# UNIVERSITY OF OSLO

## Faculty of mathematics and natural sciences

| | |
|---|---|
| Exam in: | MAT2200 — Groups, Rings and Fields |
| Day of examination: | Thursday 9. June 2022 |
| Examination hours: | 15:00 – 19:00 |
| This problem set consists of 5 pages. | |
| Appendices: | none |
| Permitted aids: | all |

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

Justification must be provided for all solutions. Solutions can be submitted in English or Norwegian. The format may be in Latex or as scanned handwritten notes.

## Problem 1 Group theory

1. (5 points) Let $G$ be a group of order 200. What are the sizes of Sylow p-subgroups of $G$?

   **Solution**

   First factor $200 = 2^3 * 5^2$. Therefore the only p-subgroups are of order $p = 2, 5$ and the Sylow 2-subgroups are of order $2^3 = 8$ and the Sylow 5-subgroups are of order $5^2 = 25$.

2. (10 points) Let $G = \mathbb{Z}_{12} \times \mathbb{Z}_8$. Find the order of the element $(4, 2) \in G$. Determine the quotient group $G/\langle(4, 2)\rangle$ up to isomorphism.

   **Solution**

   The order of $(4, 2)$ is the smallest $k \in \mathbb{Z}_{>0}$ such that $k(4, 2)$ is $(0, 0)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_8$. Therefore $k$ must be a multiple of 3 and a multiple of 4. The least common multiple of 3 and 4 is 12. Therefore $(4, 2)$ is of order 12.

   The quotient group $K = G/\langle(4, 2)\rangle$ is therefore a group of order 8. Moreover, it is abelian since it is the quotient of an abelian group. By the structure theorem of finite abelian groups $K$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_8$.

   To determine which of the three is isomorphic to $H$ we first write out the elements of $H = \langle(4, 2)\rangle$:

   $$\{(0,0), (4,2), (8,4), (0,6), (4,0), (8,2), (0,4), (4,6), (8,0), (0,2), (4,4), (8,6)\}.$$

   We notice that the element of $K$ given by $(1, 1) + H$ has order 4 in $K$. Hence $K$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ which only has elements of order 2 and 1.

*(Continued on page 2.)*

Lastly $K$ is isomorphic to $\mathbb{Z}_8$ if and only if there exists and element $(k,l)+H$ of order 8. For any element $(k,l)+H$ of $K$ the element $4(k,l)+H=(m,n)+H$ where $m\in\{0,4,8\}$ and $n=\{0,4\}$. Checking the list of elements above we see that such an $(m,n)$ is always contained in $H$. Hence every element of $K$ has order divisible by 4 and thus $K$ is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_4$.

3. (10 points) Let $p$ be a prime number. Suppose $G$ is a group of order $p^n$ acting on a set $X$ such that $p$ does not divide $|X|$. Show that the action of $G$ must have a fixed point, i.e. there exists an $x\in X$ such that $|\mathcal{O}_x|=1$.

   Hint: Consider the partition of $X$ into the orbits of the action and use that $|\mathcal{O}_x|=[G:G_x]=|G|/|G_x|$.

   **Solution**

   The action of $G$ partitions $X$ into disjoint orbits $\mathcal{O}_1,\dots,\mathcal{O}_s$. Suppose for contradiction that $|\mathcal{O}_x|>1$ for all $x\in G$. Since $|\mathcal{O}_x|=[G:G_x]=|G|/|G_x|$ we must have that $|\mathcal{O}_x|=p^{k_x}$ for some $k_x>0$. This means that $\mathcal{O}_i$ must have size $p^{k_i}$ for some $k_i>0$.

   Now since the orbits partition $X$ we have

$$|X|=\sum_{i=1}^{s}|\mathcal{O}_i|=\sum_{i=1}^{s}p^{k_i}.$$

   We see that $p$ divides the right hand side of the equation hence $p$ divides $|X|$. We arrive at a contradiction, therefore there must exist an orbit of size 1, equivalently the action of $G$ has a fixed point.

## Problem 2 Ring theory

1. (5 points) Show that $\mathbb{Z}_{12}$ is not an integral domain.

   **Solution**

   A ring is an integral domain if it contains no zero divisors. Consider the elements 3 and 4 in $\mathbb{Z}_{12}$. Then $3\cdot 4=0$ yet $3\neq 0$ and $4\neq 0$. Hence this ring is not an integral domain.

2. (10 points) Let $p$ be a prime number and $n>1$. Find a maximal ideal $M$ of $\mathbb{Z}_{p^n}$ and identify the quotient $\mathbb{Z}_{p^n}/M$.

   **Solution**

   A maximal ideal $M$ is the principal ideal $\langle p\rangle$. To see this notice first that every ideal of $\mathbb{Z}_{p^n}$ is also an additive subgroup. As a group $\mathbb{Z}_{p^n}$ is cyclic hence all subgroups are of the form $\langle a\rangle$. Moreover they can all be generated by divisors of $p^n$. Hence every subgroup is of the form $\langle p^k\rangle$ for $0\leq k<n$, and we have $\langle p^k\rangle\leq\langle p^l\rangle$ if and only if $k\geq l$ and $\langle p^0\rangle=\mathbb{Z}_{p^n}$. Therefore, $\langle p\rangle$ is maximal among the proper subgroups and hence the proper ideals.

   **Alternatively, one could use the surjective homomorphism $\phi:\mathbb{Z}\to\mathbb{Z}_{p^n}$ and argue with pulling back ideals.**

*(Continued on page 3.)*

The quotient of a commutative ring with unity by a maximal ideal is a field. Since $\mathbb{Z}_{p^n}$ is finite, the quotient will be a finite field. Up to isomorphism these are determined by their size. We see that the quotient $\mathbb{Z}_{p^n}/M$ has exactly $p$ elements, therefore the quotient is isomorphic to the finite field $\mathbb{Z}_p$.

3. (10 points) Show that if an ideal $I$ of the polynomial ring $\mathbb{Q}[x]$ contains both $f(x) = x^3 - x^2 + x$ and $g(x) = x^2 - 1$ then $I = \mathbb{Q}[x]$.

   Hint: Show that $I$ contains the remainder $r(x)$ when $f(x)$ is divided by $g(x)$.

   **Solution**

   Performing long division on the polynomials $g(x)$ and $f(x)$ we see that $f(x) = (x-1)(x^2-1)+2x$. Since $f(x)$ and $g(x)$ are both in $I$ and $I$ is an ideal, we have that $(x-1)g(x)$ is in $I$ and also that $f(x)-(x-1)(x^2-1)$ is in $I$. This implies that $2x$ is in $I$, we can further conclude that $x \in I$ since $1/2 \in \mathbb{Q}$.

   Now we have that $f(x), g(x)$, and $x$ are all in $I$. Performing long division for $g(x)$ divided by $x$ we obtain a remainder of $-1$. By the same argument above we conclude that the element $-1$ is in $I$. The element $-1$ is a unit in $\mathbb{Q}[x]$ therefore $I = \mathbb{Q}[x]$.

   **During the zoom check in I became convinced the hint of the exercise was misleading in that it was not as direct as I intended. I suggested that the degree 3 polynomial be changed to $x^3-x^2-x$. Many did not receive this message. The statement is true either way, but slightly more is required to prove the original statement. Most points were given for the justification of the hint if it was applied or attempted to be applied.**

## Problem 3 Finite fields

Consider $F = \mathbb{Z}_3$ and the irreducible polynomial $f(x) = x^3 + 2x + 2 \in F[x]$. Let $E$ be the field $F[x]/\langle f(x)\rangle$.

1. (5 points) What is the size of $E$?

   **Solution** $E$ is a finite field which arises as a degree 3 extension of the field of size 3. Therefore, $E$ is of size $3^3 = 27$.

2. (10 points) Let $\alpha \in \overline{F}$ denote a zero of $f(x)$ so that $E \cong F(\alpha)$. Let

   $$\sigma_3 : F(\alpha) \to F(\alpha)$$

   denote the Frobenius automorphism defined by $\sigma_3(a) = a^3$ for all $a \in F(\alpha)$.

   Write $\sigma_3(\alpha)$ and $\sigma_3^2(\alpha)$ in the basis $\{1, \alpha, \alpha^2\}$ for $F(\alpha)$ over $F$.

   **Solution** First consider $\sigma_3(\alpha) = \alpha^3 = -(2\alpha + 2) = \alpha + 1$. Next $\sigma_3^2(\alpha) = (\alpha+1)^3 = \alpha^3+1^3$ this is by applying the "Freshman's dream" for the binomial expansion of the third power mod 3. Therefore, $\sigma_3^2(\alpha) = \alpha + 1 + 1 = \alpha + 2$.

*(Continued on page 4.)*

3. (10 points) Assume $g(x) = x^3 + 2x + 1 \in F[x]$ is irreducible over $F$ and let $\beta \in \overline{F}$ be a zero of $g(x)$.

   Prove that $F(\alpha)$ and $F(\beta)$ are isomorphic without giving an isomorphism. However explain why a map $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ which fixes $F$ and sends $\alpha$ to $\beta$ cannot be made into a field isomorphism.

   **Solution** The fields $F(\alpha)$ and $F(\beta)$ are both finite fields of order $3^3$. By the uniqueness of Galois fields of size $p^n$ up to isomorphism we have that $F(\alpha)$ and $F(\beta)$ must be isomorphic.

   A field isomorphism $F(\alpha) \to F(\beta)$ which fixes $F$ must send $\alpha$ to a conjugate element over $F$. Two elements are conjugate over $F$ if they have the same irreducible polynomial. The irreducible polynomials of $\alpha$ and $\beta$ are not the same hence, $\psi_{\alpha,\beta}$ cannot be a field isomorphism.

   **Alternatively, one may show directly that the homomorphism property is not satisfied for some elements for the map $\psi_{\alpha,\beta}$.**

## Problem 4 Galois Theory

Let $K = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$ where $\zeta_5 = e^{\frac{2\pi i}{5}}$.

1. (5 points) Find a polynomial $f(x) \in \mathbb{Q}[x]$ for which $K$ is its splitting field over $\mathbb{Q}$.

   The polynomial $f(x) = x^5 - 2$ has splitting field $K$.

2. (10 points) Consider the intermediate field $E = \mathbb{Q}(\sqrt[5]{2})$. What are the degrees $[E : \mathbb{Q}]$, $[K : E]$, and $[K : \mathbb{Q}]$? You may assume $p(x) = x^4 + x^3 + x^2 + x^1 + 1$ is irreducible over $E$.

   The degree $[E : \mathbb{Q}] = \deg irr(\sqrt[5]{2}, \mathbb{Q})$. The irreducible polynomial of $\sqrt[5]{2}$ is $f(x)$ which has degree 5. The irreducible polynomial of $[K : E] = \deg irr(\zeta_5, E) = \deg x^4 + x^3 + x^2 + x^1 + 1 = 4$.

   We can use the product formula for degrees of field extensions to see that $[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 5 \cdot 4 = 20$.

3. (10 points) Consider the intermediate field $F = \mathbb{Q}(\zeta_5)$. The Galois group $G(F/\mathbb{Q})$ is the cyclic group of order 4 generated by the automorphism $\sigma : F \to F$ satisfying $\sigma(\zeta_5) = \zeta_5^2$.

   Show that $\sigma^2 : F \to F$ acts by complex conjugation and that the fixed field of the subgroup $H = \langle \sigma^2 \rangle < G(F/\mathbb{Q})$ is $\mathbb{Q}(\zeta_5 + \zeta_5^4)$.

   **Solution**

   Since $\sigma(\zeta_5) = \zeta_5^2$ we have that $\sigma^2(\zeta_5) = \zeta_5^4$. Notice that $\sigma^2(\zeta_5) = \zeta_5^4 = \overline{\zeta_5}$ where the overline denotes complex conjugation. Every element of $F$ can be written as $a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3$ for $a, b, c, d \in \mathbb{Q}$ and since complex conjugation is a group homomorphism as well we see that $\sigma^2(\alpha) = \overline{\alpha}$.

   The fixed field $F_{\sigma^2}$ of $\sigma^2$ must be a field extension of degree 2 of $\mathbb{Q}$. Notice that $\mathbb{Q}(\zeta_5 + \zeta_5^4)$ is contained in $F_{\sigma^2}$, since $\sigma^2(\zeta_5 + \zeta_5^4) = \zeta_5^4 + \zeta_5$. Suppose that $\mathbb{Q}(\zeta_5 + \zeta_5^4) \neq F_{\sigma^2}$, then $[F_{\sigma^2} : \mathbb{Q}(\zeta_5 + \zeta_5^4)] > 1$. However,

   $$2 = [F_{\sigma^2} : \mathbb{Q}] = [F_{\sigma^2} : \mathbb{Q}(\zeta_5 + \zeta_5^4)][\mathbb{Q}(\zeta_5 + \zeta_5^4) : \mathbb{Q}].$$

*(Continued on page 5.)*

So if $\mathbb{Q}(\zeta_5 + \zeta_5^4) \neq F_{\sigma^2}$ we must have that $[\mathbb{Q}(\zeta_5 + \zeta_5^4) : \mathbb{Q}] = 1$ and hence $\mathbb{Q}(\zeta_5 + \zeta_5^4) = \mathbb{Q}$. However, we can see that $\zeta_5 + \zeta_5^4 = 2cos(2\pi/5)$ is not a rational number by checking that $cos(2\pi/5)$ is not rational. Therefore the fixed field of $\sigma^2$ is $\mathbb{Q}(\zeta_5 + \zeta_5^4)$.