

Name:

Student number:

--	--	--	--	--	--	--

**Time: 3 hours.**

**The questions are to be answered with adequate explanation.**

---

1. (4 points) Give the definition of the following notions:
  - (a) an ideal of a commutative ring  $R$ ;
  - (b) a principal ideal domain (PID);
  - (c) the Galois group  $G(K/F)$  of an extension field  $K$  of  $F$ ;
  - (d) a separable extension  $K$  of a field  $F$ .

2. (8 points) State and prove primitive element theorem.

3. (8 points) Let  $F$  be a field. Prove the following statement.

Every polynomial in  $F[X]$  has a root in some extension field of  $F$ .

4. (8 points) Prove the following statement.

Let  $\alpha, \beta$  be algebraic over a field  $F$  with  $n = \deg(\alpha, F) = \deg(\beta, F)$ . The map

$$\psi_{\alpha, \beta} : F(\alpha) \rightarrow F(\beta) : \sum a_i \alpha^i \mapsto \sum a_i \beta^i$$

is an isomorphism if and only if  $\alpha$  and  $\beta$  are conjugate over  $F$ .

5. (2 points) Find all prime and maximal ideals in  $\mathbb{Z}_2 \times \mathbb{Z}_4$ .
6. (10 points)
  - (a) Give a construction of a field  $F$  with 27 elements.
  - (b) Determine a primitive element  $\alpha$  in  $F$  (a generator of the multiplicative group).
  - (c) Give a basis  $B$  for the field  $F$  as a vector space over  $\mathbb{Z}_3$ .
  - (d) Write  $\alpha^{11}$  as a linear combination of the elements of  $B$ .
  - (e) Determine the order of the element  $\alpha^4 + \alpha^7$  in the multiplicative group of  $F$ .
7. (10 points) Let  $K$  denote the splitting field of  $f(X) = X^4 + 1$  over  $\mathbb{Q}$ .
  - (a) Determine whether  $f(X)$  is irreducible over  $\mathbb{Q}$ .
  - (b) Determine  $\alpha \in K$  such that  $K = \mathbb{Q}(\alpha)$ .
  - (c) Describe the elements of the Galois group  $G(K/\mathbb{Q})$ , in terms of the element  $\alpha$  determined in (b).
  - (d) For each subgroup  $H$  of  $G(K/\mathbb{Q})$  of order two, and determine its fixed field (as a subfield of  $K$ ).
  - (e) Write each of the subfields of  $K$  determined in (d) as a simple extension of  $\mathbb{Q}$ .