NTNU
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **MA3202 Galois Theory**

Academic contact during examination: Sverre Olaf Smalø

Phone: 73591750/48293975

Examination date: 6th of May 2020

Examination time (from–to): 09:00–13:00

Permitted examination support material: All printed or handwritten notes allowed.

Language: English

Number of pages: ??

Number of pages enclosed: 0

Checked by:

Informasjon om trykking av eksamensoppgave
Originalen er:
1-sidig ☐ **2-sidig** ☒
sort/hvit ☒ **farger** ☐
skal ha flervalgskjema ☐

Date Signature

Problem 1

a) Let K be a field and G a finite subgroup of $K^* = K\backslash\{0\}$ under multiplication.

Prove that G is a cyclic group.

b) Find a generator for the cyclic group $\mathbb{Z}_{31}^*$.

c) Let K be a Galois field of odd characteristic.

Prove that exactly half of the polynomials $\{x^2 - b \,|\, b \in K\backslash\{0\}\}$ are irreducible.

d) Let K be a Galois field with q elements. Prove that there are for each natural number $n \geq 2$ at least $\frac{\Phi(q^n-1)}{n}$ monic irreducible polynomials of degree n over K, where Φ is the Euler Φ-function.

Problem 2 Let $p_1, p_2, \ldots, p_n$ be prime numbers with $p_i \neq p_j$ for $i \neq j$.

a) Prove that for any two p_i, p_j with $i \neq j$ that $[\mathbb{Q}(\sqrt{-p_i}, \sqrt{-p_j}) : \mathbb{Q}] = 4$, and that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-p_i}, \sqrt{-p_j})$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

b) Let $K = \mathbb{Q}(\sqrt{-p_1}, \sqrt{-p_2}, \ldots, \sqrt{-p_n})$. Considering K as a subfield of $\mathbb{C}$, we observe that complex conjugation is an automorphism of K of order 2.

Find the fix point field of K under complex conjugation. (Hint: Try with $n = 2$ first.)

c) Find the Galois group of K over $\mathbb{Q}$ and conclude that $[K : \mathbb{Q}] = 2^n$.

Problem 3 Let $K = \mathbb{Q}(x)$, the field of rational functions in one variable over $\mathbb{Q}$.

a) For $a, b, c, d \in \mathbb{Z}$ with $ac - bd = 1$ define $\mu_{(a,b,c,d)} : \mathbb{Q}(x) \to \mathbb{Q}(x)$ by

$$\mu_{(a,b,c,d)}(f) = f(\frac{ax + b}{cx + d}).$$

Prove that $\mu_{(a,b,c,d)}$ is a field automorphism.

b) Consider the special cases $(a, b, c, d) = (0, -1, 1, 0)$ and $(a, b, c, d) = (0, 1, -1, 1)$ and prove that $\mu_{(0,-1,1,0)}$ is of order two and that $\mu_{(0,1,-1,1)}$ is of order three and find the fix point fields of $\mu_{(0,-1,1,0)}$ and $\mu_{(0,1,-1,1)}$.

c) Show that $\mu_{(0,-1,1,0)} \circ \mu_{(0,1,-1,1)}$ has infinite order.