NTNU

Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **MA3202 Galois Theory**

Academic contact during examination: Sverre O. Smalø

Phone: 48293975

Examination date: June 4th 2018

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

Permitted examination support material: B: Simple calculator.

Language: English

Number of pages: 1

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 Consider the field extension $E = \mathbb{Q}[2^{\frac{1}{2}}, 3^{\frac{1}{3}}, e^{\frac{2\pi i}{3}}]$ of $\mathbb{Q}$.

a) Find $[E : \mathbb{Q}]$ and show that E is a splitting field.

b) Find the Galois group $G(E/\mathbb{Q})$.

c) How many fields K exist with $\mathbb{Q} \subseteq K \subseteq E$ and how many of them are normal extensions of $\mathbb{Q}$?

Problem 2 Consider the subring $R = \mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,\ b \in \mathbb{Z}\}$ of $\mathbb{Q}[\sqrt{2}]$.

a) Prove that the group of units in R is infinite.

b) Prove that the minimal polynomial in $\mathbb{Q}[X]$ of $\alpha \in \mathbb{Q}[\sqrt{2}]$ is in $\mathbb{Z}[X]$, if and only if α is in R.

c) Prove that R is an Eeuclidian domain where $d : R \to \mathbb{N}$ is given by $d(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Hint: Prove that for $a + b\sqrt{2} \neq 0$ in R and $x + y\sqrt{2}$ in R, $d(x + y\sqrt{2} - (s + t\sqrt{2})(a + b\sqrt{2})) \leq \frac{3}{4}d(a + b\sqrt{2})$ where s is an integer closest to the fraction $\frac{ya-2xb}{a^2-2b^2}$ and t is an integer closest to the fraction $\frac{xa-yb}{a^2-2b^2}$.

Problem 3 Consider a prime number p and a natural number n.

a) Find a formula for how many monic irreducible polynomiasl f of degree n exist in $\mathbb{Z}_p[X]$ with the property that if $f(\alpha) = 0$ in $GF(p^n)$, then α is a generator for $GF(p^n)^*$, the multiplikative group of units in $GF(p^n)$.

b) Let $n = q_1^2 q_2^2 q_3^2$ with q_i primes and $q_i \neq q_j$ for $i \neq j$. Find a formula for the number of irreducible polynomial of degree n in $\mathbb{Z}_p[X]$.

Problem 4 Let p be a prime number and let $GL_3(\mathbb{Z}_p)$ be the group of invertible 3×3-matrices over $\mathbb{Z}_p$.

a) Prove that the order of any element of $GL_3(\mathbb{Z}_p)$ is less than or equal to $p^3 - 1$.

b) Prove that if α is an element of $GL_3(p^n)$ of order $p^3 - 1$, then the subgroup $\langle\alpha\rangle$, generated by α, together with 0 is a subfield of the ring of 3×3 matrices over $\mathbb{Z}_p$.