotient $\frac{U_K}{\mu_K \cdot U_{K^+}}$ has cardinality one or two.

e) Give a concrete example of K^+, K and compute the cardinality $\frac{U_K}{\mu_K \cdot U_{K^+}}$ for the example you have chosen.

Exercise 11.6 Consider the equation $Y^2 = X^3 - 51$. We will prove that this has no integer solutions; this is a particularly interesting example, since it turns out that this equation has a solution modulo each prime $p \in \mathbb{Z}$.

a) Let $K = \mathbb{Q}(\sqrt{-51})$. Show that there are no elements of norm 3 in $\mathcal{O}_K$.

b) Prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

c) Suppose that there is an integer solution to $Y^2 = X^3 - 51$. Working modulo 8, prove that X must be odd. Show also that Y and 51 must be coprime in $\mathbb{Z}$.

d) Rewrite the equation as $X^3 = (Y + \sqrt{-51})(Y - \sqrt{-51})$ in $\mathcal{O}_K$. Show that if $Y + \sqrt{-51}$ and $Y - \sqrt{-51}$ have a common prime ideal factor $\mathfrak{p}$, then either $\mathfrak{p} = 2\mathcal{O}_K$ or $\mathfrak{p} \supseteq (Y, \sqrt{-51})$. Conclude that $Y + \sqrt{-51}$ and $Y - \sqrt{-51}$ are coprime in $\mathcal{O}_K$.

e) Prove that there is an ideal $I \subseteq \mathcal{O}_K$ such that $(Y + \sqrt{-51}) = I^3$. Conclude that I is principal, so that there is an element $\beta \in \mathcal{O}_K$ such that $(Y + \sqrt{-51}) = (\beta^3)$.

f) Show that $Y + \sqrt{-51} = \pm\beta^3$. Hence, if $\alpha = \frac{1+\sqrt{-51}}{2}$ there are $r, s \in \mathbb{Z}$ such that

$$(Y - 1) + 2\alpha = Y + \sqrt{-51} = (r + s\alpha)^3$$

Derive a contradiction.

Exercise 11.7 Consider the ring $A = \mathbb{Z}\left[\frac{1}{2}\right]$.

a) Find a multiplicatively closed subset $S \subseteq \mathbb{Z}$ such that $A = S^{-1}\mathbb{Z}$.

b) Find all prime ideals $\mathfrak{p} \subseteq A$ and describe the localizations $A_\mathfrak{p}$.

c) Is A a Dedekind domain? Give a proof of your answer.

Exercise 11.8 Consider the number field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$.

a) Prove that $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-6})$ are all the quadratic fields contained in K.

b) Let F be one of the fields in (a). Prove that if $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{K/F}(\alpha) \in \mathcal{O}_F$. Deduce that every $\alpha \in \mathcal{O}_K$ can be written as

$$\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{-3} + \frac{c}{2}\sqrt{2} + \frac{d}{2}\sqrt{-6}. \qquad \text{with } a, b, c, d \in \mathbb{Z}$$

c) Let F be one of the fields in (a). Prove that if $\alpha \in \mathcal{O}_K$ then $N_{K/F}(\alpha) \in \mathcal{O}_F$. Deduce that in the expression before we have $a \equiv b \mod 2$ and $c \equiv d \mod 2$. Hence, an integral basis of $\mathcal{O}_K$ is

$$1, \frac{1 + \sqrt{-3}}{2}, \sqrt{2}, \frac{\sqrt{2} + \sqrt{-6}}{2}.$$

d) Show that the discriminant of K is $\Delta_K = 16 \cdot 3 \cdot 2 \cdot 6$.

e) Prove that $\mathcal{O}_K = \mathcal{O}_{\mathbb{Q}(\sqrt{2})}[\frac{1+\sqrt{-3}}{2}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}[\sqrt{2}]$. Deduce that in $\mathcal{O}_K$ we have the prime factorizations

$$2\mathcal{O}_K = (\sqrt{2}\mathcal{O}_K)^2, \qquad 3\mathcal{O}_K = (\sqrt{3}\mathcal{O}_K)^2$$

[*Hint*: you can factor 2 and 3 first in $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}, \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ and then in $\mathcal{O}_K$.]

f) Show that $\mathcal{O}_K$ is an UFD.