Math 322 **Homework 7 Solutions** Due: Wednesday, April 10

Instructions: Same rules as usual. Work together, write-up alone, no internet!

(9pts) 1. Consider the normal series below for $\mathbb{Z}_{24}$:

$$\mathbb{Z}_{24} \supset \langle 12 \rangle \supset \{0\}$$

(a) Find the two quotient groups for the series. Find the "standard" abelian groups each is isomorphic to.

> **Solution:** $\mathbb{Z}_{24}/\langle 12 \rangle \cong \mathbb{Z}_{12}$ since the cosets are $\langle 12 \rangle, \langle 12 \rangle + 1, \langle 12 \rangle + 2, \ldots \langle 12 \rangle + 11$. The other quotient group is $\langle 12 \rangle/\{0\} = \{0, 12\} \cong \mathbb{Z}_2$.

(b) For the quotient group that is not simple found above, find a non-trivial normal subgroup, and realize it as a quotient group $G'/\langle 12 \rangle$ for some G'.

> **Solution:** We need to find a subgroup of $\mathbb{Z}_{12}$. We could take $\{0, 4, 8\}$ for example. In cosets, this corresponds to $\{\langle 12 \rangle, \langle 12 \rangle + 4, \langle 12 \rangle + 8\}$ which is the result of taking $\langle 4 \rangle$ in $\mathbb{Z}_{24}$ and modding out by $\langle 12 \rangle$. Thus $\{0, 4, 8\} \cong \langle 4 \rangle/\langle 12 \rangle$.
>
> There are other correct solutions here: we could take G' to be $\langle 6 \rangle$, $\langle 3 \rangle$ or $\langle 2 \rangle$ as well.

(c) Demonstrate/explain how this shows us how to build a longer normal series for $\mathbb{Z}_{24}$.

> **Solution:** Using the quotient group we found in the previous part, we see that we can create a longer normal series:
>
> $$\mathbb{Z}_{24} \supset \langle 4 \rangle \supset \langle 12 \rangle \supset \{0\}$$
>
> The G' you find always allows you to find an intermediate normal subgroup since it will necessarily be a normal subgroup of G and contain H.

(6pts) 2. Find two different composition series for $\mathbb{Z}_{28}$. Then use quotient groups to demonstrate that the two series are "isomorphic" (and explain what this means).

> **Solution:** Here are some of the choices:
>
> $$\mathbb{Z}_{28} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$$
>
> $$\mathbb{Z}_{28} \supset \langle 7 \rangle \supset \langle 14 \rangle \supset \{0\}$$
>
> $$\mathbb{Z}_{28} \supset \langle 2 \rangle \supset \langle 14 \rangle \supset \{0\}$$
>
> (in fact, these are the only possibilities).
>
> For the first one, the quotient groups are $\mathbb{Z}_2$, $\mathbb{Z}_2$ and $\mathbb{Z}_7$ (reading from left to right). The second series has quotient groups $\mathbb{Z}_7$, $\mathbb{Z}_2$ and $\mathbb{Z}_2$. The third: $\mathbb{Z}_2$, $\mathbb{Z}_7$, and $\mathbb{Z}_2$. This is the way that the composition series are isomorphic: they have exactly the same quotient groups up to isomorphism and the order in which they occur.

(4pts) 3. Suppose G is a group that contains a normal subgroup H which is itself a non-abelian simple group. Explain how you know that G is not solvable. Note, this is not difficult at all if you know the definitions of simple and solvable.

> **Solution:** To say that G is solvable means it has a composition series in which every quotient group is abelian. To say H is simple means it contains no non-trivial normal subgroups. Now if H is simple and is included in a composition series, then the composition series must end in $\ldots \supset H \supset \{e\}$. The final quotient group will be $H/\{e\} \cong H$ which is not abelian. By the Jordan-Hölder theorem, every composition series will be isomorphic to this one, so each will have a non-abelian quotient group.

(6pts) 4. Consider the polynomial $p(x) = x^7 - 1 = (x-1)(x^6 + x^5 + \cdots + x + 1)$. Let $\omega = e^{2\pi i/7}$ be a root of $p(x)$. Then $\mathbb{Q}(\omega)$ is the splitting field for $p(x)$.

(a) Explain how we know that the Galois group $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is isomorphic to $\mathbb{Z}_7^*$. Give two examples of elements in $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ and say what elements in Z_7^* they correspond to.

> **Solution:** Note that it makes sense to consider $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ since $\mathbb{Q}(\omega)$ is the splitting field for $p(x)$. Each element in the Galois group will be completely determined by where we send ω (since every other root is a power of ω). We can send ω to any of its 6 powers (including ω, but not including $\omega^7 = 1$). Thus there are 6 elements in the Galois group. Further, if $\sigma(\omega) = \omega^k$ and $\tau(\omega) = \omega^j$ then
>
> $$\sigma\tau(\omega) = \omega^{kj} = \omega^{jk} = \tau\sigma(\omega)$$
>
> so the Galois group is abelian. Thus we know that $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q}) \cong \mathbb{Z}_6 \cong \mathbb{Z}_7^*$. But considering $\mathbb{Z}_7^*$ is a little nicer since there we multiply number mod 7. Here, we can think of each automorphism as multiplying the exponent by a number $\{1, 2, \ldots, 6\}$ and since we simple travel around the 7 points on the unit circle, we do so mod 7.
>
> Two specific elements might be σ and τ where $\sigma(\omega) = \omega^2$ and $\tau(\omega) = \omega^3$. These correspond to the elements 2 and 3 in $\mathbb{Z}_7^*$.

(b) $\mathbb{Z}_7^*$ has a composition series $\mathbb{Z}_7^* \supset \{1, 6\} \supset \{1\}$. Find the corresponding series of extension fields of $\mathbb{Q}$. In other words, find the intermediate field E such that $\mathrm{Gal}(\mathbb{Q}(\omega) : E) \cong \{1, 6\}$.

> **Solution:** Let $\beta \in \mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ be the element corresponding to $6 \in \mathbb{Z}_7^*$. Specifically $\beta(\omega) = \omega^6$. Then β is complex conjugation. Now consider $\omega + \omega^6$. This is not an element of $\mathbb{Q}$, but it is fixed by β. So we can take $E = \mathbb{Q}(\omega + \omega^6)$. Note that $\omega + \omega^6 = 2\sin(3\pi/14)$ is a real number and a root of the polynomial $x^3 + x^2 - 2x - 1$ (thanks WolframAlpha!). So $\mathbb{Q}(\omega + \omega^6)$ is a degree 3 extension of $\mathbb{Q}$. Note that this means that $\mathbb{Q}(\omega)$ is a degree 2 extension of $\mathbb{Q}(\omega + \omega^6)$, which is not a surprise since $|\,\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q}(\omega + \omega^6))| = 2$.

(5pts) 5. Find a degree 5 polynomial whose Galois group is isomorphic to S_5. Explain how you know your example works. Your example should be different from the one we discuss in class.

Solution: We must find an irreducible polynomial of degree 5 with exactly two non-real roots. This will guarantee that the Galois group contains a 5-cycle (since the polynomial is irreducible, using Cauchy's theorem) and a 2-cycle (since complex conjugation switches just the two non-real roots), so contains all permutations in S_5.

Such a polynomial is $p(x) = 3x^5 - 15x + 5$, which is irreducible by Eisenstein's criterion. That it has exactly two non-real roots can be seen by graphing, or more carefully, by considering the derivative $15x^4 - 15$ which has exactly two real roots (± 1), so the original polynomial only has one maximum and one minimum. Then use the intermediate value theorem to prove that there are roots between -2 and -1, between -1 and 1 and between 1 and 2 (specifically, $p(-2) = -61$ and $p(-1) = 17$ so there is a zero between $x = -2$ and $x = -1$; similarly for the other intervals).

(5000bns-pts) 6. Bonus: express the roots of the polynomial you found in the previous question in terms of rational numbers, field operations and roots (e.g., square roots, cube roots, etc.)

Solution: Since S_5 is not a solvable group, the polynomial will not be solvable by radicals. Thus it is impossible to complete this problem. Hilarius, right?