

1. (a) (10 pts) For a finite abelian group $G = \{a_1, \dots, a_s\}$, define its exponent by $\exp(G) := \text{lcm}(\text{ord}(a_1), \dots, \text{ord}(a_s))$. Show that G is cyclic if and only if $\exp(G) = |G|$.
- (b) (10 pts) Let K be a field. Show that any finite subgroup of the multiplicative group K^* is cyclic.

2. (a) (10 pts) For an integer $x \in \mathbb{Z}$ and an odd prime p , define the Legendre symbol by

$$\left(\frac{x}{p}\right) := \begin{cases} 1 & \text{if } x \text{ is a square mod } p \\ -1 & \text{if } x \text{ is not a square mod } p. \end{cases}$$

Prove that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

- (b) (10 pts) Determine all integers that are prime in the ring $\mathbb{Z}[i]$ of Gaussian integers.
3. Consider the ring $R := \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \mid a, b \in \mathbb{Z}\}$.

- (a) (10 pts) Consider the norm function $N : R \rightarrow \mathbb{Z}$ defined by $N(a + i\sqrt{5}b) = a^2 + 5b^2$. Show that N is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$. Use this to find all units of R .
- (b) (10 pts) Show that $6 = 2 \cdot 3$ and $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ give two different irreducible factorizations of 6. Is R a UFD? Is R a PID?

4. (15 pts) Consider the submodule M of \mathbb{Z}^2 generated by three vectors $\begin{pmatrix} 6 \\ 4 \end{pmatrix}$, $\begin{pmatrix} 2 \\ 5 \end{pmatrix}$ and $\begin{pmatrix} -2 \\ -3 \end{pmatrix}$. Show that M is a free \mathbb{Z} -module by computing a free basis of M .

5. (a) (10 pts) Let p be an arbitrary given prime. Give an example of a nonabelian group G of order p^3 .
- (b) (5 pts) For the group G constructed above, compute its center Z_G and order $|Z_G|$.

6. (10 pts) Show that the order of a finite field is a power of a prime.