

# Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu  
 Coordinator: Dr. Danylo Radchenko

## Exercise Sheet 2

**Exercise 2.1.** Let  $A = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$  and  $K = \mathbb{Q}(\sqrt{-3})$ . Show that the integral closure of  $A$  in  $K$  is  $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$ .

**Exercise 2.2.** Show that the following numbers are algebraic integers:

- (a)  $\alpha = \frac{\sqrt{3} + \sqrt{7}}{2}$ ;
- (b)  $\beta = \frac{\alpha^2 - \alpha}{2}$ , where  $\alpha$  is a root of  $x^3 + x - 6$ . (To find a polynomial equation that  $\beta$  satisfies, write down the matrix of multiplication by  $\beta$  in  $\mathbb{Q}(\alpha)$ .)

**Exercise 2.3.** Let  $p$  be a prime, and let  $\zeta_p$  be a primitive  $p$ -th root of unity. Show that the integral closure of  $\mathbb{Z}$  in  $\mathbb{Q}(\zeta_p)$  is  $\mathbb{Z}[\zeta_p]$  as follows. Let  $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ .

- (a) Using the Galois action show that if  $\alpha$  is an algebraic integer, then  $pa_j \in \mathbb{Z}$ ;
- (b) Show that  $\frac{p}{(1-\zeta_p)^l}$  is an algebraic integer for  $0 \leq l \leq (p-1)$ ;
- (c) Show that  $\alpha$  can be written as

$$\alpha = \frac{m_0 + m_1(1 - \zeta_p) + \cdots + m_{p-2}(1 - \zeta_p)^{p-2}}{p},$$

where  $m_i \in \mathbb{Z}$ , and, assuming that some  $m_j$  is not divisible by  $p$ , obtain a contradiction using part (b).

**Exercise 2.4 (Gauss sums).** Let  $p$  be an odd prime, and let  $\zeta_p$  be a primitive  $p$ -th root of unity. For  $a \in (\mathbb{Z}/p\mathbb{Z})^\times$  define

$$\tau(a) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x}{p}\right) \zeta_p^{ax},$$

where  $\left(\frac{a}{p}\right)$  is the Legendre symbol.

- (a) Show that  $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$ ;
- (b) Show that  $\tau(1)^2 = (-1)^{\frac{p-1}{2}}p$ ;
- (c) Let  $K/\mathbb{Q}$  be a quadratic extension. Prove that there exists a root of unity  $\zeta$  such that  $K \subseteq \mathbb{Q}(\zeta)$ .

*Hint: in (c) note that  $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ , and use the result of part (b).*