Exam 2 Study Guide
Hints and Answers

Math 322 | Spring 2019

1. Here is the table for D_3:

$*$	R_0	R_{120}	R_{240}	F_v	F_x	F_{-x}
R_0	R_0	R_{120}	R_{240}	F_v	F_x	F_{-x}
R_{120}	R_{120}	R_{240}	R_0	F_x	F_{-x}	F_v
R_{240}	R_{240}	R_0	R_{120}	F_{-x}	F_v	F_x
F_v	F_v	F_{-x}	F_x	R_0	R_{240}	R_{120}
F_x	F_x	F_v	F_{-x}	R_{120}	R_0	R_{240}
F_{-x}	F_{-x}	F_x	F_v	R_{240}	R_{120}	R_0

For each of the elements of D_3, we find a permutation in S_6 (6 because there are 6 elements of D_3). The identity permutation is $\pi_{R_0} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$. Now to find $\pi_{R_{120}}$ we look at the result of multiplying each element by R_{120} (on the left). This gives

$$\pi_{R_{120}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}$$

This is because if we multiply the first element of D_3 (R_0) by R_{120} we get R_{120} (the second element of D_3). If we multiply element 2 by R_{120} we get element 3 (since $R_{120}R_{120} = R_{240}$). If we multiply element 3 by R_{120} we get element 1. If we multiply element 4 (F_v) by R_{120} we get element 5 (F_x). And so on.

Here are the other permutations:

$$\pi_{R_{270}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix} \qquad \pi_{F_v} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}$$

$$\pi_{F_x} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix} \qquad \pi_{F_{-x}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 6 & 4 & 3 & 2 & 1 \end{pmatrix}$$

2. We look for the last occurrence of 5, which is in the final transposition. Now (34)(45) = (35)(34), so we can write

$$\varepsilon = (13)(24)(35)(14)(12)(15)(35)(34)$$

Now (15)(35) = (35)(13) so we gets

$$\varepsilon = (13)(24)(35)(14)(12)(35)(13)(34)$$

Then (12)(35) = (35)(12) since the transpositions are disjoint so,

$$\varepsilon = (13)(24)(35)(14)(35)(12)(13)(34)$$

and similarly

$$\varepsilon = (13)(24)(35)(35)(14)(12)(13)(34)$$

But (35)(35) = (1) so we end up with

$$\varepsilon = (13)(24)(14)(12)(13)(34)$$

3. (a) $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$.

(b) $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$

(c) $fgf^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$

(d) $f^3g^2fg^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

(e) $f = (134)$, $g = (1245)$.

(f) $f = (13)(34)$, $g = (12)(24)(45)$

(g) $fg = (12)(345) = (12)(34)(45)$, $f^{-1} = (143) = (14)(34)$, $fgf^{-1} = (1532) = (15)(53)(32)$, $f^3g^2fg^{-1} = (123)(45) = (12)(23)(45)$.

4. (a) By Lagrange's theorem, the order of α must divide 120, the order of S_5. Thus 120 is a multiple of the order of α. But $\alpha^t = (1)$ if and only if t is a multiple of $\operatorname{ord}(\alpha)$, so $\alpha^{120} = (1)$.

   (b) No, since S_5 is not cyclic. If there were an element of 120, then that element would generate S_5.

   (c) Yes. For example, $(12)(345)$ has order 6.

   (d) No. By Lagrange's theorem, the order of any element must divide the order of the group. 120 is not divisible by 7.

5. (a) False. for example, if a and b are inverses of each other, then $\operatorname{ord}(ab) = 1$ but if $a \neq e$ then $\operatorname{ord}(a) \cdot \operatorname{ord}(b) > 1$.

   (b) False as well. The same counterexample works.

   (c) This is also false. For example, $a = (12)$ and $b = (13)$ in S_3. Then $\operatorname{ord}(ab) = 3$ but $\operatorname{ord}(a)\operatorname{ord}(b) = 4$.

   (d) For any of these to be true, we need a and b to commute. In this case, part (c) is true, but the other two are still false (since an element and its inverse commute). To make (a) and (b) true, we could insist the orders be relatively prime.

6. If $H = G$ we are done (since G/H would be trivial). So assume $a \notin H$. We claim that Ha generates G/H. Since every element in G/H is Hb for some element $b \in G$, and every element in G is a power of a, we have every element of G/H is $H(a^k)$ for some k. But $H(a^k) = (Ha)^k$ so every element of G/H is a power of Ha. In other words, G/H is cyclic.

7. (a) H must be cyclic, and must have order dividing n.

   (b) Let $H = \langle a^{n/k} \rangle$. Then H has order k, since its generator has order k.

   (c) No. For example, A_4 has order 12 but has no subgroup of order 6.

8. The subgroups are just $\{0\}$ and $\mathbb{Z}_{17}$. Since the order of $\mathbb{Z}_{17}$ is 17, a prime number, the order of any subgroup can only be 1 or 17.

9. If G is a finite group and H is a subgroup of G, then the order of H is a factor of the order of G. We know this is true because we can always form the cosets of H, which form a partition of G. Each coset has the same number of elements as H. Thus the number of cosets (i.e., the index of H in G) is $|G|/|H|$. Since this is a whole number, $|H|$ must divide evenly into $|G|$.

10. Cauchy's theorem is a sort of converse of Lagrange's theorem (the converse of Lagrange's theorem would be that if n divides the size of G, then there is a subgroup H of G with order n, but this is false, so Cauchy's theorem is the best we can hope for). Specifically, if p is a prime that divides the order of a finite group G, then there is an element of G which has order p. We proved this in the abelian case by induction on the size of the group. For the inductive case, if there wasn't an element of order p, then we could take any element whose order was not an element of p and consider the cyclic group generated by this element. We then modded out by this subgroup to get a quotient group which was of smaller size, but still a size divisible by p. Thus the quotient group would have an element of order p (by the inductive hypothesis) and we could use that to move back to the original group and find an element of order p (by first finding an element whose order was a multiple of p).

11. Note that $480 = 2^5 * 3 * 5$. By the Fundamental Theorem of Finite Abelian Groups, we know that we can write any abelian group as the direct product of cyclic p-groups. In this case, those p-groups will be 2-groups, 3-groups and 5-groups. The 3-groups and 5-groups must be $\mathbb{Z}_3$ and $\mathbb{Z}_5$ respectively. The 2-groups can be one of

$$\mathbb{Z}_{2^5} \qquad \mathbb{Z}_{2^4} \times \mathbb{Z}_2 \qquad \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} \qquad \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Which case we are in depends on the distribution of elements of particular order. For example, if there are elements of order 32, we will be looking at $\mathbb{Z}_{2^5} \times \mathbb{Z}_3 \times \mathbb{Z}_5$. If there are no elements of order 4, we will be in

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

12. (a) The series is not a composition series (by definition) since not all of the quotient groups are simple. $G/H \cong \mathbb{Z}_{10}$ has non-trivial normal subgroups.

    (b) We can find a non-trivial subgroup of $\mathbb{Z}_{10}$ and use that to find a subgroup of G containing H. There are two non-trivial subgroups of $\mathbb{Z}_{10}$, $\langle 2\rangle$ and $\langle 5\rangle$, and each of these will produce a different intermediate group. Specifically, let K_1 be a subgroup of G such that $K_1/H \cong \mathbb{Z}_5 \cong \langle 2\rangle$ (as a subgroup of $\mathbb{Z}_{10}$) and K_2 be a subgroup of G such that $K_2/H \cong \mathbb{Z}_2 \cong \langle 5\rangle$ (as a subgroup of $\mathbb{Z}_{10}$). Note that $G/K_1 \cong \mathbb{Z}_2$ and $G/K_2 \cong \mathbb{Z}_5$. We get the two composition series

    $$G \supset K_1 \supset H \supset \{e\}$$

    $$G \supset K_2 \supset H \supset \{e\}$$

    These are composition series since all the quotient groups are simple (we know $H/\{e\}$ is simple because H is).

    (c) Since $H \cong H/\{e\}$, we have that all the quotient groups of the two series above are abelian. Since the series above are composition series, all composition series are isomorphic to these, so all of their quotient groups are also abelian. This is the definition of a group being solvable.

    (d) E will have subfields corresponding to the subgroups of G: the fixed fields of the subgroups. Call these F_{K_1}, F_{K_2} and F_H. We match them up by what elements are fixed by the automorphisms in the subgroup. So the subgroup K_1 contains automorphisms of E that fix F_{K_1}, for example. Viewed this way, $K_1 \cong \mathrm{Gal}(E : F_{K_1})$. Note that in using this notation, $F_G = \mathbb{Q}$ and $F_{\{e\}} = E$. We get two sequences of fields: $\mathbb{Q} \subset F_{K_1} \subset F_H \subset E$ and $\mathbb{Q} \subset F_{K_2} \subset F_H \subset E$. Note in particular that F_{K_1} is smaller than F_H, precisely because K_1 is *larger* than H. Since $G/K_1 \cong \mathbb{Z}_2$ we see that F_{K_1} is a degree 2 extension of $\mathbb{Q}$. We also know that F_H will be a degree 5 extension of F_{K_1}. We can do a similar analysis for the other chain of fields. Since we do not know what the size of H is, we do not know what the degree of E over F_H is (although since H is simple and abelian, we can be sure that it is a prime number).

13. (a) Since $p(x)$ is irreducible in $\mathbb{Q}$, we know that $\mathbb{Q}(\alpha)$ will have degree 3 over $\mathbb{Q}$, where α is any root of $p(x)$. Thus the degree of E will be either 3 or 6. This means that the size of G will either be 3 or 6, but in either case, by Cauchy's theorem, since 3 divides the order of the group and 3 is prime, there must be an element of order 3.

    (b) Note that $p(x)$ only has one real root, so the other two roots are complex. This means that the complex conjugation automorphism will switch two roots, so this is a non-identity element of G. But since complex conjugation is its own inverse, we see that this element has order 2.

    (c) No matter what G is (it will be S_3 or $\mathbb{Z}_6$), there is a normal subgroup H. Using the Galois correspondence, this means that the fixfield of H will be a normal extension, i.e., an extension which is the splitting field for some polynomial.

    (d) We get this again by the Galois correspondence. One of the intermediate fields between $\mathbb{Q}$ and E is $\mathbb{Q}(\alpha)$ where α is the real root of $p(x)$. Since this field is purely real, we know that it is NOT a splitting field. Therefore its fixer is a subgroup of G that is not normal. But $\mathbb{Z}_6$ is abelian, so all its subgroups are normal.

    (e) In fact, $p(x)$ is solvable by radicals, as are all degree 3 polynomials (Cardano's formula). The key here is that S_3 is a solvable group, since $S_3 \supset A_3 \subset \{(1)\}$ is a normal series in which each quotient group is abelian.