Math 120 Homework 1 Solutions

April 10, 2008

p. 21

6.) Note: addition is associative in each of these parts since it is inherited from $\mathbb{Q}$. It therefore suffices to check that the set in question is closed under addition and taking inverses (since $a + (-a) = 0$ will then force the set to contain the identity).

a. This is a group: if $\frac{a}{b}$ and $\frac{c}{d}$ are in lowest terms with b and d odd, then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ has bd odd. Eliminating any common factors with the numberator cannot produce an even denominator. Also $-\frac{a}{b} = \frac{-a}{b}$ has odd denominator.

b. This is not closed under addition: $\frac{1}{6} + \frac{1}{6} = \frac{1}{3}$.

c. This is not closed under addition: $\frac{1}{2} + \frac{1}{2} = 1$.

d. This is not closed under addition: $\frac{3}{2} + \frac{-1}{1} = \frac{1}{2}$.

e. This is a group (sometimes written $\frac{1}{2}\mathbb{Z}$). We can represent the given elements as $\frac{a}{2}$ where a may be even or odd. Then the sum of two such is $\frac{a}{2} + \frac{b}{2} = \frac{a+b}{2}$ which is in the set, and also $-\frac{a}{2} = \frac{-a}{2}$ is in the set.

f. This is not closed under addition: $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$.

10.) Suppose $G = \{g_1, ..., g_n\}$ is abelian. Then if a_{ij} represents the i, j entry in the group table, we have $a_{ij} = g_i g_j = g_j g_i = a_{ji}$ so the matrix is symmetric. On the other hand, if $a_{ij} = a_{ji}$ for all i, j then this says for each g_i, g_j we have $g_i g_j = a_{ij} = a_{ji} = g_j g_i$ so G is abelian.

20.) First note that $(x^n)^{-1} = (x^{-1})^n$ for all $n \geq 1$. This follows by induction. Indeed, $x^{-1} = (x^{-1})^1$. Suppose this holds for $k < n$. Then we may write $x^n(x^{-1})^n = x(x^{n-1}(x^{-1})^{n-1})x^{-1} = x(1)x^{-1} = xx^{-1} = 1$.

Next observe that for $n \geq 1$ we have $x^n = 1$ and $x^n(x^{-1})^n = 1$ together imply $1(x^{-1})^n = 1$ so $(x^{-1})^n = 1$ and since $x = (x^{-1})^{-1}$, symmetry implies $x^n = 1 \Leftrightarrow (x^{-1})^n = 1$. Thus the first positive power of x that gives 1 is also the first positive power of x^{-1} that gives 1, so $|x| = |x^{-1}|$ if $|x|$ is finite, and if $|x| = \infty$ then $x^n \neq 1$ for all $n > 0$ implies $(x^{-1})^n \neq 1$ for all $n > 0$ so that $|x^{-1}| = \infty$.

24.) First we'll show that $a^m b^n = b^n a^m$ for all $m, n \geq 0$ by induction on k, where

$0 \leq m, n < k$. If either $m = 0$ or $n = 0$ then the statement reduces to the fact that all elements commute with the identity, so we assume $m, n \geq 1$. If $1 \leq m, n < 2$, i.e. $m = n = 1$, then $a^m b^n = ab = ba = b^n a^m$ holds. Assume inductively that $a^m b^n = b^n a^m$ holds for all $0 \leq m, n < k$ where $k \geq 2$. Now take m, n with $1 \leq m, n < k + 1$. We have $a^m b^n = aa^{m-1} b^{n-1} b = ab^{n-1} a^{m-1} b$ where we have used the fact $a^{m-1} b^{n-1} = b^{n-1} a^{m-1}$, which is the inductive assumption. Now applying the same reasoning two more times, we get $(ab^{n-1})(a^{m-1} b) = (b^{n-1} a)(ba^{m-1}) = b^{n-1}(ab)a^{m-1} = b^{n-1} baa^{m-1} = b^n a^m$ as desired, and this completes the inductive step, so that $a^m b^n = b^n a^m$ holds for all $m, n \geq 0$.

Next we prove that $(ab)^n = a^n b^n$ for positive n. We have $(ab)^1 = a^1 b^1$ holds. Let $n > 1$ and inductively assume that $(ab)^{n-1} = a^{n-1} b^{n-1}$. Then $(ab)^n = (ab)(ab)^{n-1} = ab(a^{n-1} b^{n-1}) = aa^{n-1} bb^{n-1} = a^n b^n$ where we have used the fact $a^m b^n = b^n a^m$ from above. This completes the proposition for all $n > 0$.

For $n = 0$, $(ab)^0 = e = ee = a^0 b^0$.

For $n = -1$, observe $ab(a^{-1} b^{-1}) = baa^{-1} b^{-1} = beb^{-1} = bb^{-1} = e$ so $a^{-1} b^{-1} = (ab)^{-1}$. Note that $(ab)^{-1} = b^{-1} a^{-1}$ as well, so $a^{-1} b^{-1} = b^{-1} a^{-1}$ and a^{-1} and b^{-1} commute.

Finally for $n < 0$, $(ab)^{-|n|} = ((ab)^{-1})^{|n|} = (a^{-1} b^{-1})^{|n|}$, and since a^{-1} and b^{-1} commute, our above result for positive n implies that $(a^{-1} b^{-1})^{|n|} = (a^{-1})^{|n|} (b^{-1})^{|n|} = a^n b^n$ so that $(ab)^n = a^n b^n$ for negative n as well.

25.) We have, for all $x, y \in G$: $(xy)(xy) = 1$ so $(xyxy)yx = yx$. But now $xyxyyx = xyx(y^2)x = xy(x^2) = xy$ since $x^2 = y^2 = 1$. Thus $xy = yx$ and G is abelian.

30.) By componentwise multiplication, $(a, 1)(1, b) = (a, b) = (1, b)(a, 1)$ so $(a, 1)$ and $(1, b)$ commute. It follows by problem 25 that $(a, b)^n = (a, 1)^n (1, b)^n$ for all n. Now we claim that $(a, 1)^n = (a^n, 1)$ for positive n (this holds for negative n as well). Indeed, for $n = 1$, $(a, 1)^1 = (a^1, 1)$. For $n > 1$ if we assume $(a, 1)^{n-1} = (a^{n-1}, 1)$ then $(a, 1)^n = (a, 1)(a^{n-1}, 1) = (a^n, 1)$ so the claim holds for all positive n by induction. Similarly $(1, b)^n = (1, b^n)$ so $(a, b)^n = (a, 1)^n (1, b)^n = (a^n, 1)(1, b^n) = (a^n, b^n)$. In particular, for positive n, $(a, b)^n = (1, 1)$ if and only if $a^n = 1$ and $b^n = 1$. Thus if either $|a| = \infty$ or $|b| = \infty$ then $(a, b)^n \neq (1, 1)$ for all $n > 0$ so $|(a, b)| = \infty$ and $|(a, b)| = l.c.m.(|a|, |b|)$ in this case.

If both $|a|$ and $|b|$ are finite, then putting $l = l.c.m.(|a|, |b|)$ we have that $(a, b)^l = (a^l, b^l) = ((a^{|a|})^{l/|a|}, (b^{|b|})^{l/|b|}) = (1^{l/|a|}, 1^{l/|b|}) = (1, 1)$ so $|(a, b)|$ divides l. On the other hand, if $(a, b)^m = (1, 1)$ then $a^m = 1$ and $b^m = 1$ so $|a|$ divides m and $|b|$ divides m, so that l divides m. Hence l divides $|(a, b)|$ so we must have $l = |(a, b)|$ in this case as well.

Note: this solution makes use of the general fact that if $x^n = 1$ and $|x|$ is finite then $|x|$ divides n. (The stipulation that $|x|$ be finite is simply to avoid the case $n = 0$ and $|x| = \infty$ since if $n \neq 0$ then we know there is a finite positive power of x that is 1, namely either n or $-n$.) We can check this fact as follows: use the division algorithm to write $n = k|x| + r$ where $0 \leq r < |x|$. Then $x^n = (x^{|x|})^k x^r = 1^k x^r = x^r = 1$. Since $0 \leq r < |x|$, $r = 0$ because

$|x|$ is the least positive power of x that gives 1.

31.) As suggested in the hint, define $t(G)$ by $t(G) = \{g \in G : g \neq g^{-1}\}$. Define relation $\sim$ on $t(G)$ by $x \sim y$ means $x = y$ or $x = y^{-1}$. This defines an equivalence relation. Indeed, $x \sim x$, and $x \sim y$ means either $y = x^{-1}$, in which case $x = y^{-1}$, or $x = y$ which is symmetric. Finally $x \sim y$ and $y \sim z$ means $y = x^a$ and $z = y^b$ where a and b are ± 1. Then $z = x^{ab} = x^{\pm 1}$ so $x \sim z$. It follows that the equivalence classes of $\sim$ partition $t(G)$. Let x be in an equivalence class $\overline{x}$. Then $x^{-1} \neq x$ and $x \sim x^{-1}$ so $x^{-1} \in \overline{x}$ so that $\overline{x}$ has at least two members. It may have no more than two since every element is either x or x^{-1}. It follows that each equivalence class has two members, so the number of elements of $t(G)$ is twice the number of equivalence classes, hence is even.

Now observe $|G| = |t(G)| + |n(G)|$ where $n(G)$ is the collection of elements that are their own inverse. Since $|G|$ is even and $|t(G)|$ is even, $|n(G)|$ is even. Moreover, $n(G) \neq \emptyset$ since $1 \in n(G)$. So there is at least one other non-identity element of $n(G)$, say $y \in n(G)$. Then $y \neq 1$ and $y = y^{-1}$ so $|y| > 1$ but $|y| \leq 2$ so $|y| = 2$ as desired.

34.) Suppose $x^n = x^m$ for some $n < m$. Then $1 = x^{-n}x^n = x^{-n}x^m = x^{m-n}$. We have $m - n > 0$ but $x^{m-n} = 1$, a contradiction. Hence $x^n \neq x^m$ for all $n \neq m$.

p. 27

2.) If x is not a power of r then $x = sr^k$ for some $0 \leq k < n$. Then $rx = rsr^k = sr^{-1}r^k = sr^{k-1} = sr^k r^{-1} = xr^{-1}$ as desired.

p. 34

14.) Let $\sigma \in S_n$ have cycle decomposition $\sigma = \sigma_1 \dots \sigma_k$ where the σ_i are disjoint cycles. Since the cycles commute, we have $\sigma^m = \sigma_1^m \sigma_2^m \dots \sigma_k^m$ which follows by induction from problem 24 on page 22.

For each i, let A_i denote the subset of $\{1, 2, ..., n\}$ not fixed by the cycle σ_i, (that is, those elements contained in the cycle). Then the sets A_i, $i = 1, 2, ..., k$ are disjoint. Moreover if $x \in A_i$ then $\sigma^m(x) = \sigma_i^m(x)$ since $\sigma^m(x) = \sigma_i^m \circ (\prod_{j \neq i} \sigma_j^m)(x) = \sigma_i^m(x)$, where we have used the fact that the σ_j commute, together with $(\prod_{j \neq i} \sigma_j^m)$ is the compositions of maps that fix x, hence fixes x. Then it follows that $\sigma^m = 1$, the identity, if and only if $\sigma_i^m = 1$ for each i. Indeed, if $\sigma_i^m = 1$ for all i, then $\sigma^m = 1^k = 1$. But if $\sigma_i^m \neq 1$ for some i, then there exists $j \in A_i$ with $\sigma_i^m(j) \neq j$, hence $\sigma^m(j) = \sigma_i^m(j) \neq j$ and $\sigma^m \neq 1$.

Now assume $|\sigma| = p$. Then $\sigma_i^p = 1$ for all i. But for a cycle σ_i, σ_i^m moves the first element

in the cycle m positions to the right, where the rotation is taken modulo the length of the cycle. Hence $\sigma_i^m = 1$ if and only if the length $|\sigma_i|$ of σ_i divides m. It follows that if $\sigma^p = 1$ for prime p, then $|\sigma_i|$ divides p for each i, and since σ_i is not a trivial cycle, it must be a p cycle. Thus we've shown that an element σ of order p in S_n has a decomposition as a product of disjoint p cycles.

On the other hand, if $\sigma = \sigma_1 \dots \sigma_k$ where each σ_i is a p-cycle and the cycles are disjoint, then $\sigma^p = \sigma_1^p \dots \sigma_k^p = 1$ since each p-cycle has order p. Thus $|\sigma|$ divides p. We may not have $|\sigma| = 1$ since $\sigma_1^1 \neq 1$. Hence $|\sigma| \geq |\sigma_1|$ and $|\sigma|$ divides p forces $|\sigma| = p$.

To see that there exists elements of composite order m not obtained via m cycles, consider the permutation $\sigma = (1\ 2)(3\ 4\ 5)$ in S_5. We have $\sigma^2 = (3\ 5\ 4)$, $\sigma^3 = (1\ 2)$, $\sigma^4 = (3\ 4\ 5)$, $\sigma^5 = (1\ 2)(3\ 5\ 4)$ and $\sigma^6 = 1$ so $|\sigma| = 6$ but σ is the product of a 2-cycle and a 3-cycle in its cycle decomposition.

15.) For permutation $\sigma \in S_n$, let σ have cycle decomposition $\sigma = \sigma_1 \dots \sigma_k$, where the σ_i are disjoint cycles. As in the previous problem, $\sigma^m = \sigma_1^m \dots \sigma_k^m$ and $\sigma^m = 1$ if and only if $\sigma_i^m = 1$ for each i. Now for an s-cycle τ, $|\tau| = s$ because τ^j shifts each element in the cycle ahead j places in the cycle, where the rotation is taken modulo s. Hence if $\ell = l.c.m.(|\sigma_1|, \dots, |\sigma_k|)$ then $\sigma_i^\ell = (\sigma_i^{|\sigma_i|})^{\ell/|\sigma_i|} = 1$ for each i, so $\sigma^\ell = 1$ and $|\sigma|$ divides ℓ. But if $\sigma^m = 1$, then $\sigma_i^m = 1$ for each m, which implies $|\sigma_i|$ divides m for each i, that is ℓ divides m. Thus ℓ divides $|\sigma|$ and $|\sigma|$ divides ℓ, so $|\sigma| = \ell$.

p. 40

2.) We first check that $\phi(x^n) = \phi(x)^n$. For $n = 0$ this just states that $\phi(1) = 1$, which we can obtain by writing $1 = 1 \cdot 1$ so that $\phi(1) = \phi(1)\phi(1)$, which implies $\phi(1) = 1$ after cancelation. Writing $1 = xx^{-1}$ we then obtain $1 = \phi(1) = \phi(x)\phi(x^{-1})$ so $\phi(x^{-1}) = \phi(x)^{-1}$. For $n > 1$, $\phi(x^n) = \phi(x)\phi(x^{n-1}) = \phi(x)^n$ by induction. Then $\phi(x^{-n}) = \phi((x^{-1})^n) = \phi(x^{-1})^n = (\phi(x)^{-1})^n = \phi(x)^{-n}$ so that the proposition holds for all $n \in \mathbb{Z}$.

Now to prove the order relation, if $|x| < \infty$ we have $1 = \phi(1) = \phi(x^{|x|}) = \phi(x)^{|x|}$ so that $|\phi(x)| \leq |x|$ (which holds even if $|x| = \infty$). But if $\phi(x)^n = 1$ for $1 \leq n < |x|$ then $\phi(x^n) = \phi(x)^n = 1$ implies ϕ maps $x^n \neq 1$ to 1, so that ϕ is not injective, a contradiction. Thus $|\phi(x)| \geq |x|$ so $|\phi(x)| = |x|$.

For fixed n, let $A_n = \{x \in G : |x| = n\}$ and let $B_n = \{y \in H : |y| = n\}$. Our proof above shows that ϕ restricts to a map of A_n into B_n and the mapping is injective because ϕ is injective $G \to H$. But ϕ is surjective from G to H, so that every element of B_n is mapped to from an element of G. That element must have order n, hence was in A_n. Thus the restriction of ϕ to A_n is a bijection onto B_n and it follows that A_n and B_n have the same cardinality.

The condition $|\phi(x)| = |x|$ need not hold if ϕ is a homomorphism but not an isomorphism.

Indeed, one can check that the map $\phi(x) = 1$ is a homomorphism from G to the trivial group of one element, for any group G. The image of any element here has order 1.

17.) Suppose $\phi(g) = g^{-1}$ is a homomorphism. Then for all $x, y \in G$, $x^{-1}y^{-1} = \phi(x)\phi(y) = \phi(xy) = (xy)^{-1}$. Thus $x^{-1}y^{-1}xy = 1$, or multiplying by yx on the left, $xy = yx$ so x and y commute for all $x, y \in G$, that is G is abelian.

Now suppose that G is abelian and define $\phi : G \to G$ by $\phi(x) = x^{-1}$. We have $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$, where we used the commutativity of x^{-1} and y^{-1} in the next to last step. This proves that ϕ is a homomorphism.

20.) Let σ and τ be two isomorphisms $G \to G$. Note then that $\sigma \circ \tau$ also maps $G \to G$. We have $\sigma \circ \tau(xy) = \sigma(\tau(xy)) = \sigma(\tau(x)\tau(y)) = \sigma(\tau(x))\sigma(\tau(y)) = \sigma \circ \tau(x)\sigma \circ \tau(y)$ and this proves that $\sigma \circ \tau$ is a homomorphism $G \to G$.

Next we check that $\sigma \circ \tau$ is a bijection. Take $g \in G$. Then there exists h with $\sigma(h) = g$ since σ is surjective, and there exists k with $\tau(k) = h$ since τ is surjective. Hence $\sigma \circ \tau(k) = \sigma(h) = g$ and $\sigma \circ \tau$ is surjective. Finally, suppose $\sigma \circ \tau(x) = \sigma \circ \tau(y)$. Then as σ is injective, $\tau(x) = \tau(y)$. But then as τ is injective, $x = y$, which proves that $\sigma \circ \tau$ is injective, hence is bijective, so is an isomorphism. This proves that $Aut(G)$ is closed under function composition, and function composition is a well defined binary operation $Aut(G) \times Aut(G) \to Aut(G)$.

Since function composition is associative, the product on $Aut(G)$ is associative. The identity isomorphism is the identity $1(g) = g$ for all $g \in G$ ($1(xy) = xy = 1(x)1(y)$ so this is a homomorphism, and it is a bijection). We check: $\sigma \circ 1(g) = \sigma(g) = 1 \circ \sigma(g)$ for all $g \in G$ so 1 is indeed an identity in $Aut(G)$. For $\sigma \in Aut(G)$, the inverse is the set-theoretic inverse σ^{-1}. This is certainly a bijection $G \to G$, and it satisfies $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$, so we just need to check that it is a homomorphism to check that is the group-inverse of σ in $Aut(G)$. But if $\sigma(x') = x$ and $\sigma(y') = y$ then since σ is a homomorphism, $\sigma(x'y') = xy$ so that $\sigma^{-1}(xy) = x'y' = \sigma^{-1}(x)\sigma^{-1}(y)$ as desired. This completes the proof that $Aut(G)$ is a group.

p. 44

4.) a. Suppose g, h satisfy $ga = a$ and $ha = a$ for all $a \in A$. Then $gha = g(ha) = ga = a$ for all $a \in A$ and the kernel is closed under the group operation. Also $a = 1a = g^{-1}ga = g^{-1}a$ for all a so the kernel is closed under taking inverses. The kernel contains the identity, hence is non-empty, and is a subgroup.

b. 1 is in the stabilizer since $1a = a$, so the stabilizer is non-empty. If g and h are

in the stabilizer, the same two arguments above go through symbol for symbol, that is $gha = g(ha) = ga = a$ so gh is in the stabilizer, and $a = 1a = g^{-1}ga = g^{-1}a$ so g^{-1} is in the stabilizer. This proves that the stabilizer of a is a subgroup.

19.) We'll first check the statement of problem 18, that $a \sim b$ iff $a = hb$ some $h \in H$ defines an equivalence relation on A when H acts on A. Since $1a = a$ we have $a \sim a$. If $a \sim b$ then we have $a = hb$ some $h \in H$ so $h^{-1}a = h^{-1}hb = 1b = b$ and $b \sim a$. Finally if $a \sim b$ and $b \sim c$ then there exist $h, g \in H$ with $b = hc$ and $a = gb$. Then $a = ghc$ so $a \sim c$. This proves that $\sim$ is an equivalence relation.

Next we check that the stated map $H \to \mathcal{O}$, $h \mapsto hx$ is a bijection. If $h_1x = h_2x$ then applying x^{-1} on the right (in G), we get $h_1 = h_2$, so we have an injection. But then if $y \sim x$ then $y = hx$ some $h \in H$ so y is in the image of the map and so the mapping is a surjection, hence a bijection. It follows that $|\mathcal{O}| = |H|$ for all orbits $\mathcal{O}$ of the action. Now since the orbits $\mathcal{O}$ are exactly the equivalence classes of G under the equivalence relation $\sim$, they partition G. As $|G|$ is finite, it can have only finitely many equivalence classes under $\sim$, so there exist disjoint orbits $\mathcal{O}_1, \ldots, \mathcal{O}_k$ such that $G = \mathcal{O}_1 \cup \ldots \cup \mathcal{O}_k$. Then $|G| = \sum_{i=1}^{k} |\mathcal{O}_i|$, but for each $\mathcal{O}_i$, $|\mathcal{O}_i| = |H|$, so $G = k|H|$ and $|H|$ divides $|G|$, proving Lagrange's theorem.