

## Algebra II: Homework assignment 7

Due date: April 7

1. Let  $\eta$  be a primitive  $p$ -th root of unity. Show that if  $p$  is prime, then the cyclotomic field  $\mathbb{Q}(\eta)$  contains either  $\sqrt{p}$  or  $\sqrt{-p}$ .

*Hint: Let residue  $a$  be a generator of the multiplicative group  $(\mathbb{Z}/p\mathbb{Z})^*$ . Show that the periods*

$$\varepsilon_1 = \eta^a + \eta^{a^3} + \dots + \eta^{a^{p-2}}; \quad \varepsilon_2 = \eta^{a^2} + \eta^{a^4} + \dots + \eta^{a^{p-1}}$$

*satisfy a quadratic equation with integer coefficients and find these coefficients explicitly.*

2. Is it possible to square a triangle (i.e. to construct a square whose area is equal to the area of a given triangle)?

3. Show that for  $a \in \mathbb{F}_p^*$  the polynomial  $x^p - x - a$

(a) is irreducible over  $\mathbb{F}_p$ ,

(b) is irreducible over  $\mathbb{F}_{p^n}$  if and only if  $p$  and  $n$  are relatively prime.

4. (a) Find all irreducible polynomials of degree  $< 5$  over  $\mathbb{F}_2$ .

(b) Find the number of irreducible polynomials of degree 3 over  $\mathbb{F}_3$ .

(c) Find the number of irreducible polynomials of degree 2 and 3 over  $\mathbb{F}_9$ .

(d) Denote by  $I_m$  the number of irreducible polynomials of degree  $m$  over  $\mathbb{F}_p$ . Prove the following identity:

$$p^n = \sum_{d|n} dI_d.$$

5. Give an example of a finite extension that does not have a primitive element.

6. Show that any finite field  $\mathbb{F}_{p^n}$  is a Galois extension of the field  $\mathbb{F}_p$  and find its Galois group.