Universität Tübingen
Fachbereich Mathematik
D. Agostini, K. Heesterbeek,
C. Nollau

Algebraic Number Theory
SS 2026

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

Sheet 2

If you want your solutions to be corrected, upload them on URM by the end of May 4.
Write your name and matriculation number on each sheet. If you upload the exercises as a group, only one person can do it instead of the whole group.
The exercises marked with $*$ might be more complicated or involved than the others.

Exercise 2.1

(i) (Eisenstein's criterion) Let R be an UFD, $F = \operatorname{Frac} R$ its fraction field and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ be such that there is a prime element $p \in R$ with $p \mid a_0, \ldots, a_{n-1}, p^2 \nmid a_0$. Prove that $f(x)$ is irreducible in $R[x]$, and then also in $F[x]$ by Gauss' lemma.

(ii) Let $p \in \mathbf{Z}_{>0}$ be a prime number. The p-th cyclotomic polynomial is defined as

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

Prove that $\Phi_p(x)$ is irreducible in $\mathbf{Q}[x]$

(iii) Let $\zeta_p = e^{2\pi i/p} \in \mathbf{C}$. The p-th cyclotomic field is $\mathbf{Q}(\zeta_p)$. Show that this is a number field and compute the degree $[\mathbf{Q}(\zeta_p) : \mathbf{Q}]$. Find also all embeddings $\sigma\colon \mathbf{Q}(\zeta_p) \hookrightarrow \mathbf{C}$

(iv) Find the minimal polynomial over $\mathbf{Q}$ of $\zeta_5 + \zeta_5^{-1}$.

Exercise 2.2 Which of the following statements hold? Prove them if they are true, and give a counterexample if they are false.

(i) Let R be a ring and consider the free R-module $R^{\oplus n}$. Then any finite set of generators of $R^{\oplus n}$ contains a basis as a subset.

(ii) Let R be a ring and consider the free R-module $R^{\oplus n}$. Then any linearly independent set of $R^{\oplus n}$ can be extended to a basis.

(iii) Let R be a domain, $F = \operatorname{Frac} R$ its field of fractions, and $A \in R^{m\times n}$ a matrix. Then $L_A\colon R^{\oplus n} \to R^{\oplus m}$ is surjective if and only if $L_A^{(F)}\colon F^{\oplus n} \to F^{\oplus m}$ is surjective.

(iv) Let $d, e \in \mathbf{Z}$ be two square-free integers. Then $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{e})$ if and only if $d = e$.

(v) Let $F \subseteq K$ be number fields, $\alpha \in K^\times$ a non-zero element and $m_{F,\alpha} = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$ the minimal polynomial of α over F. Then $a_0 \neq 0$.

(vi) The ring $\mathbf{Z}[\sqrt{2}]$ has infinitely many invertible elements.

(vii) If $n \in \mathbf{Z}_{>0}$, the real numbers $\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n})$ are integral over $\mathbf{Z}$.

(viii) If $n \in \mathbf{Z}_{>0}$, the real numbers $2\cos(\frac{2\pi}{n}), 2\sin(\frac{2\pi}{n})$ are integral over $\mathbf{Z}$.

(ix) If $\alpha \in \mathbf{C}$ is algebraic over $\mathbf{Q}$, then the complex conjugate $\overline{\alpha}$ is also algebraic over $\mathbf{Q}$ with the same minimal polynomial as α.