Prof. Dr. Fabien Morel

Dr. Andrei Lavrenov, Oliver Hendrichs, Katharina Novikov

Sommersemester 2025

2. Juni 2025

Lineare Algebra II – Tutoriumsblatt 6

Aufgabe 1.

1. Recall that for a finite abelian group $(A, +)$ one defines the *order* of an element $a \in A$ as $\operatorname{ord}(a) := \min\{k \in \mathbb{N} \mid ka = 0\}$. Prove that for $n \in \mathbb{N}$ one has $na = 0 \Leftrightarrow \operatorname{ord}(a) \mid n$.
2. Recall that for a finite abelian group $(A, +)$ one defines the *order* of A as its cardinality $|A|$. For $a \in A$ prove that $\operatorname{ord}(a)$ coincides with the order of the group $\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$.
3. For a finite abelian group $(A, +)$ of order n and $a \in A$ prove that $na = 0$.
   Hint: Prove that $+a\colon A \to A$ is a bijection and consider a sum of all elements in A.
4. For a finite abelian group $(A, +)$ one defines the *exponent* of A as $\exp(A) := \min\{k \in \mathbb{N} \mid \forall\, a \in A \;\; ka = 0\}$. Prove that $\exp(A)$ divides the order of A.

Aufgabe 2.

1. (Fermat's Little Theorem) For a prime p and $a \not\equiv 0 \mod p$, prove that $a^{p-1} \equiv 1 \mod p$.
2. (Euler's Theorem) For $n \in \mathbb{N}$ define *Euler's totient function* $\varphi(n) := |\{1 \leq k \leq n \mid \text{g.c.d.}(k, n) = 1\}|$. For an integer a coprime to n prove that $a^{\varphi(n)} \equiv 1 \mod n$.

Aufgabe 3.
Let A, B be finite abelian groups, and $C := A \times B$.

1. For $(a, b) \in C$ prove that $\operatorname{ord}(a, b) = \text{l.c.r.}\big(\operatorname{ord}(a), \operatorname{ord}(b)\big)$.
2. Prove that $|C| = |A| \cdot |B|$ and $\exp(C) = \text{l.c.r.}\big(\exp(A), \exp(B)\big)$.

Remark: compare with Aufgabe 2 from Tutoriumsblatt 4.

Aufgabe 4.

1. For a finite abelian group $(A, +)$ prove that $\exp(A) = \text{l.c.r.}\{\operatorname{ord}(a) \mid a \in A\}$.
2. Recall that for a finite dimensional vector space V over a field K with an endomorphism $f\colon V \to V$, and $v \in V$ one defines $\langle v \rangle_f = \langle v, f(v), f^2(v), \ldots \rangle =: U$ and $\mu_v := \mu_{f|_U}$. Prove that $\mu_f = \text{l.c.r.}\{\mu_v \mid v \in V\}$.