MAT 511 **Final Exam** Name SOLUTIONS
12/18/13
250 points

1.(25) Suppose $f\colon G \longrightarrow H$ and $g\colon G \longrightarrow H$ are homomorphisms.

(a) Show that the set $\{x \in G \mid f(x) = g(x)\}$ is a subgroup of G. Let $K = \{x \in G \mid f(x) = g(x)\}$

Since f and g are homomorphisms, $f(e_G) = e_H$ and $g(e_G) = e_H$, so $f(e_G) = g(e_G)$. Thus $e_G \in K$. Let $x, y \in K$. Then $f(x) = g(x)$ and $f(y) = g(y)$. Then $f(xy) = f(x)f(y) = g(x)g(y) = g(xy)$, so $xy \in K$. Also $f(x^{-1}) = f(x)^{-1} = g(x)^{-1} = g(x^{-1})$, so $x^{-1} \in K$. Thus $\leq G$.

(b) Suppose $S \subseteq G$ satisfies $\langle S \rangle = G$. Prove: if $f(x) = g(x)$ for all $x \in S$, then $f = g$.

By hypothesis $S \subseteq K$ (notation from part (a)). Since $K \leq G$, $\langle S \rangle \subseteq K$. Then $G \subseteq K$ so $f(x) = g(x)$ for all $x \in G$. Thus $f = g$.

2.(25) (a) Prove: if G is a finite simple group, and $\varphi\colon G \longrightarrow G$ is a nontrivial homomorphism, then φ is an automorphism.

$\ker(\varphi) \trianglelefteq G$ and G is simple, so $\ker(\varphi) = 1$ or G. Since φ is nontrivial, $\ker(\varphi) \neq G$. Then $\ker(\varphi) = 1$. Then φ is injective. Then $|\varphi(G)| = |G|$, so $\varphi(G) = G$ since $|G| < \infty$ and $\varphi(G) \leq G$. Thus φ is surjective. Therefore φ is an automorphism.

(b) Let $\varphi\colon G \longrightarrow H$ be a homomorphism of finite groups. Prove $|\operatorname{im}(\varphi)|$ divides both $|G|$ and $|H|$.

$\operatorname{im}(\varphi) \cong G/\ker(\varphi)$ by the first isomorphism theorem. Then $|\operatorname{im}(\varphi)| = |G : \ker(\varphi)|$, and $|G| = |G : \ker(\varphi)|\,|\ker(\varphi)|$ so $|\operatorname{im}(\varphi)|$ divides $|G|$. Also $\operatorname{im}(\varphi) \leq H$, so $|\operatorname{im}(\varphi)|$ divides $|H|$ by Lagrange's Theorem.

3.(20) Let R be a commutative ring and let a be an element of R. Prove that $I_a := \{x \in R \mid ax = 0\}$ is an ideal in R.

Since $a \cdot 0 = 0$, $0 \in I_a$. Let $x, y \in I_a$. Then $ax = 0$ and $ay = 0$. Then $a(x-y) = ax - ay = 0 - 0 = 0$. Thus $x - y \in I_a$. Then I_a is an additive subgp. Let $x \in I_a$ and $r \in R$. Then $ax = 0$ so $a(xr) = (ax)r = 0 \cdot r = 0$, so $xr \in I_a$. Since R is commutative, $rx \in I_a$. Thus I_a is a (2-sided) ideal in R.

4.(20) Suppose G is a group, and H is a subgroup of G. Prove that the number of conjugates H^x, $x \in G$, of H in G divides the index $|G : \underset{H}{\cancel{\mathbf{N}_G(H)}}|$ of the normalizer $\underset{H}{\cancel{\mathbf{N}_G(H)}}$ in G.

G acts on the set Ω of subgroups of G by conjugation. The orbit of H is $\{H^x \mid x \in G\}$ and the stabilizer of H is

$\{x \in G \mid H^x = H\} = N_G(H)$. Then by the orbit-stabilizer theorem, $|\{H^x \mid x \in G\}| = |G : N_G(H)|$.

Since $H \leq N_G(H)$, $|G : H| = |G : N_G(H)|\,|N_G(H) : H|$

$= |\{H^x \mid x \in G\}| \cdot |N_G(H) : H|$.

Thus $|\{H^x \mid x \in G\}|$ divides $|G : H|$.

5.(25) Suppose the group G acts on the left on the set Ω.

(a) Let $x \in \Omega$, $g \in G$ and $y = g \cdot x$. Show $G_y = (G_x)^g$.

Let $h \in G$. Then $h \cdot y = y \iff h \cdot (g \cdot x) = g \cdot x \iff (hg) \cdot x = g \cdot x \iff g^{-1} \cdot ((hg) \cdot x) = g^{-1} \cdot (g \cdot x) \iff (g^{-1}hg) \cdot x = (g^{-1}g) \cdot x \iff (g^{-1}hg) \cdot x = x$. Thus $h \in G_y \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1} = (G_x)^g$. Thus $G_y = (G_x)^g$

(b) Using (a), show, if G is abelian and the action is faithful and transitive, then $G_x = 1$.

If G is abelian then $G_y = (G_x)^g = G_x$, and since the action is transitive, for every $y \in \Omega$, $y = g \cdot x$ for some $g \in G$, so $G_y = G_x$ for all $y \in \Omega$. If $h \in G_x$, then $h \cdot y = y$ for all $y \in \Omega$, which implies $h = 1$ since the action is faithful.

6.(35) Suppose G is a group of order 1225. Show G is abelian. List all possibilities for G, up to isomorphism.

$|G| = 1225 = 5^2 \cdot 7^2$. $n_7 \equiv 1 \bmod 7$ and $n_7 \mid 5^2 = 25$. Then $n_7 = 1$ since $8, 15$. do not divide 25. Then $\exists\, K \trianglelefteq G$ with $|K| = 7^2$. (K is the unique Sylow 7-subgp.) Also $n_5 \equiv 1 \bmod 5$, and $n_5 \mid 7^2 = 49$. Since $6, 11, 16, 21, 26$ do not divide 49, $n_5 = 1$. Then $\exists\, H \trianglelefteq G$ with $|H| = 5^2$. (H is the unique Sylow 5-subgp.). Now $K \cap H = 1$ since $|K \cap H|$ divides both $|K|$ and $|H|$, and $|K|$ and $|H|$ are relatively prime. Then $|KH| = |K||H| / |K \cap H| = |K||H| = 5^2 \cdot 7^2 = |G|$, hence $KH = G$. Then $G \cong K \times H$. K and H are abelian since any group of order p^2, p prime is abelian. Thus G is abelian. By the classification of finite abelian groups, $G \cong \mathbb{Z}_{25} \oplus \mathbb{Z}_{49} \cong \mathbb{Z}_{1225}$ or $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{49} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{245}$ or $\mathbb{Z}_{25} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_7 \oplus \mathbb{Z}_{175}$ or $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{35} \oplus \mathbb{Z}_{35}$.

7.(35) Recall a group G is metabelian iff there is a normal subgroup N of G such that N and G/N are abelian.

(a) Give an example of a metabelian group that is not abelian.

D_4 is not abelian, but $\langle r \rangle \cong \mathbb{Z}_4$ is abelian and index two in D_4, hence $\langle r \rangle \trianglelefteq D_4$ and $\langle r \rangle \cong \mathbb{Z}_4$ and $D_4/\langle r \rangle \cong \mathbb{Z}_2$ are abelian. Then D_4 is metabelian. (S_3 is another (smaller) example.)

(b) Let $G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$ be the derived series of G.[1] Prove: if $G^{(2)} = 1$ then G is metabelian.

$G^{(1)} = [G, G]$ is normal in G, and $G/G^{(1)}$ is abelian. $[G^{(1)}, G^{(1)}] = G^{(2)} = 1$ by hypothesis, so $G^{(1)}$ is abelian. Then G is metabelian.

(c) Suppose $\varphi\colon G \longrightarrow H$ is a surjective homomorphism, with H a metabelian group. Prove there is a surjective homomorphism $\bar{\varphi}\colon G/G^{(2)} \longrightarrow H$ satisfying $\bar{\varphi}(xG^{(2)}) = \varphi(x)$.

Let $N \trianglelefteq H$ with H/N abelian and N abelian. Since H/N is abelian, $H^{(1)} = [H,H] \subseteq N$. Since N is abelian, $[N,N] = 1$. Then $H^{(2)} = [H^{(1)}, H^{(1)}] \subseteq [N,N] = 1$, so $H^{(2)} = 1$. Since $\varphi(G^{(2)}) \subseteq H^{(2)}$ (as is easily shown), $\varphi(G^{(2)}) = 1$, so $G^{(2)} \subseteq \ker(\varphi)$. Then, by a result from lecture (HW #?), φ induces a well-defined homomorphism $\bar{\varphi} : G/G^{(2)} \longrightarrow H$, given by $\bar{\varphi}(xG^{(2)}) = \varphi(x)$. Since φ is surjective, $\bar{\varphi}$ is surjective.

[1] $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$ for $k \geq 1$.

8.(20) Let $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ be a short exact sequence of abelian groups, with C isomorphic to $\mathbb{Z}$. Prove $B \cong A \times C$.

Since $C \cong \mathbb{Z}$, C is a free $\mathbb{Z}$-module (or free abelian group). Then we can construct $\sigma : C \longrightarrow B$ satisfying $\beta \circ \sigma = id_C$, as follows: Write $C = \langle c \rangle$ (so c corresponds to $1 \in \mathbb{Z}$). Since β is onto, $c = \beta(b)$ for some $b \in B$. Define $\sigma(c) = b$, and extend to a well-defined homom. $\sigma : C \longrightarrow B$, $\sigma(c^n) = b^n$. Then $\beta \circ \sigma(c) = c$, so $\beta \circ c = id_C$ by Problem 1(b). Let $K = \operatorname{Im}(\alpha)$ and $H = \operatorname{Im}(\sigma)$. Then $K \trianglelefteq B$, $H \trianglelefteq B$. Claim $K \cap H = 0$. Indeed, if $x \in K \cap H$ then $x = \sigma(y)$ for some (over)

9.(25) A *simple* ring is a ring with no nonzero proper 2-sided ideals. The *center* of a ring R is $Z(R) = \{x \in R \mid rx = xr \text{ for all } r \in R\}$. Show that the center of a simple ring with 1 is a field.

First $Z(R)$ is a subring: $r \cdot 0 = 0 = 0 \cdot r$ $\forall r \in R$ so $0 \in Z(R)$; $rx = xr$ and $ry = yr$ for all $r \in R \Longrightarrow r(x - y) = rx - ry = xr - yr = (x-y)r$, so $x, y \in Z(R) \Longrightarrow x - y \in Z(R)$. Also $r(xy) = (rx)y = (xr)y = x(ry) = x(yr) = (xy)r$, so $x, y \in Z(R) \Longrightarrow xy \in Z(R)$. Clearly $Z(R)$ is commutative. It remains to show every $x \in Z(R)$, $x \neq 0$, has a multiplicative inverse in $Z(R)$. Let $x \in Z(R)$, $x \neq 0$. Consider xR. Since $x \in Z(R)$, $xR = Rx$, so xR is a 2-sided ideal. Since $x = x \cdot 1 \in xR$, $xR \neq 0$. (over)

10.(20) Let R be a ring and M a right R-module. For (right) submodules I and J of M, let $(I : J) = \{r \in R \mid Jr \subseteq I\}$. Prove that $(I : J)$ is the annihilator of the submodule $(I + J)/I$ of the module M/I.

Suppose $r \in (I:J)$. Then $Jr \subseteq I$. Then, if $y \in I + J$, $(y + I)r = yr + I$, and, writing $y = u + v$ with $u \in I, v \in J$, $yr = ur + vr$, and $ur \in I$ because I is a right ideal, and $vr \in I$ since $r \in (I:J)$. Then $yr \in I$ so $yr + I = I$, and $(y + I)r = I = 0_{R/I}$. Thus $r \in \operatorname{ann}(I+J/I)$. Conversely, let $r \in \operatorname{ann}(I+J/I)$, and let $y \in J$. Then $(y + I)r = yr + I = 0_{M/I} = I$, so $yr \in I$. Then $r \in (I:J)$. Thus $(I:J) = \operatorname{ann}(I+J/I)$.

(8) cont'd. $y \in C$ and $\beta(x) = 0$ since $x \in \text{im}(\alpha) = \ker(\beta)$

Then $y = \beta \circ \sigma(y) = \beta(x) = 0$, so $x = \sigma(y) = \sigma(0) = 0$.

Thus $K \cap H = 0$. Claim $K + H = B$. Indeed,
if $x \in B$, then $x = (x - \sigma(\beta(x))) + \sigma(\beta(x))$,
$\sigma(\beta(x)) \in \text{im}(\sigma) = H$, and, since $\beta(x - \sigma(\beta(x)))$
$= \beta(x) - (\beta \circ \sigma)(\beta(x)) = \beta(x) - \beta(x) = 0$,
$x - \sigma(\beta(x)) \in \ker(\beta) = \text{im}(\alpha) = K$. Thus $K + H = B$.
Then $B \cong K \oplus H$. Since $\beta \circ \sigma = id_C$, σ is
injective, and α is injective, so $H \cong C$ and $K \cong A$.
Thus $B \cong A \times C$ (or, better, $A \oplus C$).

---

(9) (cont'd) Then since R is simple, $xR = R$. Then $\exists\, y \in R$
with $xy = 1$, and since $x \in Z(R)$, $yx = 1$ as well.
Claim $y \in Z(R)$. Let $r \in R$. Then $yr = (yr) \cdot 1 = (yr)(xy)$
$= y(rx)y = (yx)ry = 1 \cdot ry = ry$. Thus $y \in Z(R)$.
Therefore $Z(R)$ is a field.