Universität Wien
Prof. Dr. D. Burde

Algebraic number theory
— Exercises —

Exercises WS 2021

Exercise 1. Consider the polynomial $f = X^4 - X^2 + 1$. Show that f is irreducible in $\mathbb{Z}[X]$, but reducible in $R[X]$, where $R = \mathbb{Z}[i]$ is the ring of Gaussian integers.

Exercise 2. Decide for each of the following numbers whether or not it is integral over $\mathbb{Z}$.

(a) $i + \sqrt{2}$.

(b) $\zeta(2) = \frac{\pi^2}{6}$.

(c) $e^{2\pi i/3} + 2$.

(d) $\sqrt{17} + \sqrt{19}$.

Exercise 3. Determine each of the following quotient rings

$$R_1 = \mathbb{Z}[i]/(2),\ R_2 = \mathbb{Z}[i]/(3),\ R_3 = \mathbb{Z}[i]/(13),$$

and decide, whether or not they are a field, or a product of two fields, or none of it.

Exercise 4. Let $K = \mathbb{Q}(\sqrt{-19})$ and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ its ring of integers. Decide whether or not

$$35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{19})$$

contradicts the unique factorization property for the ring $\mathcal{O}_K$.

Exercise 5. Decide for each ring below, whether it is integrally closed or not and justify your decision.

$$\mathbb{Z}[\sqrt{-3}],\ \mathbb{Z}[\sqrt{3}],\ \mathbb{Z}[\sqrt{2}+\sqrt{3}],\ \mathbb{Z}[\sqrt{2},\sqrt{3}].$$

Exercise 6. Let d be a squarefree integer. Show that the ring $\mathbb{Z}[\sqrt{d}]$ has Krull dimension 1, but need not be a PID. Indeed, show that all rings $\mathbb{Z}[\sqrt{d}]$ for squarefree $d \le -3$ are not UFD's and hence not PID's.

Exercise 7 - extra. Determine all integer solutions of the Diophantine equation $y^2 = x^3 - 4$ by using properties of the ring $\mathbb{Z}[i]$.

Exercise 8. Let $\overline{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. Determine the Krull dimension of $\overline{\mathbb{Z}}$ and show that $\overline{\mathbb{Z}}$ is not a PID. Show that $\overline{\mathbb{Z}}$ has no irreducible elements and decide which of the elements $\frac{-1+\sqrt{3}}{2}$, $\frac{-1+\sqrt{-3}}{2}$ is in $\overline{\mathbb{Z}}$.

Exercise 9. Let $\alpha = \sqrt[3]{2}$ and $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha)$. Compute the trace $\mathrm{tr}_{L/K}(z)$ and the norm $N_{L/K}(z)$ of an arbitrary element $z = a + b\alpha + c\alpha^2$ in L. Find an integral basis $\{1, \xi_1, \xi_2\}$ of $\mathcal{O}_L$ over $\mathbb{Z}$ (without proof) and compute the discriminant $D(1, \xi_1, \xi_2)$ in at least two different ways.

Exercise 10. Let A be a Dedekind domain and I a nonzero ideal of A. Show that A/I is a product of principal ideal rings and I can be generated as an ideal by two elements.

Exercise 11. Let $R = \mathbb{Z}[\sqrt{-3}]$ and let I be a nonzero ideal of R. Define its norm by $N(I) = \#(R/I)$. Show that this norm is finite, but not multiplicative.

Exercise 12. Consider the following ideals in $\mathbb{Z}[\sqrt{-3}]$,

$$P_1 = (2), P_2 = (3), P_3 = (5), P_4 = (1+\sqrt{-3}), P_5 = (2, 1+\sqrt{-3}).$$

Which of these ideals is a prime ideal? Conclude that the unique decomposition into prime ideals does not hold in $\mathbb{Z}[\sqrt{-3}]$, and that the ideal (2) has no decomposition into prime ideals.

Exercise 13. Let A be a Dedekind domain and let I and I' be nonzero ideals. Then there exists an ideal J coprime to I' such that IJ is principal.

Exercise 14- extra. Find without proof the imaginary quadratic number fields $\mathbb{Q}(\sqrt{-d})$ with minimal squarefree $d > 0$ having class group $\mathbb{Z}/n$ for each $1 \leq n \leq 9$. Can you find a prime $p \geq 3$ such that $(\mathbb{Z}/p)^3$ is the class group of an imaginary quadratic number field? What about $p = 2$? Determine without proof all finite abelian groups of order $n \leq 100$, which do not arise as the class group of an imaginary quadratic number field.

Exercise 15. Let $A = (a_{ij}) \in M_n(\mathbb{R})$ and

$$L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} a_{ij} x_j$$

be real linear forms for $1 \leq i \leq n$ with $\det(A) \neq 0$. Let $c_1, \ldots, c_n$ be positive real numbers with $c_1 \cdots c_n > |\det(A)|$. Show that there exists integers $m_1, \ldots, m_n$, not all zero, such that $|L_i(m_1, \ldots, m_n)| < c_i$ for all $1 \leq i \leq n$.

Exercise 16. Let $G = \mathbb{R} \cdot (1, \alpha)$ be a line in the plane $\mathbb{R}^2$ with irrational slope $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Use Exercise 15 to show that for any $\varepsilon > 0$ there are infinitely many lattice points $P \in \mathbb{Z}^2$ with distance $d(P, G) < \varepsilon$.

Exercise 17. Determine all quadratic number fields $\mathbb{Q}(\sqrt{d})$ with a squarefree integer d, such that the Minkowski bound is less than 2, and compute this bound explicitly in these cases. Give an example of a number field K with class number 1, but Minkowski bound $B_K > 2$.

Exercise 18. Determine all groups G which can arise as the group of roots of unity μ_K for a quartic number field K, i.e., with $[K : \mathbb{Q}] = 4$. Give an example of such a field K having the given unit group in each case.

Exercise 19. Let K be a number field of degree n with $\mathcal{O}_K^\times \cong \mathbb{Z} \times \mu_K$. Determine all possible degrees $n \geq 1$ and the group μ_K in all cases.

Exercise 20. Let $K/\mathbb{Q}$ be a cubic extension which is not Galois, with negative discriminant d. So it has only one real embedding. View K this way as a subfield of $\mathbb{R}$. Let $\varepsilon > 1$ be a fundamental unit of K. Show that

$$\frac{|d|}{4} < \varepsilon^3 + 7.$$

Exercise 21- extra. Let K be a cubic number field with exactly one real embedding. Use Hadamard's inequality to show that for any unit $u \in \mathcal{O}_K^\times$ with $u > 1$ we have

$$|D(1, u, u^2)| \leq 3\left(u^2 + \frac{2}{u}\right)\left(u^4 + \frac{2}{u^2}\right).$$

Compare this with the estimate $|D(1, u, u^2)| < 4(u^3 + \frac{1}{u^3} + 6) < 4(u^3 + 7)$ from Exercise 20.

Exercise 22. Show that $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a fundamental unit of $\mathcal{O}_K^\times$ for the number field $K = \mathbb{Q}(\sqrt[3]{2})$.

Exercise 23. Let $K = \mathbb{Q}(\sqrt{21})$. Show that $u = 55 + 12\sqrt{21}$ is a unit in $\mathcal{O}_K^\times$, but not a fundamental unit.

Exercise 24. Compute the class number of $\mathbb{Q}(\sqrt{-5})$ by using the analytic class number formula and the fact that $L(1, \chi)$, for an imaginary quadratic number field K with discriminant d_K and quadratic character $\chi(n) = (d_K/n)$, can be computed by

$$L(1, \chi) = -\frac{\pi}{|d_k|^{3/2}} \sum_{r=1}^{|d_k|-1} \chi(r)r.$$

Exercise 25. Give an example of number fields K and L and a prime number p such that p is inert in $K/\mathbb{Q}$ and $L/\mathbb{Q}$, but not in the compositum $KL/\mathbb{Q}$.

Exercise 26. Let $K \subseteq E \subseteq L$ be a tower of number field extensions with intermediate field E. Let $\mathcal{O}_K, \mathcal{O}_E, \mathcal{O}_L$ be the corresponding rings of integers and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Show that if $\mathfrak{p}$ splits completely in L, then $\mathfrak{p}$ also splits completely in E.

Exercise 27. Let p be a prime not dividing n, $K = \mathbb{Q}(\zeta_n)$ and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ lying over p. Show that the residual degree $f = f(\mathfrak{p}, p)$ is exactly the order of the element $p \in (\mathbb{Z}/n)^\times$. In particular, p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \bmod n$.

Exercise 28 - Extra. Let $K = \mathbb{Q}(\zeta_7)$ and $F \subseteq K$ be the unique subfield with $[F : \mathbb{Q}] = 3$. Describe which rational primes p are ramified, split or inert in $F/\mathbb{Q}$ in terms of congruences of p modulo 7.

Exercise 29. Let p be an odd prime and $L = \mathbb{Q}(\zeta_p)$. Show that the discriminant of L is given by

$$d_L = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

Use the result that $d_K \mid d_L$ for a tower of number fields $\mathbb{Q} \subseteq K \subseteq L$, to show that L contains a unique quadratic extension of $\mathbb{Q}$, namely

$$K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right).$$

Exercise 30. Show that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension. Find a Galois extension of $\mathbb{Q}$ with non-abelian Galois group and conclude that it is not contained in a cyclotomic extension.

Exercise 31. Show that the equation $x^2 = 2$ has two solutions in $\mathbb{Z}_7$, the ring of 7-adic integers, and compute its first ten 7-adic digits.

Exercise 32. Let p be a prime number and a an integer coprime to p. Show that the sequence $a_n = a^{p^n}$ converges in $\mathbb{Q}_p$ and determine its limit.

Exercise 33. Let p be an odd prime. Show that $\mathbb{Q}_p$ has no p-th root of unity other than 1, and that $\mathbb{Q}_2$ has no 4-th roots of unity other than ± 1.

Exercise 34. Show that the p-adic fields $\mathbb{Q}_p$ are pairwise non-isomorphic for different primes $p \in \mathbb{P}$ and $p = \infty$ by considering roots of unity in these fields.

Exercise 35 - Extra. Let $\mathbb{Z}[[X]]$ denote the ring of formal power series in one variable. Show that there is a ring isomorphism $\mathbb{Z}[[X]]/(X-p) \cong \mathbb{Z}_p$.

Exercise 36. Show that the p-adic series $\sum_{n=1}^{\infty} n \cdot n!$ and $\sum_{n=1}^{\infty} n^2 \cdot (n+1)!$ converge in $\mathbb{Q}_p$ with

$$\sum_{n=1}^{\infty} n \cdot n! = -1,$$

$$\sum_{n=1}^{\infty} n^2 \cdot (n+1)! = 2,$$

whereas $\sum_{n=1}^{\infty} \frac{1}{n!}$ diverges in $\mathbb{Q}_p$.

Exercise 37. Let K be a field that is complete with respect to a non-trivial absolute value $|\cdot|$. Show that K is uncountable.

Exercise 38. Show that the equation $x^2 - 82y^2 = 2$ has solutions in $\mathbb{Z}_p$ for every prime p, and but has no solutions in $\mathbb{Z}$.

Due: January 31, 2022