Exam 2 Study Guide
Hints and Answers

Math 322 Spring 2020

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) 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).

4. (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.

5. (a) The number 1560 is $\varphi(1643) = 30 \cdot 52$, which is the size of the group $U(1643)$ (i.e., the number of numbers less than 1643 relatively prime to 1643). Every number in $U(1643)$ has order dividing the size of the group, so every number in $U(1643)$, when raised to the group's order, will be the identity, which in this group is 1. Thus $42^{1560} \equiv 1 \pmod{1643}$. In fact, $a^{1560} \equiv 1 \pmod{1643}$ for any $a \in U(1643)$; any a relatively prime to 1643.

   (b) We want to find D such that $7D \equiv 1 \pmod{1560}$. We can do this using the Euclidean algorithm forward and backward. Doing so gives $D = 223$. This requirement will say that $7D = k \cdot 1560 + 1$. In fact, we have $7 \cdot 223 = 1561$ in this case. Now if we take a^{7D} we will have $a^{k \cdot 1560+1} = (a^{1560})^k \cdot a \equiv 1^k \cdot a \pmod{1643}$ which is what we want.

6. Given two groups G and H, we can form their external direct product $G \times H = \{(g, h) : g \in G, h \in H\}$ to get a new larger group. Alternatively, given a group G, we can find two *subgroups* H_1 and H_2 such that $H_1 \cap H_2 = \{e\}$ and $H_1H_2 = \{h_1h_2 : h_1 \in H_1, h_2 \in H_2\} = G$ (we also need $h_1h_2 = h_2h_1$ for all pairs taken from these subgroups). It is true that internal direct products will be isomorphic to the external direct product as well.

   For example, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is an external direct product. It happens to be isomorphic to $\mathbb{Z}_6$, but since $\mathbb{Z}_2$ is not a subgroup of $\mathbb{Z}_6$ (and neither is $\mathbb{Z}_3$), this is not an internal direct product. However, we can take $H_1 = \{0, 3\}$ and $H_2 = \{0, 2, 4\}$ and we will have that $H_1 + H_2 = \mathbb{Z}_6$, and $H_1 \cap H_2 = \{0\}$, so $\mathbb{Z}_6$ is the internal direct product of H_1 and H_2. We can then also say that $\mathbb{Z}_6 \cong H_1 \times H_2$ (although not equal, since $H_1 \times H_2$ is a set of ordered pairs). Further, $H_1 \cong \mathbb{Z}_2$ and $H_2 \cong \mathbb{Z}_3$.

7. (a) Yes, there must be an element of order 3. If a has order 9, then a^3 has order 3.

   (b) Yes, there must be elements of order 10. If a has order 2 and b has order 5, then ab has order 10.

   (c) The group might be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, but might not be. It could also be that the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times Z_5$. Or any number of other things.

   (d) The group might be cyclic, but might not be cyclic. We don't know how many elements there are of order 2, for example. If we break down the group using p-groups as inner direct products, the 2-group, which would only contain the identity and order 2 elements (since there are no order 4 elements). If there is more than 1 order 2 element in this group, then we will need to break down the 2-group even further, since it won't be cyclic. However, if the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$, then it is cyclic: that group is isomorphic to $\mathbb{Z}_{90}$.

8. 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

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

9. $X_{(1)} = \{1,2,3,4,5,6\}$, $X_{(12)} = \{3,4,5,6\}$, $X_{(345)} = X_{(354)} = \{1,2,6\}$, $X_{(12)(345)} = X_{(12)(354)} = \{6\}$.

   $G_1 = G_2 = \{(1),(345),(354)\}$, $G_3 = G_4 = G_5 = \{(1),(12)\}$, $G_6 = G$.

   $\mathcal{O}_1 = \mathcal{O}_2 = \{1,2\}$, $\mathcal{O}_3 = \mathcal{O}_4 = \mathcal{O}_5 = \{3,4,5\}$, $\mathcal{O}_6 = \{6\}$.

   Note that $|\mathcal{O}_1| \cdot |G_1| = 2 \cdot 3 = 6$ and same for $x = 2$. We have $|\mathcal{O}_3| \cdot |G_3| = 3 \cdot 2 = 6$ and $|\mathcal{O}_6| \cdot |G_6| = 6 \cdot 1 = 6$.

   For Burnside's theorem, we see that we have 3 different orbits. That is the same as $\frac{1}{|G|}\sum_{g \in G} |X_g| = \frac{1}{6}(6+4+3+3+1+1)$.

10. Use $S_3 = D_3$ as the group acting on the triangle. Using Burnside's theorem, we have $\frac{1}{6}(3^3 + 3 \cdot 3^2 + 2 \cdot 3) = 10$ orbits, i.e., there are 10 ways to color the vertices of the triangle.

11. We have a set of three positions, and each position can be filled with one of 7 flavors, but no flavor can be used more than once. We act on the cones with the group S_3, that permutes the three positions.

    Now $|X_{(1)}| = P(7,3) = 7 \cdot 6 \cdot 5$. We have $|X_g| = 0$ for all other $g \in S_3$ (since no non-identity permutation will fix any cone when all the flavors must be different). Thus Burnside's Theorem says the number of orbits is $\frac{1}{6}(P(7,3))$.