FINAL EXAM SOLUTIONS MATH 701 FALL 2023

Write your answers as **legibly** as you can on the blank sheets of paper provided. Write **complete** answers in **complete sentences**. Make sure that your **notation is defined**!

Use only **one side** of each sheet; start each problem on a **new sheet** of paper; and be sure to number your pages. Put your solution to problem 1 first, and then your solution to number 2, etc.

If some problem is incorrect, then give a counterexample and/or supply the missing hypothesis and prove the resulting statement. If some problem is vague, then be sure to explain your interpretation of the problem.

You should KEEP this piece of paper.
Take a picture of your exam (for your records) just before you turn the exam in. I will e-mail your grade and my comments to you. I will keep your exam. **Fold your exam in half** before you turn it in.

The exam is worth 100 points. There are nine problems.

1. (11 points) **Prove that there is no finite group G with $G/Z(G)$ has exactly 143 elements.**

   Suppose such a group exists. We will obtain a contradiction.

   We first observe that $G/Z(G)$ is cyclic. Let n_{11} and n_{13} be the number of Sylow 11 and Sylow 13 subgroups of $G/Z(G)$, respectively. The Sylow Theorems guarantee that $n_{11} \equiv 1 \mod 11$, $n_{11}|13$, $n_{13} \equiv 1 \mod 13$, and $n_{13}|11$. Thus, $n_{13} = n_{11} = 1$. Let H be the Sylow subgroup of $G/Z(G)$ of order 11 and K be the Sylow subgroup of $G/Z(G)$ of order 13. Each of these subgroups is a normal subgroup of $G/Z(G)$; each of these subgroups is cyclic; the intersection of the two subgroups is the identity element of $G/Z(G)$, elements of H commute with elements of K:
   $$(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{\text{id}\}.$$
   We conclude that $G/Z(G)$ is a cyclic group. Let g be an element of G so that the coset $g * Z(G)$ generates $G/Z(G)$. It follows that every element of G has the form $g^i z$ for some i and some $z \in Z(G)$. It follows further that G is Abelian. Thus $Z(G) = G$. We have reached a contradiction. It is not possible for $G/Z(G)$ to have exactly 143 elements and at the same time to have exactly 1 element.

2. (11 points) **Let U be the multiplicative group of complex numbers of modulus 1, let $\mathbb{R}$ be the additive group of real numbers, and let $\mathbb{Z}$ be the additive group of integers. Prove that $U \cong \mathbb{R}/\mathbb{Z}$.**

   Let $\phi : \mathbb{R} \to U$ be the function $\phi(r) = e^{2\pi r}$. Observe that ϕ is a group homomorphism; ϕ is surjective; and the kernel of ϕ is $\mathbb{Z}$. Apply the First Isomorphism Theorem.

3. (11 points) **Let G_1 and G_2 be Abelian groups and let $\alpha : G_1 \to G_2$ and $\beta : G_2 \to G_1$ be group homomorphisms so that $\beta\alpha(g) = g$, for all $g \in G_1$. Prove that G_2 is isomorphic to $\operatorname{im}\alpha \oplus \ker\beta$.**

   We let + denote the operation in each group G_i. Consider the homomorphism

   $$\phi : \operatorname{im}\alpha \oplus \ker\beta \to G_2,$$

   which is given by $\phi(x, y) = x + y$. The map makes sense because $\operatorname{im}\alpha$ and $\ker\beta$ are both subgroups of G_2. We show that ϕ is a bijection by showing $\operatorname{im}\alpha \cap \ker\beta = \{0\}$ and $\operatorname{im}\alpha + \ker\beta = G_2$.

   $\operatorname{im}\alpha \cap \ker\beta = \{0\}$: If $g_2 \in \operatorname{im}\alpha \cap \ker\beta$, then $g_2 = \alpha g_1$ for some $g_1 \in G_1$ and $0 = \beta(g_2) = (\beta\circ\alpha)(g_1) = g_1$; hence, $g_2 = \alpha(g_1) = 0$.

   $\operatorname{im}\alpha + \ker\beta = G_2$: If $g_2 \in G_2$, then $g_2 = (\alpha\circ\beta)(g_2) + (g_2 - (\alpha\circ\beta)(g_2))$, with $(\alpha\circ\beta)(g_2) \in \operatorname{im}\alpha$ and $(g_2 - (\alpha\circ\beta)(g_2)) \in \ker\beta$.

4. (11 points) **Consider $\alpha : \frac{\mathbb{Z}}{\langle 9\rangle} \to \frac{\mathbb{Z}}{\langle 18\rangle}$, given by $\bar{n} \mapsto \bar{n}$, and $\beta : \frac{\mathbb{Z}}{\langle 18\rangle} \to \frac{\mathbb{Z}}{\langle 9\rangle}$ given by $\bar{n} \mapsto \bar{n}$. Is α a group homomorphism? Is β a group homomorphism? Explain.**

   Consider the subgroups $\langle 18\rangle \subseteq \langle 9\rangle$ of $\mathbb{Z}$. It follows that $\frac{\langle 9\rangle}{\langle 18\rangle}$ is a subgroup of $\frac{\mathbb{Z}}{\langle 18\rangle}$. Thus, β is a group homomorphism. Indeed β is the natural quotient map

   $$\frac{\mathbb{Z}}{\langle 18\rangle} \to \frac{\frac{\mathbb{Z}}{\langle 18\rangle}}{\frac{\langle 9\rangle}{\langle 18\rangle}}$$

   followed by the isomorphism of the Second Isomorphism Theorem

   $$\frac{\frac{\mathbb{Z}}{\langle 18\rangle}}{\frac{\langle 9\rangle}{\langle 18\rangle}} \xrightarrow{\cong} \frac{\mathbb{Z}}{\langle 9\rangle}.$$

   Thus β is a group homomorphism.

   On the other hand, "α" is not a function $\bar{0} = \bar{9}$ in $\frac{\mathbb{Z}}{\langle 9\rangle}$; but "$\alpha$"$(\bar{0}) = \bar{0}$,"$\alpha$"$(\bar{9}) = \bar{9}$, and $\bar{0} \neq \bar{9}$ in $\frac{\mathbb{Z}}{\langle 18\rangle}$. So, α is not a group homomorphism.

5. (11 points) **Let R be a commutative ring. Let I be a prime ideal of R such that R/I satisfies the descending chain condition on ideals. Prove that R/I is a field.**

   It suffices to show that if D is a (commutative) domain which satisfies the descending chain condition on ideals, then D is a field. Let d be a non-zero element of D. Observe that

   $$(d) \supseteq (d^2) \supseteq (d^3) \supseteq \dots$$

   is a descending chain of ideals of D. It follows that there exists an index i with $(d^i) = (d^{i+1})$. In particular, $d^i = \alpha d^{i+1}$ for some α in D. Thus $d^i(1 - \alpha d) = 0$. The element d^i is a non-zero element of the domain D; thus, $1 = \alpha d$ and d is a unit. Every non-zero element of D is a unit; hence D is a domain.

6. (11 points) **Let $R = \mathbb{Z}[x]$. Give three prime ideals of R that contain the ideal $(6, 2x)$.**

   The ideals $(3, x)$, $(2, x)$, and (2) are prime ideals of R which contain $(6, 2x)$.

7. (11 points) **Prove the following form of the Chinese Remainder Theorem. Let R be a commutative ring and suppose that I and J are ideals of R such that $I + J = R$. Then $\frac{R}{I\cap J}$ and $\frac{R}{I} \oplus \frac{R}{J}$ are isomorphic rings. (The direct sum of two rings is a ring; the multiplication takes place coordinate-wise.)**

   Define the the ring homomorphism $\phi : R \to \frac{R}{I} \oplus \frac{R}{J}$ by $\phi(r) = (\bar{r}, \bar{r})$. We are told that there exist elements $i \in I$ and $j \in J$ with $i + j = 1$. Thus, $\phi(1 - i) = (\bar{1}, \bar{0})$ and $\phi(1 - j) = (\bar{0}, \bar{1})$. The homomorphism ϕ is surjective. The kernel of ϕ is $I \cap J$. Apply The First Isomorphism Theorem.

8. (12 points) **Let R be a commutative ring. For $x \in R$, let $A(x) = \{r \in R \mid xr = 0\}$. Suppose $\theta \in R$ has the property that $A(\theta)$ is not properly contained in $A(x)$ for any $x \in R$. Prove the $A(\theta)$ is a prime ideal of R.**

   This problem should state that x and θ are non-zero elements of R.

   Suppose r_1 and r_2 are in R with $r_1r_2 \in A(\theta)$. Suppose further that $r_1 \notin A(\theta)$. In particular, $r_1\theta \neq 0$ and $A(\theta) \subseteq A(r_1\theta)$. It is clear that $r_2 \in A(r_1\theta)$. The hypothesis that $A(\theta)$ is not properly contained in $A(x)$ for any $x \in R$ ensures that r_2 is an element of $A(\theta)$ and the proof is complete.

9. (11 points) **Let p be the smallest prime dividing the order of the finite group G. Prove that any subgroup of index p in G is a normal subgroup.**

   Let H be a subgroup of G of index p and let S be the set of left cosets of H in G. Notice that S has p elements. Let G act on S by left translation. That is, g_1 sends gH to g_1gH. It follows that there is a group homomorphism $\phi : G \to \text{Sym}(S)$. The kernel of ϕ is a normal subgroup of G and $\frac{G}{\ker\phi}$ is isomorphic to a subgroup of $\text{Sym}(S)$. If follows that $|\frac{G}{\ker\phi}|$ divides $p!$. (In particular, the prime factorization of $|\frac{G}{\ker\phi}|$ involves primes of size p and smaller and p can be involved at most once.)

   On the other hand, $|\frac{G}{\ker\phi}|$ divides $|G|$; hence the smallest prime that can divide $|\frac{G}{\ker\phi}|$ is p.

   At this point we know that $|\frac{G}{\ker\phi}|$ is one or p.

   Observe that $\ker\phi \subseteq H$. Indeed, if $g \in \ker\phi$, then $g \cdot \text{id}\, H = \text{id}\, H$; hence $g \in H$. (One consequence of this is that $|\frac{G}{\ker\phi}|$ is not equal to one; hence $|\frac{G}{\ker\phi}| = p$.)

   We have $\ker\phi \subseteq H \subseteq G$ with $[G : \ker\phi] = [G : H]$. We conclude that $H = \ker\phi$, which is a normal subgroup of G.