MATH 503

Fall 2018

Midterm Exam 2

Solution

Instructions: Give a complete solution to each problem. You may use any result from class, the book, or homework **except** the statement you are asked to prove (or one whose proof relies on the given statement). Be sure to justify your statements.

1. **(10 points)**. If $\varphi : G \to G'$ is a surjective homomorphism, and $N \triangleleft G$, prove $\varphi(N) \triangleleft G'$.

   Solution: Let $x \in \varphi(N)$, and $h \in G'$. Then $x = \varphi(n)$ for some $n \in N$, and since φ is surjective, $h = \varphi(g)$ for some $g \in G$. Now $hxh^{-1} = \varphi(g)\varphi(n)\varphi(g)^{-1}$. Since φ is a homomorphism, $\varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(gng^{-1})$. Since $N \triangleleft G$, we have $gng^{-1} \in N$, so $\varphi(gng^{-1}) \in \varphi(N)$. Thus, for all $x \in \varphi(N)$ and any $h \in G'$, we have $hxh^{-1} \in \varphi(N)$, so $\varphi(N) \triangleleft G'$. $\square$

2. **(12 points)** Let $n \geq 1$. Prove that $\mathbb{Z}/n\mathbb{Z}$ has non-zero nilpotent elements if and only if $p^2|n$ for some prime p.

   Solution: An element $a \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if $a^k = 0$, for some $k > 0$. That is, $a^k \equiv 0 \mod n$ for some $k > 0$. First suppose there is a prime p with $p^2|n$, and let $a = \dfrac{a}{p}$. Then $1 < a < n$, and $a^2 = \dfrac{n^2}{p^2} = n\dfrac{n}{p^2}$. By assumption $n/p^2 \in \mathbb{Z}$, so $a^2 = 0$, and so a is nilpotent. Converseley, suppose $a \in \mathbb{Z}/n\mathbb{Z}$ is a non-zero nilpotent element. Choose $k > 0$ with $a^k = 0$. Suppose $a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and each $\alpha_i > 0$. For each i, we have $p_i|n$, so $p_i|a^k$, and hence, since p_i is prime, $p_i|a$. So, if $\alpha_i = 1$ for each i, then $n|a$, which contradicts our choice of a, and thus, $\alpha_i \geq 2$, for some i. So there is a prime p with $p^2|n$. $\square$

3. **True/False (5 points each)** Determine whether each of the following statements is true or false. If true, give a proof. If false, give a concrete counterexample.

(a) If G is a non-abelian group and $N \triangleleft G$, with $\{e\} \subsetneq N \subsetneq G$, then G/N is non-abelian.

(b) $\mathbb{Z}[x^2]$ is an ideal of $\mathbb{Z}[x]$.

(c) If R is an integral domain and $x^2 = 1$, then $x = \pm 1$.

(d) If α is an odd permutation, then α^{-1} is an odd permutation.

(e) $2\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic rings.

Solution:

(a) **False.** Let $G = S_3$, which is nonabelian, and $N = \langle(123)\rangle = \{1, (123), (132)\}$. Then $|G : N| = 2$, so $N \triangleleft G$, and $G/N \simeq \mathbb{Z}/2\mathbb{Z}$ is abelian.

(b) **False.**. Note $x \in \mathbb{Z}[x]$ and $x^2 \in \mathbb{Z}[x^2]$, but $x \cdot x^2 = x^3 \notin \mathbb{Z}[x^2]$, so $\mathbb{Z}[x^2]$ is not an ideal of $\mathbb{Z}[x]$.

(c) **True.** If $x^2 = 1$, then $x^2 - 1 = (x-1)(x+1) = 0$. Since R is an integral domain, one of the two factors is zero, so $x - 1 = 0$, or $x + 1 = 0$, i.e., $x = \pm 1$.

(d) **True.** Suppose $\alpha = \alpha_1\alpha_2 \cdots \alpha_{2k+1}$, with each α_i a transposition, then $a^{-1} = \alpha_{2k+1} \cdots \alpha_2\alpha_1$ is also a product of an odd number of transpositions, so is also odd. (Alternatively, $\alpha\alpha^{-1} = 1$ is even, and since α is odd, α^{-1} must also be odd.)

(e) **False.** Suppose $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ is any homomorphism. Let $\varphi(2) = 3a$. Then $\varphi(4) = \varphi(2+2) = \varphi(2) + \varphi(2) = 6a$, but $\varphi(4) = \varphi(2^2) = \varphi(a)^2 = 9a$. So, $9a = 6a$, which says $3a = 0$, or $a = 0$. Thus the zero map is the only homomorphism from $2\mathbb{Z}$ to $3\mathbb{Z}$, and hence there is no isomorphism between these two rings. $\square$

4. **(15 points)** Let G be a finite group of composite order n with the property that G has a subgroup of order k for each $k|n$. Prove G is not simple.

Solution: Since n is composite, there is some prime p with $1 < n/p < n$. Let p be the smallest prime dividing n and let $n = pk$. Then, by assumption, there is a subgroup H of G with $|H| = k$. Thus, $|G : H| = p$, with p the smallest prime dividing $|G|$, so $H \triangleleft G$, with $1 \subsetneq H \subsetneq G$. Thus, G is not simple. $\square$

5. **(20 points)** Let R be a ring, and $I \subset R$ an ideal of R.. Let $M_n(R)$ be the ring of $n \times n$ matrices of R. Prove $M_n(R)/M_n(I) \simeq M_n(R/I)$.

Solution:. Let $\varphi : R \to R/I$ be the natural map, i.e., $\varphi(a) = a + I$. Let $\psi : M_n(R) \to M_n(R/I)$ be given by $\psi(A)_{ij} = \varphi(A_{ij})$, i.e., we apply φ to the entries of A. Then, since the operations of $M_n(R)$ and $M_n(R/I)$ are given by combinations of the ring operations in R and R/I, respectively, and all such operations are respected by φ, we have ψ is a ring homomorphism. Now we clearly have ψ is surjective, and $A \in \ker\varphi$ if and only if $A_{ij} \in I$, for each i, j, i.e., $\ker\varphi = M_n(R/I)$. Thus, by the First Isomorphism Theorem,

$$M_n(R)/M_n(I) \simeq M_n(R/I).$$

$\square$

6. **(18 points)** State and prove the Class Equation.

Theorem (The Class Equation): Let G be a finite group with center Z and let $g_1, g_2, \ldots, g_k$ be a set of representatives for the non-central conjugacy classes in G. Then

$$|G| = |Z| + \sum_{i=1}^{k} |G : C_G(g_i)|.$$

Proof: Consider G acting on itself by conjugation. Since conjugacy the classes are the equivalence classes of this action, they partition G. Note, if $z \in Z$, then $xzx^{-1} = z$ for all $x \in G$, so $\{z\}$ is its conjugacy class. Let $\mathcal{C}_j = \{xg_jx^{-1} | x \in G\}$ be the conjugacy class of g_j. Then, we have

$$G = Z \coprod \mathcal{C}_1 \coprod \mathcal{C}_2 \cdots \coprod C_k. \tag{1}$$

For each j, the conjugacy class C_j is the orbit of g_j under conjugation, and hence, by the Orbit-Stabilizer Theorem $|\mathcal{C}_j| = |G : \mathrm{Stab}_G(g_j)|$. Now

$$\mathrm{Stab}_G(g_j) = \{x \in G | xg_jx^{-1} = g_j\} = \{x \in G | xg_j = g_jx\} = C_G(g_j).$$

Now from equation (1) we have

$$|G| = |Z| + \sum_{i=1}^{k} |\mathcal{C}_i| = |Z| + \sum_{i=1}^{k} |G : C_G(g_i)|,$$

as claimed. $\square$