HW ANSWERS IN 3340, SPRING 2017

ALLEN KNUTSON

HW # 1 DUE THURSDAY 2/2

1. Prove that the composite of two onto functions is onto.

Answer. Let $X \xrightarrow{g} Y \xrightarrow{f} Z$ each be onto. Then for any $z \in Z$, $\exists y \in Y$ s.t. $f(y) = z$ (since f is onto). Then $\exists x \in X$ s.t. $g(x) = y$ (since f is onto). Hence $(f \circ g)(x) = z$. Since we have shown that each $z \in Z$ is in the image of $f \circ g$, we have shown that $f \circ g$ is onto.

2. Prove: If $f \circ g$ is onto, so is f.

Answer. For any $z \in Z$, $\exists x \in X$ s.t. $(f \circ g)(x) = z$. Hence $f(g(x)) = x$, so x is in the image of f.

3. Prove: If $f \circ g = e \circ g$, and g is onto, then $f = e$.

Answer. Here $e : Y \to Z$ is another map. We want to show that $f(y) = e(y) \forall y \in Y$. So pick $x \in X$ with $g(x) = y$, using g onto. Then $f(y) = f(g(x)) = (f \circ g)(x) = (e \circ g)(x) = e(g(x)) = e(y)$.

4. For each n up to 10, find a graph with exactly n automorphisms. They don't have to be smallest possible, but if you want to prove that your examples are indeed smallest possible, please do!

Answer. It's easy to get $2n$ – use a wheel of circumference n. The hard part is to spoil the reflection symmetry. One option is to use a wheel of circumference $3n$, and attach tails of length $0, 1, 2, 0, 1, 2, \ldots, 0, 1, 2$ to the vertices.

5. Count the number of partitions of a set with n elements, for n = 1,...,5. Then look up this sequence on the On-line Encyclopedia of Integer Sequences. Example: there are three partitions of the number 3: 3, 2+1, 1+1+1. But there are five partitions of the set a,b,F: a,b,F, a,b U F, a,F U b, b,F U a, a U b U F.

`http://oeis.org/A000110`

6. Label the vertices of the left graph by 1-10 and the right by A-J. Find a correspondence between them, giving an isomorphism of the graphs (i.e. taking connected pairs to connected pairs).

Answer. It's hard to go wrong here as there are 5! ways to do it.

HW#2 due Thursday 2/9: [Beachy & Blair] 2.1 #1,6,16. 2.3 #1,2,5. 3.1 #2,3,11,12,15.

2.1#1a. Both. b. Onto only. c. Depends on whether $\gcd(m, n) = 1$. d. Both.

#6a. $2^3, 3^2$. b. None, all but two. c. 6, none.

#16. $\Leftarrow$ To see f is onto, i.e. hits any $b \in B$, note $f(g(b)) = b$.

Date: March 18, 2017.

$\Rightarrow$ For each $b \in B$, pick an $a \in A$ with $g(a) = b$, and define f by $f(b) = a$. (Actually these requires infinitely many arbitrary choices, which it's not clear you can make; being able to is the Axiom of Choice.)

2.3#1a. (1 2 3 6)(4 7 5). b. (1562)(347). c. (143756). d. (1653). e. (23)(4756) f. (2736)

#2. $\sigma = (1356) = (13)(35)(56)$, $\tau = (12)(3547) = (12)(35)(54)(47)$.

#5. $\sigma\tau^{-1} = (1m)$. Follow any number backwards along τ, then forwards along σ. The composite action is trivial except at the end values of τ.

3.1#2a. Nope, not enough inverses. b,d. Nope, no identity (nor inverses). c. Nope, not associative. e. Yes! f. Nope, 0 doesn't have an inverse.

#3. We have two groups $(G, *), (G, \cdot)$. The map $\phi : g \mapsto g^{-1}$ gives an isomorphism from one to the other. Then the group axioms of $(G, \cdot)$ follow from those of $(G, *)$. There are longer ways to write this out, of course. If G is nonabelian, e.g. $G = S_3$, then $* \neq \cdot$.

#11. The identity is indeed of that form, and the inverse of a matrix of that form is also of that form. We don't need to think hard about associativity etc. since matrix multiplication has that for sure.

#12. The only matrices *at all* that commute with this matrix are diagonal. So, take the $b = 0$ guys in this subgroup.

#15. Multiply by sides by g^{-1} (on, say, the left).

HW #3 DUE THURSDAY 2/16:

1. Recall a relation $R \subseteq A \times B$ is any set of ordered pairs, whereas an equivalence relation $R \subseteq A \times A$ on A is a relation enjoying reflexivity, symmetry, and transitivity.

• Given a relation $R \subseteq A \times A$, prove there is a unique smallest equivalence relation $E \subseteq A \times A$ containing R.

Answer. Let E_1, E_2 be two equivalence relations containing R. Then their intersection $E_1 \cap E_2 \supseteq R$ also, and we can check that it's again an equivalence relation (i.e. that it's still reflexive, symmetric, transitive). The same works for any set of, not just two, equivalence relations. So we want to intersect *all* the equivalence relations containing R. We need to be sure there is one at all; the relation $A \times A$ itself (everything related to everything else) is such a relation.

Now we can intersect all the equivalence relations containing R, and obtain the unique smallest one, E.

• Given R, how would you test whether two elements b, c of A are E-equivalent?

Consider chains $r_0, r_1, \ldots, r_k$ where $r_0 = b$ and $r_k = c$, for all $k \in \mathbb{N}$, where for each $i \in [0, k)$ we have $(r_i, r_{i+1}) \in R$ or $(r_{i+1}, r_i) \in R$ or both. Then by induction on k, $(r_0, r_k) \in E$. In other words, let $F = \{(b, c) : \exists$ such a chain$\}$; so far we've shown $F \subseteq E$.

This relation F is reflexive, by the $k = 0$ chains; symmetric, by the $k = 1$ chains; and transitive by concatenating chains together. So F is an equivalence relation, hence $F \supseteq E$ since E was supposed to be smallest. Together, $F = E$.

2. Let $D_n := \{r^i, r^i f : i = 1, ..., n\}$ be the rotations and reflections of an n-gon (r for rotate, f for flip).

• Find all the two-element subgroups of D_n.

Answer. Let $\{e = r^n, g\}$ be a two-element subgroup. Then $g^2 = e$ but $g \neq e$. So we look for all the elements g like that.

$$(r^i)^2 = r^{2i}, \qquad (r^i f)^2 = r^i f r^i f$$

To compute the latter, we use $frf = r^{-1}$ to show $fr^j f = r^{-j}$ for all $j > 0$ by induction: $fr^j f = fr^{j-1}rf = fr^{j-1}ffrf = r^{1-j}r^{-1} = r^{-j}$ (we could stick in ff since $ff = e$). Hence $(r^i f)^2 = r^i f r^i f = r^i r^{-i} = e$.

So every $g = r^i f$ gives us such an element, and such a subgroup. But r^i only does if $2i = n$, in particular, if n is even.

• For each one, list the right cosets by that subgroup.

For $H = \{e, r^{n/2}\}$: $r^j H = \{r^j, r^{n/2+j}\}$, $r^j f H = \{r^j f, r^j f r^{n/2} = r^j r^{-n/2} f = r^{j-n/2} f\}$ (though in fact $r^{-n/2} = r^{n/2}$).

For $H = \{e, r^i f\}$: $r^j H = \{r^j, r^{j+i} f\}$, $r^j f H = \{r^j f, r^j f r^i f = r^j r^{-i} f f = r^{j-i}\}$.

3. Let G be a group and g an element. Let $C = \{h \in G : hg = gh\}$. Prove that C is a subgroup. (Which means, check axioms 0,1,2.)

Answer.

0: $eg = g = ge$ so $e \in C$.

1: If $hg = gh$, multiply on both sides by h^{-1} to get $gh^{-1} = h^{-1}g$. Hence $h \in C \implies h^{-1} \in C$.

2: If $h, k \in C$, then $hkg = hgk = ghk$, so $hk \in C$.

4. Given two elements $g, h \in G$, define $[g, h] := ghg^{-1}h^{-1}$, called the commutator of the two. (It's not quite the same thing you would do with matrices, where you could mix addition and multiplication.) It "measures" the failure of g and h to commute.

•Show (which always means "prove") that the set of commutators satisfies two of the axioms for being a subgroup. (What's much harder is finding an example where the third is not satisfied.)

Answer. Let C be the set of commutators.

0: $[g, g] = e$, so $e \in C$.

1: If $c \in C$ i.e. $c = [g, h]$ for some g, h, then $[h^{-1}, g^{-1}] = h^{-1}g^{-1}hg = [g, h]^{-1} = c^{-1}$, so $c^{-1} \in C$.

•The **commutator subgroup** is the group generated by the set of commutators. What's the most succinct description of an element of the commutator subgroup? (I.e., it should be tighter than our general description of elements of a subgroup generated by something.)

Answer. The commutator subgroup is the set of all k-fold products of commutators. (We don't have to say "...and their inverses" like we needed to for the more general definition.)

HW#4 due Thursday 2/23: [B & B] 2.2 #5,9. 3.1 #3,13,23. 3.2 #7

2.2#5. Concentric circles around the origin.

#9. We're given that it's reflexive, i.e. $(a,a) \in R$. If $(a,b) \in R$, then using $(a,a) \in R, (a,b) \in R$ we get $(b,a) \in R$. Now if $(a,b) \in R$ and $(b,c) \in R$, we get $(c,a) \in R$, hence $(a,c) \in R$ since we just checked symmetry.

3.1#3. Oops, not this one again.

3.1#13. What's the identity? Some z such that $a = a * z = a + z + az$, i.e. $z + az = 0$ for all a, e.g. $a = 0$. Hence the identity must be $z = 0$.

What are inverses? Now we want $0 = a * z = a + z + az$, i.e. $z = \frac{-a}{1+a}$, which is okay to divide by since $a \neq -1$. We need to be sure that z isn't -1. If it were, then $a = 1 + a$, contradiction.

Is this associative? $(a * b) * c = a * b + c + (a * b)c = a + b + ab + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc$ and $a * (b * c)$ leads to that same answer.

3.1#23. $(ab)^2 = abab = e$, but $a^2 = e$ and $b^2 = e$, so $abab = aabb$ hence $ba = ab$.

HW#5 due Thursday 2/30:

1. Let g be an element of a group G, and $\phi : G \to G$ be the function taking $h \mapsto hgh^{-1}$. In particular the image is "the conjugacy class of g". (Note that this is **not** the map $g \to hgh^{-1}$, in which h would be fixed and g varying, though of course that thing's interesting too.)

a. Find all G, g for which this function is a group homomorphism. (Prove you have the exact list.)

Answer. $\phi(e) = ege^{-1} = g$. For ϕ to be a homomorphism, we need this to be e. Conversely, if $g = e$, then $\phi(h) = heh^{-1} = e$ for all h, and that's definitely a group homomorphism. Hence ϕ is a homomorphism *exactly if* $g = e$.

b. Find all G, g for which this function is 1:1. (Prove you have the exact list.)

Answer. $\phi(e) = \phi(g) = e$. So for ϕ to be $1:1$, we need $g = e$. But then $\phi(h) = e$ for all h. So there should be only one h. Hence the only choice is $G = \{e\}$, $g = e$. Conversely, ϕ is definitely 1:1 then.

c. Find all G, g for which this function is onto. (Prove you have the exact list.)

Answer. If it's onto, we should hit e, i.e. $e = hgh^{-1}$ for some h. But then $g = e$. So once again, $\phi(h) = e$ for all h. If that constant map is onto, we're back at the $G = \{e\}$, $g = e$ situation. Conversely, ϕ is definitely onto then.

2. Same G, g, ϕ as above. Show there is a subgroup H such that ϕ factors as $G \twoheadrightarrow G/H \to G$, where the first map is the usual one, and the second map is 1:1. (Neither are likely to be group homomorphisms. Hint: figure out what this H must be.)

Answer. First we figure out what H must be. The map $G \to G/H$ takes $e \mapsto eH = H$, which then (by the statement that ϕ factors in this way) has to go to $\phi(e) = g$ under the second map $G/H \to G$. So all other $h \in H$ also go to H then to $\phi(e)$, i.e. $h \in H \implies \phi(h) = \phi(e) = g \implies hgh^{-1} = g \Leftrightarrow hg = gh$.

Guess: $H = \{h : hg = gh\}$.

Now we check that ϕ actually factors through this $G \to G/H$, i.e. $aH = bH \implies \phi(a) = \phi(b)$. This holds, because $aH = bH \iff a = bh$ for some $h \in H$, and then $\phi(a) = \phi(bh) = bhg(bh)^{-1} = bhgh^{-1}b^{-1} = bghh^{-1}b^{-1} = bgb^{-1} = \phi(b)$.

To see the 1:1ness, start with two elements $aH, bH \in G/H$ and see where they go, namely to $\phi(a), \phi(b)$. If $\phi(a) = \phi(b)$, then $aga^{-1} = bgb^{-1}$, so $b^{-1}ag = gb^{-1}a$, i.e. $b^{-1}a \in H$. We showed in class that that's equivalent to $aH = bH$. Hence the second map $aH \mapsto \phi(a)$ is 1:1.

3. Use this to prove that the size of each conjugacy class divides $\#G$.

Answer. The image of ϕ is the conjugacy class of g. We just showed that it's in correspondence with G/H, and $\#\, G/\#(G/H) = \#H$, an integer.

4. Consider the equivalence relation generated by $g \sim g^{-1}$, and use it to prove that $2|\#G \implies$ there is some element of order 2.

Answer. The classes in this relation are of the form $\{g, g^{-1}\}$. They're of size 1 exactly if $g = g^{-1}$, in which case g is either e or of order 2. Then $\#G = 2\#(\text{size 2 classes}) + \#(\text{size 1 classes})$.

Hence $\#(\text{size 1 classes}) \equiv \#G \equiv 0 \bmod 2$. But the number of such classes isn't 0, because $\{e\}$ is such a class. Since it's even it's not 1 either, so it's at least 2. So there's some other class $\{g\}$ where $g \neq e$ but $g = g^{-1}$.

5. Let G be abelian of even order.

a. Show that the map $Q : G \to G$, $g \mapsto g^2$, is not 1:1.

Answer. Let g be an element of order 2 (using question 4). Then $Q(e) = Q(g)$.

b. Show that the set H of elements of odd order is a subgroup.

Answer. e is of order 1, so in H. Any g has the same order as its inverse. Now if g, h are of order m, n odd numbers, then

$$(gh)^{mn} = ghghgh\cdots gh = g\cdots gh\cdots h = g^{mn}h^{mn} = (g^m)^n(h^n)^m = ee = e$$

Hence the order of gh *divides* mn, so must again be odd.

c. Show that H is in the image of Q.

Answer. If $h \in H$ has order $2m+1$, then $Q(h^{m+1}) = h^{2m+2} = h$.

d. Show that for all sufficiently large powers n, Q^n has image H.

Answer. Consider the orders of $G, Q(G), Q(Q(G)), \ldots$ Since composites of homomorphisms are homomorphisms, and images of homomorphisms are subgroups, each of these is a subgroup of G.

Assume $H \leq Q^k(G)$, as is obviously true for $k = 0$. Then by applying part (c) to $Q^k(G)$ (instead of to the original G), we find out $H \leq Q^{k+1}(G)$. So by induction it's in every $Q^m(G)$.

If $2|\#Q^k(G)$, then Q is not $1:1$ on $Q^k(G)$ by part (a), so $\#Q^{k+1}(G) < \#Q^k(G)$. This can only happen finitely many times, so for some m we have $2 \not| \#Q^m(G)$, and the image doesn't shrink after that.

At that point, all its elements are of odd order, so contained in H. Combining that with $H \leq Q^m(G)$ from before, we get $Q^m(G) = H$.

HW #6 due 3/9: [BB] 3.8 # 5,6,9,13,17. Compute the sizes of the conjugacy classes in S6; make sure the numbers add up to 6!.

5. If we invert all the elements in a coset gH, we get Hg^{-1}. So inversion gives a correspondence.

6. Let $n \in H \cap N$. Then for any $h \in H$, $hnh^{-1} \in H$ since H is a subgroup, and $hnh^{-1} \in N$ since N is normal. Hence $hnh^{-1} \in H \cap N$.

9. gHg^{-1} is another subgroup of G of the same size as H. If H is unique of that order, then $gHg^{-1} = H$ by that uniqueness. So H is normal. (It was irrelevant that G is finite – we only needed H to be the only subgroup of its cardinality.)

13. If N contains all commutators, then $aNbN = abN = ab(b^{-1}a^{-1}ba)N = baN = bNaN$.

Conversely, if G/N is abelian, then $N = [aN, bN] = aNbNa^{-1}Nb^{-1}N = aba^{-1}b^{-1}N$ i.e. $aba^{-1}b^{-1} \in N$ for all a, b.

17. Adding this element $(2,2)$ to itself, we get $(4,0)$, $(0,2)$, $(2,0)$, $(4,2)$, and finally $(0,0)$. So it's of order 6. Hence the quotient is of size 4. Let's look at $(1,1)$ in the quotient, whose sums are $(2,2)$, $(3,3)$, $(4,0) \sim (0,0) \bmod \langle(2,2)\rangle$. So our 4-element group is cyclic, since it has this element of order 4.

HW #7 due 3/16:

1. Consider 2×2 matrices of the form $\begin{matrix} a & b \\ -3b & a \end{matrix}$ where $a, b \in \mathbb{Q}$. Show that this set, with its usual (matrix) addition and multiplication, is a field.

Answer. Usual matrices are a ring, so that handles a lot of axioms (associativity...). We check this subset is closed under addition/subtraction (which is really obvious), and multiplication (easy to check:

$$\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$$

$$\begin{bmatrix} c & d \\ -3d & c \end{bmatrix} \quad \begin{bmatrix} ac - 3bd & bc + ad \\ -3(bc + ad) & ac - 3bd \end{bmatrix}$$

), so so far it's a subring. Commutativity of multiplication is also easy: it says

$$\begin{bmatrix} ac - 3bd & bc + ad \\ -3(bc + ad) & ac - 3bd \end{bmatrix} = \begin{bmatrix} ca - 3db & cb + da \\ -3(cb + da) & ca - 3db \end{bmatrix}$$

What remains is to show that for any a, b not both 0 the inverse matrix is again of this form. That inverse is

$$\frac{\begin{bmatrix} a & -b \\ 3b & a \end{bmatrix}}{a^2 + 3b^2}$$

i.e. we take $a' = \frac{a}{a^2+3b^2}$, $b' = \frac{-b}{a^2+3b^2}$, and by a, b not both 0 we know this denominator isn't zero.

2. For $p(x, y)$ a polynomial in x and y, define Rp as the polynomial such that $Rp(x, y) = p(y, x)$. For example if $p = x^2 - xy$, then $Rp = y^2 - xy$.

a. Show that $R(pq) = (Rp)(Rq)$.

Answer. Let p be an arbitrary polynomial $\sum_{i,j} c_{ij}x^iy^j$, $q = \sum_{k,l} d_{kl}x^ky^l$ likewise. Then

$$R(pq)(x,y) = R(\sum_{i,j} c_{ij}x^iy^j \sum_{k,l} d_{kl}x^ky^l) = R(\sum_{i,j}\sum_{k,l} c_{ij}d_{kl}x^{i+k}y^{j+l}) = \sum_{i,j}\sum_{k,l} c_{ij}d_{kl}y^{i+k}x^{j+l}$$
$$= \sum_{i,j}\sum_{k,l} c_{ij}y^ix^jd_{kl}y^kx^j = \sum_{i,j} c_{ij}y^ix^j \sum_{k,l} d_{kl}y^kx^j = p(y,x)q(y,x)$$

b. Use the division algorithm to show that $p-Rp$ is a multiple of $x-y$. Call this multiple Dp.

Answer. We treat the ys as constants, i.e. think of $p - Rp$ as a polynomial in x. Then the division algorithm writes $p - Rp = m(x-y) + r$, where m is the multiple and the remainder r has degree $< \deg(x-y)$ in x. That is to say, r is degree 0, it's only a function of y.

Now if we set $x = y$, the left side $p - Rp$ vanishes, as does the $m(x-y) \mapsto m(y-y)$ term, letting us find out that $r = 0$. Now $Dp = m$.

c. Show that $DDp = 0$.

Answer. $DDp = (Dp - RDp)/(x-y)$, so it's equivalent to show $Dp = RDp$. Now, $RDp = R\frac{p-Rp}{x-y} = \frac{R(p-Rp)}{R(x-y)} = \frac{Rp-RRp}{y-x} = \frac{Rp-p}{y-x} = \frac{p-Rp}{x-y} = Dp$.

3. Define $\binom{x}{n}$, where x is a letter and n is a natural number, as $x(x-1)(x-2)...(x-n+1)/n!$. This is a polynomial in x with rational coefficients.

a. Find and prove a formula for $\binom{-1}{n}$.

Answer. $\frac{(-1)(-2)...(-n)}{n(n-1)\cdots 1} = \frac{(-1)(-1)...(-1)}{1\cdots 1} = (-1)^n$

b. Show that every polynomial $p(x)$ of degree at most k is a linear combination of the polynomials $\binom{x}{i}$ for i ranging from 0 up to k.

Answer. We do this by induction on k. For $k = 0$ i.e. p is constant, we have $\binom{x}{0} = 1$, and p is a multiple of it.

If $\deg p(x) < k$, then we already know it can be made from the $\binom{x}{i}$s, by induction.

Now, $\deg p(x) = k$, i.e. its leading term is cx^k. That is also the leading term of $ck!\binom{x}{k}$. So $p(x) - ck!\binom{x}{k}$ is of lower degree, so already handled by induction.