MCS 314 Final Exam Solutions

1. (10 pts) Let A be a nonempty set, H a subgroup of the symmetric group S_A, and
$$F(H) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$
be the set of fixed points of H in A. Prove that if τ is an element of the normalizer $N_{S_A}(H)$, then τ stabilizes both $F(H)$ and $A - F(H)$. That is show that for all $a \in F(H)$, $\tau(a) \in F(H)$ and for all $a \in A - F(H)$, $\tau(a) \in A - F(H)$.

   Hint: Note that if $h \in H$ and $\tau \in N_{S_A}(H)$, then $\tau h \tau^{-1} = h'$ for some $h' \in H$. Consider $h(\tau(a))$ for $a \in F(H)$.

   Let $\tau \in N_{S_A}(H)$. Let $a \in F(A)$. We want to show $\tau(a) \in F(A)$. To be in $F(A)$, $\tau(a)$ needs to be fixed by all $h \in H$. Let h be an arbitrary element of H. Since $N_{S_A}(H)$ is a subgroup of $S(A)$, it is closed under inverses. So $\tau^{-1} \in N_{S_A}(H)$. Hence $\tau^{-1} h \tau \in H$. So $\tau^{-1} h \tau = h'$ for some $h' \in H$. Hence $h\tau = \tau h'$. Since $h' \in H$, $h'(a) = a$, and so
$$h\tau(a) = \tau h'(a) = \tau(a)$$
shows that h fixes $\tau(a)$. Since h was an arbitrary element in H, $\tau(a)$ is fixed by all $h \in H$.

   Now, let $a \in A$. We will show that if $\tau(a) \in F(A)$, then $a \in F(A)$. So if $a \in A - F(A)$, then $\tau(a)$ cannot be in $F(A)$, and hence must be in $A - F(A)$.

   Suppose $\tau(a) \in F(A)$. Since τ is an element of $N_{S_A}(H)$, so is τ^{-1}. We have already shown that $F(A)$ is stabilized by all elements of $N_{S_A}(H)$, and so by τ^{-1} in particular. Since $\tau(a) \in F(A)$,
$$a = \tau^{-1}(\tau(a)) \in F(A).$$

2. (10 pts) Let $n \geq 5$. Prove that A_n is the only proper subgroup of S_n whose index is less than n. You may use the result that for $n \geq 5$, the only normal subgroups of S_n are $\{1\}$, A_n, and S_n.

   Hint: Assume H is a proper subgroup of index less than n, and let S_n act on the left cosets of H by left multiplication.

   Assume H is a proper subgroup of S_n of index less than $m < n$. Then H has m distinct left cosets. Let A be the set of these left cosets of H. Label these with $1, 2, \ldots, m$. Let S_n act on A by left multiplication. With our labeling, we can view the permutation representation π of this action as a homomorphism $\pi : S_n \to S_m$.

   We will show $\ker(\pi) \leq H$. Suppose $\sigma \in \ker(\pi)$. Then $\sigma(gH) = gH$ for all $g \in S_n$. In particular, if $g = 1$, then $\sigma H = H$, and so $\sigma \in H$. Hence $\ker(\pi) \leq H$.

   We also know $\ker(\pi) \trianglelefteq S_n$ and for $n \neq 5$, the only other normal subgroups of S_n are $\{1\}$, A_n, and S_n. Clearly, $\ker(\pi)$ cannot be S_n, because it is a subgroup of the proper subgroup H. It is also quite clear that $\ker(\pi) \neq \{1\}$. Otherwise π would be injective, but π cannot be injective because $|S_m| = m! < n! = |S_n|$. We can conclude $\ker(\pi) = A_n$. Now
$$A_n \leq H \lneq S_n \implies 2 = [S_n : A_n] \geq [S_n : H] > [S_n : S_n] = 1 \implies [S_n : H] = 2.$$
   Hence $H = A_n$.

3. (10 pts) Let R be a ring with identity $1 \neq 0$. Prove that R is a division ring if and only if its only left ideals are (0) and R.

   Hint: To prove R is a division ring, consider the left ideal generated by any nonzero $r \in R$.

   Let R be a division ring. Obviously, (0) is a left ideal in R, as it is in every ring. Suppose I is a nonzero left ideal of R. Then I contains some nonzero $x \in R$. Since R is a division

ring, x must have an inverse x^{-1}. Hence $1 \in x^{-1}x \in I$. Now, let r be any element of R. Then $r = r1 \in I$. So $I = R$.

Conversely, suppose the only left ideals of R are (0) and R. Let x be any nonzero element in R. Then Rx is a left ideal of R. It contains the nonzero element x, so it cannot be (0). Therefore $Rx = R$. So $1 \in Rx$. Hence there must exist some $y \in R$ such that $yx = 1$. Obviously, $y \neq 0$, otherwise $yx = 0$. Repeating the previous argument with the left ideal Ry shows there is some $z \in R$ such that $zy = 1$. Hence

$$z = z1 = z(yx) = (zy)x = 1x = x.$$

So $xy = 1$. This shows y is the inverse of x. Since x was an arbitrary nonzero element in R, every nonzero element in R must have a multiplicative inverse. '

4. (10 pts) Let G be a group and $H \leq G$. Let A be the set of left cosets of H. Let G act on A by left multiplication, and let $\pi : G \to S_A$ be the permutation representation of this action. Prove that $\ker(\pi)$ is the largest normal subgroup of G contained in H.

   Hint: Prove that $K \leq \ker(\pi)$ for all normal subgroups K of G such that $K \leq H$.

   First, note that $\ker(\pi)$ is certainly a normal subgroup of G. The same argument we used in problem 2 shows that $\ker(\pi) \leq H$. We just need to show that $\ker(\pi)$ is the largest among normal subgroups of G contained in H, that is if $K \trianglelefteq G$ and $K \leq H$ then $K \leq \ker(\pi)$. So let K be such a subgroup. Now, let gH be any left coset of H and k any element of K. Since K is normal in G, there exists some $g' \in G$ such that $kg = gk'$. By $k \in K \leq H$,

$$k(gH) = kgH = g\underbrace{k'H}_{H} = gH.$$

   So $k \in \ker(\pi)$. It follows that $K \leq \ker(\pi)$, which is what we wanted to prove.

5. In this problem, you will show that up to isomorphism, the only simple group of order 12 is A_4.

   (a) (2 pts) Suppose G is a simple group of order 12. Prove that G must have exactly four distinct Sylow-3 subgroups.

   Let n_3 be the number of Sylow-3 subgroups of G. By Sylow's Theorem, $n_3|4$ and $n_3 \equiv 1 \bmod 3$. So $n_3 = 1$ or $n_3 = 4$. But we know $n_3 \neq 1$, otherwise the only Sylow-3 subgroup of G would be normal and G would not be simple. Therefore $n_3 = 4$.

   (b) (4 pts) Now, let P be a Sylow-3 subgroup of G. Let A be the set of left cosets of P and let G act on A by left multiplication. Prove that the kernel of this action is $\{1\}$.

   Hint: What did you prove in problem 4?

   As we proved in problem 4, the kernel of this action of G on A is the largest normal subgroup of G that is contained in P. Since G is simple, its only normal subgroups are $\{1\}$ and G. But $P \lneq G$, so P cannot contain G. Hence the kernel is $\{1\}$.

   (c) (4 pts) Argue that there must exist an injective homomorphism $\pi : G \to S_4$, and therefore G is isomorphic to a subgroup of S_4. Finally, conclude that this subgroup must be A_4.

   Hint: To prove this last claim, it may be useful to note that $A_4 \cap \pi(G)$ contains all 3-cycles in S_4.

   Just like in part (b), let G act on A, the set of left cosets of P, by left multiplication. Since $[G : P] = 12/3 = 4$, we can label the four left cosets in A by 1, 2, 3, and 4. This gives us a permutation representation $\pi : G \to S_4$. We have already shown that

$\ker(\pi) = \{1\}$. Hence π is injective. Therefore $G \cong \text{im}(\pi) \leq S_4$. Hence $|\,\text{im}(\pi)| = |G| = 12$. We will show $\text{im}(\pi) = A_4$.

Since the four Sylow-3 subgroups of G are of prime order, any two of them must have trivial intersection $\{1\}$. So G must contain eight elements of order 3. Hence $\text{im}(\pi)$ also contains eight elements of order 3. The only elements of order 3 in S_4 are the eight 3-cycles. These are all even permutations, hence they are elements of A_4. So $\text{im}(\pi) \cap A_4$ has at least eight elements. But $\text{im}(\pi) \cap A_4$ must be a subgroup of both $\text{im}(\pi)$ and of A_4 and so its order must divide 12. Therefore $|\,\text{im}(\pi) \cap A_4| = 12$ and $\text{im}(\pi) = \text{im}(\pi) \cap A_4 = A_4$. Therefore $G \cong A_4$.

6. (10 pts) Let R be a commutative ring and I an ideal of R. The radical of I is defined as

$$\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{Z}^+\}.$$

Prove that $\sqrt{I}$ is also an ideal in R.

Hint: If $x, y \in R$ and $m, n \in \mathbb{Z}^+$ such that $x^m, y^n \in I$, try showing that $(x+y)^{m+n} \in I$.

First, note that $0^1 = 0 \in I$, hence $0 \in \sqrt{I}$. Suppose $x \in \sqrt{I}$ and $r \in R$. Then $x^n \in I$ for some $n \in \mathbb{Z}^+$. Then $(rx)^n = r^n x^n$ because R is commutative and $r^n x^n \in I$ because I is closed under multiplication by elements of R. Hence $rx \in \sqrt{I}$. By commutativity, $xr \in \sqrt{I}$.

Suppose $x, y \in \sqrt{I}$. Then $x^m, y^n \in I$ for some $m, n \in \mathbb{Z}^+$. We will show that $(x+y)^{m+n} \in I$, and hence $x + y \in \sqrt{I}$. Since R is commutative, we can expand $(x+y)^{m+n}$ the usual way:

$$(x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}.$$

Notice that either $i \geq m$ or $m+n-i \geq n$. So either x^i or y^{m+n-i} is in I. Hence $x^i y^{m+n-i} \in I$. Therefore

$$\binom{m+n}{i} x^i y^{m+n-i} = \underbrace{x^i y^{m+n-i} + x^i y^{m+n-i} + \cdots + x^i y^{m+n-i}}_{\binom{m+n}{i} \text{ terms}} \in I,$$

because I is closed under addition. Therefore

$$\sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i} \in I$$

also by closure under addition. So $(x+y)^{m+n} \in I$.

Finally, we will prove $\sqrt{I}$ is closed under additive inverses. Let $x \in \sqrt{I}$. Then $x^n \in I$ for some $n \in \mathbb{Z}^+$. Clearly, $x^{2n} = x^n x^n \in I$. Hence $(-x)^{2n} = x^{2n} \in I$. This shows $-x \in \sqrt{I}$.

We can now conclude that $\sqrt{I}$ is an ideal of R,

Remark: The argument with the binomial coefficients above is a bit subtle. In general, you cannot assume that $\mathbb{Z} \subseteq R$. For that matter, R may not even have a 1. But multiplication by a positive integer can always be interpreted as repeated addition in any ring. And multiplication by a negative integer can be interpreted as repeated addition of the inverse. The actual value of the coefficients really does not matter here, only that they do in fact arise from counting the term $x^i y^{m+n-i}$ after distributing $(x+y)^{m+n}$.

Another remark: If we knew $1 \in R$, then we would be able to say $-1 \in R$ and hence if $x \in \sqrt{I}$, then $-x = (-1)x \in \sqrt{I}$. But we were not given that R has an identity, and this is why I needed to prove closure under additive inverses in a less direct way.

7. **Extra credit problem.** Let R be a commutative ring. Recall that an ideal I of R is *finitely generated* if there is a subset $A \subseteq I$ such that I is the smallest ideal of R that contains A. We showed in that class that this means I is the intersection of all ideals J such that $A \subseteq J$.

   A chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

   of R is called an *ascending chain* of ideals. The ring R is called a *Noetherian ring* if every ascending chain of ideals is finite in the sense that is there is some $N \in \mathbb{Z}^+$ such that

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

   Let us call R a *green mamba ring* if every ideal of R is finitely generated.

   (a) (6 pts) Prove that if R is a green mamba ring, then R is Noetherian.

   Hint: Use that the union of an ascending chain of ideals is an ideal, and therefore must be finitely generated.

   Suppose R is a green mamba ring. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

   be an ascending chain of ideals of R. Let

$$I = \bigcup_{k=1}^{\infty} I_k.$$

   We proved in class that any chain of ideals totally ordered by inclusion is an ideal. An ascending chain is just a special case of such a general chain with countably many elements. So I is an ideal of R. Hence I must be finitely generated. That is $I = (x_1, x_2, \ldots, x_n)$ for some $x_1, x_2, \ldots, x_n \in I$. Then each x_i must be in some ideal in the chain, so there exists some $k_i \in \mathbb{Z}^+$ such that $x_i \in I_{k_i}$. Let $N = \max(k_1, k_2, \ldots, k_n)$. Then $x_i \in I_{k_i} \subseteq I_N$. So I_N contains all of the x_i. By definition, I is the smallest ideal that contains $\{x_1, x_2, \ldots, x_n\}$. So $I \subseteq I_N$. Obviously, I also contains I_N, and so $I = I_N$. Now, for any integer $m \geq N$, $I_N \subseteq I_m \subseteq I = I_N$, hence $I_m = I_N$. Therefore the ascending chain is no longer increasing after the N-th term, that is it is finite.

   (b) (9 pts) Let R now be a commutative ring with $1 \neq 0$. Prove that if R is not a green mamba ring, that is R contains some ideal that is not finitely generated, then R contains a maximal non-finitely generated ideal.

   Hint: Isn't it a bit funny that Prof. Zorn's first name was Max? Could that be short for Maximal? Consider the set S of all ideal of R that are not finitely generated, and partially order S by inclusion. The trick is to prove the union of a chain is not finitely generated. Some of the ideas used to prove part (a) may work here too.

   Suppose R is not a green mamba ring. Then there exists some ideal I in R that is not finitely generated. Let S be the set of all ideals of R that are not finitely generated. Partially order S by inclusion. We will show that every chain in S has an upper bound. Let C be a chain in S. Let $I = \bigcup_{I \in C} I$. We proved in class that the union of a chain ordered by inclusion is an ideal, so I is an ideal of R. We need to prove that I is not finitely generated. Suppose I were finitely generated. So $I = (x_1, x_2, \ldots, x_n)$ for some $x_1, x_2, \ldots, x_n \in I$. Then each x_j must be in some ideal I_j in C. Consider the finite subset $T = \{I_1, I_2, \ldots, I_n\}$ of S. It is totally ordered (since it is a subset of S, and it is finite, hence it must have a largest element I_m. This I_m contains all of $x_1, x_2, \ldots, x_n$, and so $I = (x_1, x_2, \ldots, x_n) \subseteq I_m$. But I_m is obviously also a subset of I. Hence $I_m = I$. But this contradicts that the elements of S are ideals that are not finitely generated.

Therefore I is an ideal than cannot be finitely generated and is therefore an element of S and obviously an upper bound of the chain C.
Since every chain in S has an upper bound, S must have a maximal element by Zorn's Lemma. That element is a maximal non-finitely generated ideal.

Remark: So what does this have to do with Noetherian rings? It is in fact possible to prove in a Noetherian ring, every ideal is finitely generated. In other words, Noetherian rings are the same thing as green mamba rings. Perhaps this is why green mamba rings never became standard terminology. The proof is tricky and involves a few more rounds of Zorn's Lemma and the Axiom Choice. Showing that if there is a non-finitely generated ideal, then there is a maximal non-finitely generated ideal is often the initial step in the argument.