MCS 314 Exam 2 Solutions

1. (10 pts) Let $n \in \mathbb{Z}^{\geq 5}$. Show that the only normal subgroups of S_n are $\{()\}$, A_n, and S_n.

   Hint: Use that if H and K are both normal subgroups in G, then $H \cap K$ is normal in G, and in H and K as well.

   It is clear that $\{()\}$ and S_n are normal subgroups of S_n. We showed in class that $A_n \trianglelefteq S_n$. Let $H \trianglelefteq S_n$. We will show that H is one of the three normal subgroups already listed.

   Since H and A_n are both normal in S_n, so is $H \cap A_n$.Hence $H \cap A_n$ is also normal in A_n. We showed in class that A_n is a simple group for $n \geq 5$. Hence $H \cap A_n$ is either $\{()\}$ or A_n.

   Suppose $H \cap A_n = A_n$. Then $A_n \leq H$. One possibility is that $H = A_n$. If not, then $H \lneq A_n$, and so $|H : A_n| > 1$. Hence

   $$2 = |S_n : A_n| = |S_n : H| \underbrace{|H : A_n|}_{>1}$$

   shows $|S_n : H| = 1$, and so $H = S_n$.

   Suppose $H \cap A_n = \{()\}$. Suppose $x, y \in H$ are nonidentity elements. Then x and y are odd permutations. Hence x^2 and xy are even permutations in H. But the only even permutation in H is $()$. So $x^2 = xy = ()$, and we get $x = y$ by canceling x on the left. We have just shown that H can have at most one nonidentity element x, and $|x| = 2$. So $H = \{(), x\}$. By the normality of H, it must be true that $yxy^{-1} \in H$ for all $y \in S_n$. Conjugation preserves order, and so yxy^{-1} must actually be equal to x. We have just shown that x is in the center of S_n. But we know $Z(S_n) = \{()\}$ by one of our homework exercises (4.3.8). Therefore, no such nonidentity element x can be in H. Hence $H = \{()\}$.

2. (5 pts each) Let R be a commutative ring and let $x \in R$ be nilpotent, that is there exists some $m \in \mathbb{Z}^+$ such that $x^m = 0$.

   (a) Prove that x is either zero or a zero divisor.

   Hint: Set m as the least positive integer such that $x^m = 0$. Remember that x is a zero divisor if $x \neq 0$ and there exists some $y \neq 0$ such that $xy = 0$.

   Let m be the least positive integer such that $x_m = 0$. If $m = 1$, then $x = x^1 = 0$. If $m > 1$, then $x = x^1 \neq 0$, so x is a nonzero element of R. We also know $x^{m-1} \neq 0$ by the minimality of m. But $xx^{m-1} = x^m = 0$. Therefore x is a zero divisor.

   (b) Prove that $1 + x$ is a unit in R.

   Hint: Prove that if x is nilpotent, so is $y = -x$, and use this to construct a multiplicative inverse of $1 - y$.

   Let $m \in \mathbb{Z}^+$ be such that $x^m = 0$. First, let $y = -x$, and observe that $y^m = (-x)^m = (-1)^m x^m = 0$. So y is also nilpotent. Now

   $$\begin{aligned}(1 - y)(1 + y + y^2 + \cdots + y^{m-1}) &= 1 + y + y^2 + \cdots + y^{m-1} - y - y^2 - \cdots - y^m \\ &= 1 - y^m \\ &= 1\end{aligned}$$

   Hence $1 + y + y^2 + \cdots + y^{m-1}$ is a right inverse of $1 - y$. By commutativity, it must also be a left inverse of $1 - y$. Hence $1 + x = 1 - y$ is a unit.

3. Prove that there exists no simple group of order 30.

   Hint: Show that at least one of the Sylow subgroups of a group of order 30 must be normal.

   Let G be a group of order 30. We will show that G cannot be simple by showing that one of its Sylow subgroups must be normal. Let n_3 and n_5 be the number of Sylow 3-subgroups and Sylow 5-subgroups of G. By the Sylow Theorem, we know

   $$n_3|10 \quad \text{and} \quad n_3 \equiv 1 \mod 3$$

   and

   $$n_5|6 \quad \text{and} \quad n_5 \equiv 1 \mod 5$$

   So n_3 is either 1 or 10, and n_5 is either 1 or 6. Suppose $n_3 = 10$ and $n_5 = 6$. Since the Sylow 3-subgroups are all cyclic groups of prime order, the intersection of two distinct Sylow 3-subgroups must be trivial. Hence the 10 Sylow 3-subgroups must contain 20 distinct elements of order 3. Similarly, any two distinct Sylow 5-subgroups can have only the identity in common, and so they must contain 24 distinct elements of order 5. But that is already 20+24=44 nonidentity elements, and a group of order 30 cannot have that many. Therefore either $n_3 = 1$ or $n_5 = 1$ (or both), and the corresponding Sylow subgroup(s) of G must be normal in G. Hence G cannot be simple.

4. (10 pts) Let $\phi : R \to S$ be a ring homomorphism. Prove that the kernel of ϕ is an ideal of R.

   Let

   $$K = \ker(\phi) = \{x \in R \mid \phi(x) = 0\}.$$

   Regarding ϕ as a group homomorphism on the additive groups of R and S, we already know from MCS 313 that this kernel is a subgroup of the additive group of R. So the only thing we need to show is that for all $x \in K$ and all $r \in R$, K contains rx and xr.

   Since ϕ is a ring homomorphism,

   $$\phi(rx) = \phi(r)\underbrace{\phi(x)}_{0} = 0.$$

   Similarly,

   $$\phi(xr) = \underbrace{\phi(x)}_{0}\phi(r) = 0.$$

5. (10 pts) **Extra credit problem.** Let R be a ring with identity. Prove that if R is finite, then every nonzero element of R is either a unit or a zero divisor.

   Hint: For $x \in R$, consider whether the map $\phi_x : R \to R$ defined by $\phi_x(r) = xr$ is injective or not.

   Let x be a nonzero element in R. Let $\phi_x : R \to R$ be the map $\phi_x(r) = xr$. Suppose ϕ_x is not injective. Then there exist some $y \neq z$ in R such that

   $$\phi_x(y) = \phi_x(z) \implies xy = xz \implies xy - xz = 0 \implies x(y - z) = 0.$$

   Since $y \neq z$, we know $y - z \neq 0$. Therefore x is a zero divisor.

   On the other hand, if ϕ_x is injective, then it must also be surjective since it is from a finite set to itself (by Prop 1(4) in Section 0.1). Hence there exists some $y \in R$ such that $\phi_x(y) = 1$. Hence $xy = 1$. That is not quite enough to say that x is a unit because R need not be commutative.

   We can now repeat the argument with the map $\sigma_x : R \to R$ defined by $\sigma_x(r) = rx$. Just like above, if σ_x is not injective, then there must exist some nonzero $r \in R$ such that $rx = 0$,

and hence x is a zero divisor. If σ_x is injective, then it is also surjective, and this gives is some $z \in R$ such that $zx = 1$. By the associativity of multiplication,

$$y = (zx)y = z(xy) = z.$$

So y is really the inverse of x. Therefore x is a unit.