MAT 511 **Exam 3** Name SOLUTIONS
11/22/13 (due Wednesday 11/27/13, 11:30 am)
160 points

Rules: You may consult your notes, our text and/or other books, and may discuss the exam with me, but no other outside help (including internet) is permitted. If you have questions, they should be directed to me. No discussion of the exam with other students, even at a superficial level, is permitted. I will hold additional office hours on Monday, 11/25, from 10:00 - 11:00 am and 4:00 - 5:00 pm, and on Tuesday, 11/26, 11:30 am - 12:30 pm, and will respond to email inquiries over the weekend. Hints are available upon request, at no charge.

1.(40) (a) Suppose $|G| = 280$. Show G has a normal Sylow subgroup.

$|G| = 2^3 \cdot 5 \cdot 7$. $n_7 \mid 2^3 \cdot 5$ and $n_7 \equiv 1 \bmod 7 \Rightarrow n_7 = 1, 8$. If $n_7 = 1$, then the unique Sylow 7-subgroup is normal. Suppose $n_7 = 8$. $n_5 \mid 2^3 \cdot 7$ and $n_5 \equiv 1 \bmod 5 \Rightarrow n_5 = 1, 56$. If $n_5 = 1$, the unique Sylow 5-subgroup is normal. Suppose $n_5 = 56$. If $P, Q \in Syl_7(G)$ then $|P| = |Q| = 7$, so $P \cap Q = 1$ if $P \neq Q$. Similarly, if $P, Q \in Syl_5(G)$ with $P \neq Q$, then $P \cap Q = 1$. Since there are 8 Sylow 7- and 56 Sylow 5-subgroups, which have orders 7 and 5, respectively, there are $8 \cdot (7-1) = 48$ elements of order 7 and $56 \cdot (5-1) = 224$ elements of order 5, leaving $280 - 48 - 224 = 8$ elements of order different from 5 and 7. Since there is a Sylow 2-subgp, which has order 8, and all elements of Sylow 2-subgp have 2-power order, these 8 remaining elements must form the unique Sylow 2-subgroup. Thus $n_7 = 8$ and $n_5 = 56 \Rightarrow n_2 = 1$, so, in any case, G has a normal Sylow subgroup. □

(b) Use (a) to show every group of order 280 is solvable.

Lemma 1: If $|G| = 40$, then G is solvable. proof: $|G| = 2^3 \cdot 5$, $n_5 \mid 8$ and $n_5 \equiv 1 \bmod 5 \Rightarrow n_5 = 1$. Then $\exists$ $P \trianglelefteq G$ with $|G/P| = 2^3$. Then G/P is a p-group, hence nilpotent, hence solvable. $|P| = 5$ so P is abelian, hence solvable. Since P and G/P are solvable, G is solvable.

Lemma 2: If $|G| = 56$, then G is solvable. proof: If $n_7 = 1$ then there exists $P \trianglelefteq G$ with $|P| = 7$ and $|G/P| = 2^3$, which implies G is solvable as in the proof of Lemma 1. Otherwise $n_7 = 8$, which implies G has $8 \cdot (7-1) = 48$ elements of order 7, (over)

1(b) (continued) which implies $n_2 = 1$ as in 1(a). Then there exists $P \trianglelefteq G$ with $|P| = 2^3$ and $|G/P| = 7$, which implies G is solvable as before. ②

Now suppose $|G| = 280$. By (a) $\exists$ $P \trianglelefteq G$ with $|P| = 7$, $|G/P| = 40$, or $|P| = 5$, $|G/P| = 56$, or $|P| = 2^3$, $|G/P| = 35$. In the last case, $|G/P| = 35 \implies G/P$ is cyclic, by a theorem from class, since $35 = 5\cdot 7$ and $5 \nmid 7-1$. Then in any case, P and G/P are solvable, hence G is solvable. $\square$

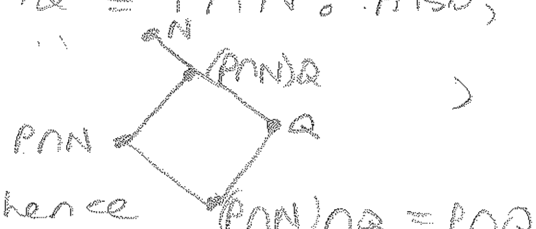
(c) Suppose $|G| = 396$. Show G is not simple.

Hint: Assume G is simple. Show G is isomorphic to a subgroup of S_{12} and that G has an element of order 33, and derive a contradiction.

$|G| = 2^2\cdot 3^2 \cdot 11$. Then $n_{11} \mid 2^2\cdot 3^2$ and $n_{11} \equiv 1 \bmod 11$, which implies $n_{11} = 1$ or 12. Assume G is simple. Then $n_{11} \neq 1$, so $n_{11} = 12$. The group G acts by conjugation on $Syl_{11}(G)$, yielding a homomorphism $G \xrightarrow{\varphi} S_{12}$, since $|Syl_{11}(G)| = 12$. This homomorphism is not trivial, since G acts transitively by Sylow C. Then, since G is simple, $\ker(\varphi) = 1$, so φ is injective. Thus G is isomorphic to a subgroup of S_{12}. Let $P \in Syl_{11}(G)$. Then $|G : N_G(P)| = |Syl_{11}(G)| = 12$, so $|N_G(P)| = |G|/12 = 33$. Since $33 = 3\cdot 11$ and $3 \nmid 11-1 = 10$, $N_G(P)$ is cyclic by a theorem from class. Then G has an element of order 33. But a permutation of order 33 must contain disjoint 3- and 11-cycles, or a 33-cycle, so must move at least 14 letters. Then S_{12} has no elements of order 33. Contradiction. Thus G is not simple. $\square$

2.(30) (a) Suppose G is a finite group and p is a prime divisor of $|G|$. Let n_p denote the number of Sylow p-subgroups of G. Prove: if ~~$|P : P\cap Q| \geq p^e$~~ $|P : P\cap Q| \geq p^e$ for every pair of distinct Sylow p-subgroups P and Q, then $n_p \equiv 1 \bmod p^e$.

Let $P \in Syl_p(G)$. Consider the action of P on $Syl_p(G)$ by conjugation. Since $P^x = P$ for all $x \in P$, $\{P\}$ is an orbit. Let $Q \in Syl_p(G)$ with $Q \neq P$. Let O_Q and P_Q denote the orbit and stabilizer of Q, respectively. Then $|O_Q| = |P : P_Q|$. Let $N = N_G(Q)$. Then $P_Q = P \cap N$. Since $Q \subseteq N$, $P\cap Q \subseteq P \cap N$. Also, from the diagram



$P\cap N / P\cap Q$ is isomorphic to a subgroup of N/Q, hence $p \nmid |P\cap N : P\cap Q|$, which implies (over)

2(a) (continued), $|P\cap N : P \cap Q| = 1$, hence $P_Q = P\cap N = P \cap Q$. Then $|\mathcal{O}_Q| = |P : P_Q| = |P : P\cap Q| \geq p^e$. Since $|\mathcal{O}_Q|$ is also a p-power, $p^e \mid |\mathcal{O}_Q|$. Thus $p^e \mid |\mathcal{O}_Q|$ for all $Q \neq P$. Since the orbits partition $\mathrm{Syl}_p(G)$, $n_p \equiv 1 \bmod p^e$. $\square$

(b) Suppose G is a simple group of order 60. Prove G is isomorphic to a subgroup of S_5. (Then it follows from Exam 2 that G is isomorphic to A_5.)

Hint: Show G has a subgroup of index 5, by considering Sylow 2-subgroups. Use (a) (in the contrapositive) to show, if $n_2 = 15$, then some two distinct Sylow 2-subgroups must have a nontrivial intersection D, and then consider $\mathbf{N}_G(D)$.

$|G| = 2^2 \cdot 3 \cdot 5$. Then $n_2 \mid 3\cdot 5$ and $n_2 \equiv 1 \bmod 2$, so $n_2 = 1, 3, 5,$ or 15. $n_2 \neq 1$ since G is simple. If $n_2 = 3$, then G acts on the 3-element set $\mathrm{Syl}_2(G)$, and the action is nontrivial, hence faithful since G is simple, which implies $|G|$ divides $3!$, a contradiction. If $n_2 = 5$, then G acts faithfully on the 5-element set $\mathrm{Syl}_2(G)$. Suppose $n_2 = 15$. Since $15 \not\equiv 1 \bmod 2^2$, there are distinct $P, Q \in \mathrm{Syl}_2(G)$ with $|P : P\cap Q| < 2^2$. (go to p. 6)

3.(30) Suppose G is a group having a subgroup K of index two, and an element $s \in G - K$ of order two.

(a) Prove G is isomorphic to a semidirect product $K \rtimes_\theta \mathbb{Z}_2$.

Let $H = \langle s \rangle$. Then $H \cong \mathbb{Z}_2$. Since $s \notin K$, $K \cap H = 1$. Since K has index 2 and $KH \neq K$, $KH = G$. Since K has index 2, $K \trianglelefteq G$. Then $G \cong K \rtimes_\theta H$ by a theorem from class, where $\theta : H \to \mathrm{Aut}(K)$ is given by $k^{\theta(h)} = k^h$ for $k \in K, h \in H$.

(b) Show every element of $G - K$ has order two if and only if $k^s = k^{-1}$ for all $k \in K$. Deduce K is abelian in this case.

By (a) every $g \in G$ can be written as $g = kh$, $k \in K$, $h \in H$. Then $g \in G - K \implies g = ks$. Then $g^2 = 1 \iff (ks)(ks) = 1 \iff k \cdot k^s = 1$ since $s^{-1} = s$, $\iff k^s = k^{-1}$.

Since conjugation by s is a homomorphism, $k_1 k_2 = (k_1^{-1})^{-1}(k_2^{-1})^{-1} = (k_1^{-1}k_2^{-1})^{-1} = k_2 k_1$ $\forall\, k_1, k_2 \in K$. Thus K is abelian.

(c) Suppose $K = \langle r \rangle$ and $r^s = r^{-1}$. (In this case G is a *dihedral group.*) Prove $\mathbf{Z}(G) = 1$ if $|r|$ is odd or infinite, and $\mathbf{Z}(G) = \langle r^m \rangle$ if $|r| = 2m$. Deduce G is nilpotent if and only if $|r| = 2^n$ for some $n \geq 1$.

Suppose $g \in Z(G)$. Write $g = r^m s^\ell$. Then $g^s = g$, so $(r^m s^\ell)^s = r^m s^\ell$. But $(r^m s^\ell)^s = (r^m)^s (s^\ell)^s = (r^s)^m s^\ell = r^{-m} s^\ell$. This implies $r^{-m} = r^m$, so $r^{2m} = 1$. (go to page 6)

4.(25) (a) Let G be a group. Prove G is solvable if and only if $G^{(n)} = 1$ for some n, where $\{G^{(k)} \mid k \geq 0\}$ is the derived series of G.

Suppose $G^{(n)} = 1$. Then $1 = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$ is a subnormal series in G, and $G^{(k)}/G^{(k+1)} = G^{(k)}/[G^{(k)}, G^{(k)}]$ is abelian. Hence G is solvable.

Suppose G is solvable. Let $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = G$ be a subnormal series with N_k/N_{k-1} abelian for all k. Then, since $G/N_{n-1} = N_n/N_{n-1}$ is abelian, $[G,G] = G^{(1)} \subseteq N_{n-1}$. Assume inductively that $G^{(k)} \subseteq N_{n-k}$. Since N_{n-k}/N_{n-k-1} is abelian $G^{(k+1)} = [G^{(k)}, G^{(k)}] \subseteq N_{n-k-1}$. It follows that $G^{(k)} \subseteq N_{n-k}$ for all k, by induction. Then $G^{(n)} \subseteq N_0 = 1$. □

(b) Use (a) to prove that any subgroup (not necessarily normal) and any quotient group of a solvable group is solvable.

Let $H \leq G$. Then $[H,H] \subseteq [G,G]$, and, for every k, $H^{(k)} \subseteq G^{(k)} \implies H^{(k+1)} = [H^{(k)}, H^{(k)}] \subseteq [G^{(k)}, G^{(k)}] \subseteq G^{(k+1)}$. Then $H^{(k)} \subseteq G^{(k)}$ for all k, by induction. Suppose G is solvable. Then $G^{(n)} = 1$ for some n. Since $H^{(n)} \subseteq G^{(n)}$, $H^{(n)} = 1$. Then H is solvable.

Let $N \trianglelefteq G$. Let $\varphi : G \longrightarrow G/N$ be the canonical (surjective) homomorphism. Then $\varphi([G,G]) = [\varphi(G), \varphi(G)]$. As above, this implies $\varphi(G^{(k)}) = (\varphi(G))^{(k)}$ for all k, by induction. Suppose G is solvable. Then $G^{(n)} = 1$ for some n. Then $(\varphi(G))^{(n)} = 1$. Then $\varphi(G) = G/N$ is solvable. □

Note: $\varphi(G^{(k)}) = NG^{(k)}/N$.

5.(15) Definition: A group G is *residually nilpotent* if, for every $x \in G$ with $x \neq 1$, there exists a nilpotent group H and a homomorphism $\varphi \colon G \longrightarrow H$ with $\varphi(x) \neq 1_H$. Prove G is residually nilpotent if and only if $\bigcap_{k \geq 0} G^k = 1$, where $\{G^k \mid k \geq 0\}$ is the lower (descending) central series of G.

Suppose G is residually nilpotent. Let $x \in \bigcap_{k \geq 0} G^k$. Suppose $x \neq 1$. Then $\exists\ \varphi : G \longrightarrow H$ with H nilpotent and $\varphi(x) \neq 1$. Claim $\varphi(G^k) \subseteq H^k$ for all k. This holds trivially for $k = 0$. Suppose inductively that $\varphi(G^k) \subseteq H^k$. Then $\varphi(G^{k+1}) = \varphi([G, G^k]) = [\varphi(G), \varphi(G^k)] \subseteq [H, H^k] = H^{k+1}$. The claim follows by induction. Since H is nilpotent, $H^n = 1$ for some n, by HW#7.3(b). Since $\varphi(G^n) \subseteq H^n$, $\varphi(G^n) = 1$. Since $x \in \bigcap_{k \geq 0} G^k$, $x \in G^n$. Then $\varphi(x) \in \varphi(G^n) = 1$, so $\varphi(x) = 1$. This is a contradiction. Thus $x = 1$. Then $\bigcap_{k \geq 0} G^k = 1$. Go to page 7 for the converse.

6.(20) Let S and T be rings. The abelian group $S \oplus T$, with product defined by $(x,y)(u,v) = (xu, yv)$, is a ring. (Here the product xu is computed in S, and yv in T.)

Let I be a right ideal of a ring R, and suppose there exists $e \in I$ such that $e \neq 0$ and $e^2 = e$. (Such an element is called an *idempotent*.) Let $J = \{x \in I \mid ex = 0\}$.

(a) Prove J is a right ideal of R.

Let $x, y \in J$. Then $x-y \in I$ and $e(x-y) = ex - ey = 0-0 = 0$. Since $0 \in I$ and $e \cdot 0 = 0$, $0 \in J$. Thus J is an additive subgroup. Let $r \in R$. Then $xr \in I$, and $e(xr) = (ex)r = 0 \cdot r = 0$, so $xr \in J$. Thus J is a right ideal of R.

(b) Prove $I = eI \oplus J$ as ~~rings~~. right R-modules.

Hint: Prove the direct sum decomposition of the underlying abelian groups, and show that the group isomorphism is a ~~ring~~ right R-module homomorphism.

I is a subring of R because it's an additive subgroup and is closed under multiplication. Let $x \in I$. Let $y = x - ex$. Then $x = ex + y$, and $ex \in eI$. Claim $y \in J$. Indeed, since $e \in I$, $ex \in I$ so $x - ex \in I$. Moreover, $e(x-ex) = ex - e^2x = ex - ex = 0$. Thus $y \in J$. Then $I = eI + J$. Suppose $x \in eI \cap J$. Write $x = ex'$ with $x' \in I$. Then, since $x \in J$, $0 = ex = e^2x' = ex' = x$. Then $eI \cap J = 0$. Then $I = eI \oplus J$ as abelian groups.

The isomorphism is given by the map $\varphi : eI \oplus J \to I$ given by $\varphi((x,y)) = x+y$. Then, if $(x,y) \in eI \oplus J$ and $r \in R$, we have $\varphi((x,y)r) = \varphi((xr, yr)) = xr + yr = (x+y)r = \varphi((x,y))r$. Thus φ is an isomorphism of right R-modules.

2(b) (continued). Then $|P : P \cap Q|$ must equal 2. Let $D = P \cap Q$ and $N = N_G(D)$. Since $|P| = |Q| = 2^2$, P and Q are abelian. Then $P \leq N$ and $Q \leq N$. Then $n_2(N) \geq 2$, and, since $n_2(N) \equiv 1 \bmod 2$, $n_2(N) \geq 3$. Also, since $P \in Syl_2(G)$ and $P \leq N$, $P \in Syl_2(N)$. Then $n_2(N) \mid |N : P|$, so $|N| \geq 2^2 \cdot 3 = 12$. Then $|G : N| = 5$ or $|G : N| = 1$. But $|G : N| \neq 1$ else $N = G$ and $D \trianglelefteq G$, not possible since G is simple and $D \neq 1$. Thus $|G : N| = 5$, and G acts on the 5-element set G/N by left multiplication. Then, in any case, G acts nontrivially on a 5-element set. Since G is simple, the resulting homomorphism $\varphi : G \to S_5$ is injective, so G is isomorphic to a subgroup of S_5. (Hence $G \cong A_5$.)

3(b) (continued). Then $m = 0$ if $|r| = \infty$, and $n \mid 2m$ if $|r| = n < \infty$. If n is odd this implies $k = 0$. If n is even, then we can conclude $m = 0$ or $n = 2m$, since assume without loss that $0 \leq m < n$. Claim $\ell = 0$, so that $g = 1$ if $|r| = \infty$ or $|r|$ is odd, and $g = 1$ or r^m if $|r| = 2m$. Suppose $\ell \neq 0$. Then without loss $\ell = 1$ (since $|s| = 2$). Then $g = s$ or $g = r^m s$. But $rs \neq sr$ (unless $|r| = 2$), since $sr = r^{-1}s \neq rs$ unless $r = r^{-1}$, so $g \neq s$, and $r \cdot r^m s \neq r^m sr$ (unless $m = 1$), because $r^m sr = r^m r^{-1} s = r^{m-1} s$, so $r \cdot r^m s = r^m sr \iff r^{m+1} = r^{m-1} \iff r^{2m+2} = r^{2m} \iff r^2 = 1$.

Thus, if $|r| = \infty$ or $|r|$ is odd, $Z(G) = 1$, and, if $|r|$ is even and $\neq 2$, $Z(G) = \langle r^m \rangle$ where $n = 2m$. (If $|r| = 2$ then $Z(G) = G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.) go to page 7

3(c) continued (from p. 6) Now suppose G is nilpotent. Then $Z(G) \neq 1$, so $|r| = 2m$ is even, and $Z(G) = \langle r^m \rangle$. Let $\bar{G} = G/Z(G) = G/\langle r^m \rangle$, and let $\bar{r}$ and $\bar{s}$ be the images of r and s in $\bar{G}$. Then $\bar{K} = K/\langle r^m \rangle$ is normal in $\bar{G}$, $\bar{K} = \langle \bar{r} \rangle$, and $|\bar{r}| = m$, $\bar{s} \in \bar{G} - \bar{K}$ has order 2, and $\bar{r}^{\bar{s}} = \bar{r}^{-1}$. Since $|\bar{G}| < |G|$ we can assume inductively that $m = |\bar{r}|$ is a power of 2, implying $|r| = 2m$ is a power of two. Conversely, suppose $|r| = 2^n$. Let $N_0 = 1$, $N_1 = \langle r^{2^{n-1}} \rangle$, $N_2 = \langle r^{2^{n-2}} \rangle$, $\ldots$, $N_k = \langle r^{2^{n-k}} \rangle$, $\ldots$, $N_{n-1} = \langle r^2 \rangle$. Then $N_k \trianglelefteq G$, since $(r^i)^r = r^i$ and $(r^i)^s = r^{-i}$ for all i. In G/N_k, $|\bar{r}| = 2^{n-k}$, so $Z(G/N_k) = \langle \bar{r}^{2^{n-k-1}} \rangle = N_{k+1}/N_k$, for $k < n-1$. In G/N_{n-1}, $|\bar{r}| = 2$, so $Z(G/N_{n-1}) = G/N_{n-1} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Then $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{n-1} \trianglelefteq G$ is the upper central series in G, hence G is nilpotent.

---

5 (continued) Suppose $\bigcap_{k \geq 0} G^k = 1$. Let $x \in G$, $x \neq 1$. Then $x \notin G^n$ for some n. G^n is a characteristic subgroup of G, and G/G^n is nilpotent, since $(G/G^n)^n = G^n/G^n = 1$, and $\varphi : G \longrightarrow G/G^n$ satisfies $\varphi(x) \neq 1$. Thus G is residually nilpotent.