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

Zahlentheorie

SoSe 2019

Exercise Sheet 1

If you want your solutions to be corrected, you should hand them in by Wednesday, April 24.
Please write your name and immatriculation number on top of every exercise

---

Exercise 1.1 (2+8 points)

a) Let A be a ring (all rings in the course will be commutative and with unity). Write down the definition of an irreducible element and of a prime element in A.

b) Let $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers that we have seen in the lectures. Show that an element $\alpha \in \mathbb{Z}[i]$ is irreducible if and only if:

- $\alpha = u \cdot p$, where $u \in \{\pm 1, \pm i\}$ and $p \in \mathbb{Z}$ is a prime number such that $p \equiv 3 \mod 4$.
- $\alpha = a + bi$, where $a^2 + b^2 \in \mathbb{Z}$ is a prime number.

Exercise 1.2 (1+3+1+5 points) We have proved in the lectures that the ring $\mathbb{Z}[i]$ is an UFD. In this exercise we will show that this is not true for every finite extension of $\mathbb{Z}$.

a) Prove that $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

b) Consider the norm map $N \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ defined by $N(a+b\sqrt{-5}) = a^2 + 5b^2$. Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for every $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.Write down all the invertible elements of $\mathbb{Z}[\sqrt{-5}]$.

c) Prove that there is no element $\alpha \in \mathbb{Z}[\sqrt{-5}]$ of norm 2 or 3.

d) Show that the element 6 has two distinct factorizations into irreducibles by conside-ring $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Exercise 1.3 (2+2+2+4 points) Consider the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

a) Show that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois and compute its Galois closure $L/\mathbb{Q}$ and the degree $[L : \mathbb{Q}]$.

b) Show that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_3$, the group of permutations of 3 elements.

c) Find an element α such that $L = \mathbb{Q}(\alpha)$.

d) Give an explicit description of the action of $\mathrm{Gal}(L/\mathbb{Q})$ on L.

Exercise 1.4 (5+5 points)

a) Let A be a ring (e..g. $A = \mathbb{Z}$) and $\mathfrak{p} \subseteq A$ a prime ideal (e.g. $\mathfrak{p} = p\mathbb{Z}$). Let also $f(x) \in A[x]$ be a polynomial that factorizes as $f(x) = g(x)h(x)$. Prove that if $f(x)$ has all coefficients in $\mathfrak{p}$, then the same is true for $g(x)$ or $h(x)$. [*Hint*: consider the homomorphism $A[x] \to (A/\mathfrak{p})[x]$].

b) Let A be an UFD (e.g. $A = \mathbb{Z}$) and let $K = \mathrm{Frac}\, A$ be its fraction field (e.g. $K = \mathbb{Q}$). Let $f(x) \in A[x]$ be a monic polynomial that factorizes as $f(x) = g(x)h(x)$ with $g(x), f(x) \in K[x]$ monic. Prove that $g(x), h(x)$ have coefficients in A as well.