Dr. Andrey Soldatenkov
Jan Hesmert

Humboldt Universität zu Berlin
Summer term 2020

# Algebraic Number Theory

## Warm-up exercise sheet

---

The following exercises are to be discussed at the first exercise session on the 22nd of April. They should only serve as a reminder of some basic notions from the algebra course. This exercise sheet will not be graded, and you should not submit solutions.

---

**Reminder: abelian groups.** Recall that an abelian group is the same thing as a $\mathbb{Z}$-module. An abelian group $A$ is called *free* if $A \simeq \mathbb{Z}^{\oplus I}$ for some set of indices $I$. The group $A$ is a *torsion group* if for any $a \in A$ there exists a non-zero $x \in \mathbb{Z}$ such that $xa = 0$. The group $A$ is *finitely generated* if there exists a surjective homomorphism $\mathbb{Z}^n \twoheadrightarrow A$ for some $n \geqslant 0$. If one can find such a surjection with $n = 1$, then $A$ is called a *cyclic group*.

Recall the structure theorem for finitely generated abelian groups: for any such group $A$ there exist unique integers $n \geqslant 0$, $m \geqslant 0$, $d_1, \ldots, d_m \geqslant 2$ such that $d_1 \mid d_2 \mid \cdots \mid d_m$ and

$$A \simeq \mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}. \tag{1}$$

**Exercise 0.1.** Prove that an abelian group $A$ is finitely generated if and only if there exist finitely many elements $a_1, \ldots, a_m \in A$ such that any $b \in A$ can be expressed as $b = n_1a_1 + \ldots + n_ma_m$ for some $n_i \in \mathbb{Z}$. Is the additive group of rational numbers $\mathbb{Q}$ finitely generated? Is it free? Same questions about the multiplicative group $\mathbb{Q}^\times_{>0}$ of positive rational numbers.

**Exercise 0.2.** For $A$ as in (1), express in terms of $m$, $n$, $d_1, \ldots, d_m$ when $A$ is free, cyclic or torsion.

**Exercise 0.3.** Is it true that a subgroup/quotient of a finitely generated free abelian group is free? That a subgroup/quotient of a torsion group is torsion? That a subgroup/quotient of a cyclic group is cyclic?

**Exercise 0.4.** For an abelian group $A$ define its *annihilator* as

$$\mathrm{Ann}(A) = \{x \in \mathbb{Z} \mid \forall a \in A \;\; xa = 0\}.$$

Prove that $\mathrm{Ann}(A)$ is an ideal in $\mathbb{Z}$. For $A$ as in (1), express $\mathrm{Ann}(A)$ in terms of $m$, $n$, $d_1, \ldots, d_m$.

**Exercise 0.5.** Given a positive integer $n$, let $n = \prod_{i=1}^N p_i^{\nu_i}$ be its prime decomposition. Recall that $\mathbb{Z}/n\mathbb{Z}$ carries the structure of a commutative ring and prove that there exists a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^N \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}.$$

**Exercise 0.6.** Let $R$ be a commutative ring. Recall that an element $x \in R$ is called a *unit* if it has a multiplicative inverse in $R$. The units form an abelian group denoted by $R^\times$, the group operation being multiplication. Find the number of elements in $\mathbb{Z}/n\mathbb{Z}^\times$. This number is usually denoted by $\varphi(n)$, and $\varphi$ is called the Euler function.