M E T U
Department of Mathematics

Abstract Algebra **Midterm 2**	
Code : *Math 367* Acad. Year : *2015* Semester : *Fall* Instructor : *Küçüksakallı* Date : *Dec 14, 2015* Time : *17:40* Duration : *120 minutes*	Last Name : Name : Student No. : Signature : 6 QUESTIONS ON 4 PAGES 100 TOTAL POINTS

1	2	3	4	5	6		

1. (25pts) For each of the following statements determine if it is **true** or **false**. Explain your answer briefly.

- Let G be a finite group and p be a prime number. There exists an element $a \in G$ of order p if and only if p divides $|G|$.

  True. $(\Rightarrow)$ by Lagrange's Theorem and $(\Leftarrow)$ by Cauchy's Theorem.

- Let G be a finite group such that $|G|$ is divisible by p^2 where p is prime. Then there exists an element $a \in G$ of order p^2.

  False. The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ does not have an element of order 4.

- Let G be a finite group such that $|G|$ is divisible by p^2 where p is prime. Then there exists a subgroup $H \leq G$ of order p^2.

  True. Sylow's First Theorem.

- The set $S = \{2a + b\sqrt{367} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{R}$.

  False. Because $\sqrt{367} \cdot \sqrt{367} = 367 \notin R$.

- The subrings $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ and $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$ of $\mathbb{Z}$ are isomorphic.

  False. Assume otherwise and let $f : 2\mathbb{Z} \to 3\mathbb{Z}$ be an isomorphism. Then $f(2) = 3k$ for some nonzero $k \in \mathbb{Z}$. Then $f(4) = f(2 \cdot 2) = f(2) \cdot f(2) = 9k^2$ and $f(4) = f(2+2) = f(2) + f(2) = 2f(2) = 6k$. We have $9k^2 = 6k$, a contradiction.

2a. (5pts) State the class equation.

Theorem(Class Equation): Let G be a finite group. Then

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C_G(a)],$$

where the sum runs over distinct conjugacy class representatives.

2b. (10pts) If G is a finite p-group with $|G| > 1$, then show that $|Z(G)| > 1$.

Theorem 7.2.7 in your textbook.

3. (10pts) Let G be a group of order 105.

- Show that G is not simple.

  Assume that $n_5 > 1$ and $n_7 > 1$. Sylow's Third Theorem implies that $n_5 = 21$ and $n_7 = 15$. There are $21 \cdot 4 = 84$ elements of order 5 and $15 \cdot 6 = 90$ elements of order 7. In total there are $90 + 84 = 174$ elements in G of order 5 or 7, a contradiction. Therefore $n_5 = 1$ or $n_7 = 1$. In either case there exists a unique Sylow p-subgroup which is normal in G. Thus G is not simple

- Show that G has a subgroup of order 35.

  Let P_5 and P_7 be a Sylow 5-subgroup and a Sylow 7-subgroup, respectively. From the previous part we know that P_5 or P_7 is normal in G. It follows that $H = P_5P_7$ is a subgroup of G. We have $P_5 \cap P_7 = \{e\}$ and therefore $|H| = |P_5||P_7|/|P_5 \cap P_7| = 35$. We conclude that there exist a subgroup $H \leq G$ of order 35.

4. (25pts) Let $M_2(\mathbb{Q})$ be the ring of 2×2 matrices with rational entries under the usual matrix addition and multiplication. Consider

$$R = \left\{ \left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right] \middle| \, a, b, c \in \mathbb{Q} \right\} \quad \text{and} \quad I = \left\{ \left[\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right] \middle| \, b \in \mathbb{Q} \right\}.$$

- Show that R is a subring of $M_2(\mathbb{Q})$.

  Pick $M = \left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right]$ and $M' = \left[\begin{smallmatrix} a' & b' \\ 0 & c' \end{smallmatrix}\right]$ in R. Then $M - M' = \left[\begin{smallmatrix} a-a' & b-b' \\ 0 & c-c' \end{smallmatrix}\right]$ and $M \cdot M' = \left[\begin{smallmatrix} aa' & ab'+bc' \\ 0 & cc' \end{smallmatrix}\right]$ are also in R. Thus R is a subring of $M_2(\mathbb{Q})$.

- Show that I is not an ideal of $M_2(\mathbb{Q})$.

  Pick $A = \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right] \in M_2(\mathbb{Q})$ and $B = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] \in I$. Then $A \cdot B = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is not an element of I. Thus I is not an ideal of $M_2(\mathbb{Q})$.

- Show that I is an ideal of R.

  It is easy to see that I is an additive subgroup of R. Pick $A = \left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right] \in R$ and $B = \left[\begin{smallmatrix} 0 & b' \\ 0 & 0 \end{smallmatrix}\right] \in I$. then $A \cdot B = \left[\begin{smallmatrix} 0 & ab' \\ 0 & 0 \end{smallmatrix}\right]$ and $B \cdot A = \left[\begin{smallmatrix} 0 & cb' \\ 0 & 0 \end{smallmatrix}\right]$ which are both in I. Thus I is an ideal of R.

- Show that the map $f\left(\left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right]\right) = (a, c)$ is a ring homomorphism from R to $\mathbb{Q} \times \mathbb{Q}$. (Here $\mathbb{Q} \times \mathbb{Q}$ is the usual ring with componentwise addition and multiplication.)

  Let $M = \left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right]$ and $M' = \left[\begin{smallmatrix} a' & b' \\ 0 & c' \end{smallmatrix}\right]$. Then

  $$f(M + M') = f(\left[\begin{smallmatrix} a+a' & b+b' \\ 0 & c+c' \end{smallmatrix}\right]) = (a + a', c + c') = (a, c) + (a', c') = f(M) + f(M'),$$

  and

  $$f(M \cdot M') = f(\left[\begin{smallmatrix} aa' & ab'+bc' \\ 0 & cc' \end{smallmatrix}\right]) = (aa', cc') = (a, c) \cdot (a', c') = f(M) \cdot f(M').$$

  Thus $f : R \to \mathbb{Q} \times \mathbb{Q}$ is a ring homomorphism.

- Show that the quotient ring R/I is isomorphic to $\mathbb{Q} \times \mathbb{Q}$.

  The map $f : R \to \mathbb{Q} \times \mathbb{Q}$ is a ring homomorphism with $\mathrm{Ker}(f) = I$. Moreover, f is surjective. The first isomorphism theorem implies that $R/I \cong \mathbb{Q} \times \mathbb{Q}$ as rings.

5. (15pts) Set $i = \sqrt{-1}$ and consider the subring $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. Let I be the ideal of R generated by 2 and $3 + i$, i.e. $I = \langle 2, 3 + i\rangle$.

- Show that $I = \langle 1 + i\rangle$.

  Note that $2 = (1 + i) \cdot (1 - i)$ and $3 + i = (1 + i) \cdot (2 - i)$. Pick $\alpha \in \langle 2, 3 + i\rangle$. Then $\alpha = r \cdot 2 + s \cdot (3 + i)$ for some $r, s \in R$. Thus $\alpha = (1 + i) \cdot (r \cdot (1 - i) + s \cdot (2 - i))$. It follows that $\langle 2, 3 + i\rangle \subseteq \langle 1 + i\rangle$. On the other hand $1 + i = (3 + i) - 2$. Pick $\beta \in \langle 1 + i\rangle$. Then $\beta = r \cdot (1 + i)$ for some $r \in R$. Thus $\beta = r \cdot (3 + i - 2)$ where $3 + i - 2 \in \langle 2, 3 + i\rangle$. Thus $\langle 2, 3 + i\rangle \supseteq \langle 1 + i\rangle$. We conclude that $\langle 2, 3 + i\rangle = \langle 1 + i\rangle$.

- Determine the number of elements in the quotient ring R/I.

  The quotient ring is given by $R/I = \{r + I \mid r \in R\}$. Note that $i - 1 = i \cdot (1 + i) \in I$. Thus $i + I = 1 + I$ since $1 - i \in I$. It follows that $a + bi + I = a + b + I$. Moreover $a + b + I$ is equal to either $0 + I$ or $1 + I$ since $2 \in I$. The elements $0 + I$ and $1 + I$ are distinct in R/I because $1 \notin I$. Therefore $|R/I| = 2$.

6. (10pts) Show that any finite field has order p^n, where p is prime. (Hint: Use the fundamental theorem of finite Abelian groups.)

Let $(F, +, \cdot)$ be a finite field. Then $(F, +)$ is a finite Abelian group and we have

$$F \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

where $p_1, \ldots, p_k$ are primes. It is enough to show that $p_i = p_j$ for all $1 \leq i, j \leq k$. Assume otherwise and let p and q be two distinct primes dividing the order F. By Cauchy's theorem, there exist elements $x, y \in F$ of order p and q, respectively. Note that $qx \neq 0$ and $py \neq 0$. On the other hand

$$(qx)(py) = qp(xy) = (px)(qy) = 0.$$

It follows that there are zero divisors in the field F, a contradiction.