# Algebraic Number Theory

Adam Kelly (ak2316@cam.ac.uk)

February 8, 2022

## 1 Algebraic Numbers

**Definition 1.1.** Let $\alpha \in \mathbb{C}$. We say that $\alpha$ is an **algebraic number** with $\alpha \in \overline{\mathbb{Q}}$ if it is the root of a monic polynomial with rational coefficients. If this polynomial has integer coefficients, we say that $\alpha$ is a **algebraic integer** with $\alpha \in \overline{\mathbb{Z}}$.

**Proposition 1.2.** *The only rational algebraic integers are regular integers.*

*Proof.* Clearly regular integers are algebraic integers, so we just check the other direction. Let $p/q$ be the root of a monic polynomial $f = \sum_{i=0}^{n} a_i X^i$ with $a_i \in \mathbb{Z}$ and $p, q$ coprime. Then since $f(p/q) = 0$, we have $q^n f(p/q) = \sum_{i=0}^{n} a_i p^i q^{n-1}$, and so $q^n f(p/q) \equiv p^n \equiv 0 \pmod{q}$, and since $p$ and $q$ are coprime, we must have $q = \pm 1$, and thus $p/q$ is an integer. $\square$