UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Examination in	MAT2200 — Groups, rings and fields.
Day of examination:	4 June 2021 at 15:00 to 4 June 2021 at 19:00
Examination hours:	15:00 – 19:00.
This problem set consists of 3 pages.	
Appendices:	All.
Permitted aids:	All.

Please make sure that your copy of the problem set is complete before you attempt to answer anything.

Important: This is a written digital home exam. The solution must be delivered in Inspera, see the guidelines elsewhere. You must provide justification for all your answers. You may deliver the solution to the exam written in Norwegian, Danish, Swedish or English. Short dictionary: field is "kropp", splitting field is "rotkropp", degree of an extension is "tallgrad", isomorphism is "isomorfi".

There are 10 subproblems distributed over 4 main problems. The 10 subproblems have equal weight.

Problem 1

For G a finite group and $g \in G$ we denote $|G|$ the order of G and $|g|$ the order of g in the group. Recall that $|g|$ is the smallest positive integer $k \in \mathbb{Z}^*$ so that $g^k = e$, with e denoting the identity in the group G.

1a

Let $\mathbb{Z}_6$ be the additive group of integers modulo 6 and $\mathbb{Z}_6^*$ the group of units modulo 6. Show that

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_6^*, b \in \mathbb{Z}_6 \right\}$$

is a group under matrix multiplication. Show that G is non-abelian. Find its order $|G|$.

1b

Find all elements of order 3 in G. Prove that G is not a simple group.

(Continued on page 2.)

Problem 2

For $d \in \mathbb{Z}^+$, the number of integers $1 \leq k \leq d$ such that $gcd(k, d) = 1$ is denoted $\phi(d)$. If G is cyclic of order $n \in \mathbb{Z}^+$ and d is a positive divisor of n with $1 \leq d \leq n$, it is known that the number of elements of order d in G is equal to $\phi(d)$. We write $d|n$ when d is such a divisor of n.

2a

Show that for each positive integer n we have $n = \sum_{d|n} \phi(d)$. Hint: if G is a cyclic group of order n, such as $\mathbb{Z}_n$, consider the subsets of G of elements of order d for each divisor $d|n$.

2b

Suppose that G is a finite group of order n such that for each positive divisor $d|n$ there is at most one subgroup of G of order d. For each such d let G_d be the subset of G consisting of elements $a \in G$ such that $|a| = d$ (note that it may be empty). Show that the number of elements in G_d is $\phi(d)$ for each positive divisor d of n. Conclude that G is cyclic.

Problem 3

For p a prime and n a positive integer, we let $\mathbb{F}_{p^n}$ be the field with p^n elements, with $\mathbb{F}_p$ denoting $\mathbb{Z}_p$.

3a

Determine if $\mathbb{F}_2[x]/\langle x^4 + 1\rangle$ is an integral domain.

3b

Show that $f(x) = x^4 + x^3 + 1$ is irreducible in $\mathbb{F}_2[x]$. Explain why $f(x)$ admits a zero θ in the field $\mathbb{F}_{16}$, seen as an extension of $\mathbb{F}_2$ with degree $[\mathbb{F}_{16} : \mathbb{F}_2] = 4$. Prove that $f(x)$ is a primitive polynomial in $\mathbb{F}_2[x]$, meaning that θ is a generator of the multiplicative group of units $\mathbb{F}_{16}^*$.

3c

Assume known that $x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. With $f(x)$ as in part 3b, explain why there is an isomorphism of fields

$$\mathbb{F}_2[x]/\langle f(x)\rangle \cong \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle.$$

(Continued on page 3.)

3d

It is known that the Galois group $Gal(\mathbb{F}_{16}/\mathbb{F}_2)$ is a cyclic group of order 4 generated by the Frobenius automorphism σ_2. Use this to write a splitting of $f(x)$ from part 3b into linear factors in $\mathbb{F}_{16}[x]$. If needed, you can use without proof that an irreducible polynomial of degree 4 in $\mathbb{F}_2[x]$ divides $x^{2^4} - x$ in $\mathbb{F}_2[x]$.

Problem 4

Let $f(x) = (x^2 - 2)(x^2 - 5)$ in $\mathbb{Q}[x]$.

4a

Find the zeros of $f(x)$ in $\mathbb{C}$ and determine the splitting field K of $f(x)$ over $\mathbb{Q}$. Show that $[K : \mathbb{Q}] = 4$. You may use without proof that the polynomial $x^4 - 14x^2 + 9$ is irreducible in $\mathbb{Q}[x]$.

4b

Find the Galois group $Gal(K/\mathbb{Q})$, and write down the diagrams of subgroups H of $Gal(K/\mathbb{Q})$ and subfields E of K with $\mathbb{Q} \subset E \subset K$ obtained as fixed fields E_H. Explain what subgroup is carried to what subfield under the Galois correspondence.

SLUTT.