Math 120 HW 2

Xiaoyu He, edits by Prof. Church

April 13, 2018

1.1.12

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.

Recall that the order $|g|$ of a group element g is the smallest positive integer n for which g^n is the multiplicative identity $\overline{1}$. In this case, $\overline{1} = \overline{13}$ are already the identity, $(\overline{-1})^2 = \overline{1}$, $(\overline{5})^2 = \overline{25} = \overline{1}$, $(\overline{7})^2 = \overline{49} = \overline{1}$, and $(\overline{-7})^2 = \overline{49} = \overline{1}$. Thus, $|\overline{1}| = |\overline{13}| = 1$ and $|\overline{-1}| = |\overline{5}| = |\overline{7}| = |\overline{-7}| = 2$.

1.1.13

Find the orders of the following elements of the additive group $(\mathbb{Z}/36\mathbb{Z})$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Since the group operation is addition, the order of an element g is actually the smallest n for which ng which is the additive identity $\overline{0}$. In other words, the order of $|\overline{x}|$ is the smallest n for which $\overline{nx} = \overline{0}$, i.e. nx is a multiple of 36. In general, the answer will be the smallest integer which contains all the prime factors of 36 that x is missing, which is

$$|\overline{x}| = \frac{36}{\gcd(x, 36)}.$$

From this formula, we easily check that the orders are $|\overline{1}| = 36, |\overline{2}| = 18, |\overline{6}| = 6, |\overline{9}| = 4, |\overline{10}| = 18, |\overline{12}| = 3, |\overline{5}| = 36, |\overline{13}| = 36, |\overline{-13}| = 36, |\overline{17}| = 36$.

1.6.13

Let G and H be groups and let $\varphi\colon G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1).

Recall (by 1.1.26 from the HW1) that to check a subset $\varphi(G) \subseteq H$ is a subgroup of H, we only need to verify three things:

1. $\varphi(G)$ contains the identity. Since any homomorphism satisfies $\varphi(1) = 1$, indeed $1 \in \varphi(G)$.
2. If $h, k \in \varphi(G)$, then so is hk. Since $h, k \in \varphi(G)$, by the definition of image there exist $g_h, g_k \in G$ such that $\varphi(g_h) = h$ and $\varphi(g_k) = k$. But then

$$\begin{aligned} hk &= \varphi(g_h)\varphi(g_k) \\ &= \varphi(g_h g_k) \end{aligned}$$

   because φ is a homomorphism. Thus $hk \in \varphi(G)$.
3. If $h \in \varphi(G)$, then so is h^{-1}. Since $h \in \varphi(G)$, by the definition of image there exists $g_h \in G$ such that $\varphi(g_h) = h$. But G is a group so g_h has an inverse $g_h^{-1} \in G$. Thus,

$$\begin{aligned} \varphi(g_h^{-1})h &= \varphi(g_h^{-1})\varphi(g_h) \\ &= \varphi(g_h^{-1} g_h) \\ &= \varphi(1_G) \\ &= 1_H. \end{aligned}$$

The second inequality is the group homomorphism property, the third is by definition of inverses, and the last is because homomorphisms take identity to identity. Thus, $\varphi(g_h^{-1}) = h^{-1}$ lies in $\varphi(G)$.

Prove that if φ is injective then $G \cong \varphi(G)$.

If φ is injective, then we claim that the map $\varphi\colon G \to \varphi(G)$ is a isomorphism, so a homomorphism and a bijection. To check that $\varphi\colon G \to \varphi(G)$ is a homomorphism, note that the group operation of $\varphi(G)$ is the same as the operation on H, so for any $x, y \in G$, $\varphi(x)\varphi(y) = \varphi(xy)$ by the fact that $\varphi\colon G \to H$ is a homomorphism. We are given that φ is injective, so it suffices to check that $\varphi\colon G \to \varphi(G)$ is surjective. But every $h \in \varphi(G)$ is equal to $\varphi(g)$ for some $g \in G$, by the definition of image. Thus φ is an isomorphism and $G \cong \varphi(G)$.

1.6.14

Let G and H be groups and let $\varphi\colon G \to H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G | \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that if the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G.

Write $\ker\varphi$ for the kernel of φ.We have to check three things:

1. $\ker\varphi$ contains the identity. Since φ is a homomorphism, $\varphi(1_G) = 1_H$, so $1_G \in \ker\varphi$.
2. If $h, k \in \ker\varphi$, then $hk \in \ker\varphi$. By the definition of kernel, $\varphi(h) = 1_H$ and $\varphi(k) = 1_H$. Thus,
$$\varphi(hk) = \varphi(h)\varphi(k) = 1_H$$
as well, using the fact that φ is a homomorphism. Thus $hk \in \ker\varphi$ as well.
3. If $h \in \ker\varphi$, then $h^{-1} \in \ker\varphi$. We know that for any homomorphism we have $\varphi(h^{-1}) = \varphi(h)^{-1}$. If $h \in \ker\varphi$, then $\varphi(h^{-1}) = \varphi(h)^{-1} = 1_H^{-1} = 1_H$, so $h^{-1} \in \ker\varphi$.

Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

(if direction.) If $\ker\varphi = \{1_G\}$, then suppose for the sake of contradiction that φ is not injective. That is, there exist two elements $g \neq h \in G$ for which $\varphi(g) = \varphi(h)$. But then
$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = 1_H,$$
and since $g \neq h$ this element gh^{-1} is not the identity but lies in $\ker\varphi$. This contradicts our assumption that $\ker\varphi = \{1_G\}$, so φ must be injective.

(only if direction.) If φ is injective, then $\varphi(g) \neq \varphi(h)$ for any $g \neq h \in G$. But $\varphi(1_G) = 1_H$, so that means that if $g \neq 1_G$, $\varphi(g) \neq 1_H$ and g doesn't lie in $\ker\varphi$. Thus, $\ker\varphi = \{1_G\}$ is the identity subgroup of G.

1.6.18

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Let φ be the map $g \mapsto g^2$.

(if direction.) Suppose G is abelian. We need to check the homomorphism property
$$\varphi(g)\varphi(h) = \varphi(gh)$$
for any two $g, h \in G$. But
$$\begin{aligned}\varphi(gh) &= (gh)^2 \\ &= ghgh \\ &= g^2h^2 \\ &= \varphi(g)\varphi(h)\end{aligned}$$

as desired. In the middle step we used commutativity $hg = gh$.

(only if direction.) If φ is a homomorphism, then for any $g, h \in G$, we have

$$\begin{aligned} \varphi(g)\varphi(h) &= \varphi(gh) \\ g^2h^2 &= (gh)^2. \end{aligned}$$

Multiplying the above equation on the left by g^{-1} and on the right by h^{-1}, we get

$$\begin{aligned} g^{-1}(g^2h^2)h^{-1} &= g^{-1}(ghgh)h^{-1} \\ gh &= hg, \end{aligned}$$

and so $gh = hg$ for any $g, h \in G$, proving that G is abelian.

2.1.8

Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

(if direction.) If $H \subseteq K$, then $H \cup K = K$ is a subgroup. If $K \subseteq H$, then $H \cup K = H$ is a subgroup.

(only if direction.) Suppose $H \cup K$ is a subgroup, and that $H \not\subseteq K$ and $K \not\subseteq H$. Then, there exists elements $h \in H \backslash K$ and $k \in K \backslash H$ which both lie in $H \cup K$.

We claim that $g = hk$ lies in neither H nor K. Without loss of generality, suppose $g \in H$. Then, $gh^{-1} = k$ also lies in H since H is a subgroup, which contradicts the fact that $k \in K \backslash H$. This is a contradiction, which proves the claim.

It follows that $H \cup K$ is not a subgroup because it's not closed under multiplication, and we have a contradiction. Thus either $H \subseteq K$ or $K \subseteq H$.

2.3.1

Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

By parts (1) and (3) of Theorem 2.3.7, every subgroup of a cyclic group is cyclic, and if $K \leq Z_{45}$ then $K = \langle x^d \rangle$ where d is a divisor of 45, and this subgroup is isomorphic to $Z_{45/d}$. Thus, the subgroups are $\langle x \rangle \cong Z_{45}, \langle x^3 \rangle \cong Z_{15}, \langle x^5 \rangle \cong Z_9, \langle x^9 \rangle \cong Z_5, \langle x^{15} \rangle \cong Z_3$, and $\langle x^{45} \rangle = \{1\}$.

They are ordered by containment in the opposite direction of divisibility; that is, $\langle x^d \rangle \subseteq \langle x^e \rangle$ if and only if e is a divisor of d. One way to see the containments nicely is to arrange them in a divisibility lattice like so:

$$\begin{array}{ccc} \langle x^5 \rangle & \subset & \langle x \rangle \\ \cup & & \cup \\ \langle x^{15} \rangle & \subset & \langle x^3 \rangle \\ \cup & & \cup \\ \langle x^{45} \rangle & \subset & \langle x^9 \rangle. \end{array}$$

Question 1

Does there exist some group K with the following property?

($*$) For every group G, the number of homomorphisms $f \colon K \to G$ is equal to the cardinality $|G|$ of G.

Describe such a group K and prove it has property ($*$), or prove that no such group K exists.

We prove that $K = \mathbb{Z}$, the infinite cyclic group, has property ($*$). For any group G, consider the function $\{\text{homomorphisms } f \colon \mathbb{Z} \to G\} \xrightarrow{\alpha} G$ defined by $\alpha(f) = f(1)$. We will prove that α is a bijection, which will show that $n(\mathbb{Z}, G) = |G|$.

First, we show that α is surjective; in other words, for any group G and any $g \in G$ there exists a homomorphism $f\colon \mathbb{Z} \to G$ with $f(1) = g$. Given $g \in G$, define the function $f_g\colon \mathbb{Z} \to G$ by $f_g(n) = g^n$ for all $n \in \mathbb{Z}$. Note that $f_g(1) = g$ by definition. We must check that f_g is a homomorphism:

$$f_g(m+n) = g^{m+n} = g^m \cdot g^n = f_g(m) \cdot f_g(n)$$

so f_g is indeed a homomorphism. This shows that α is surjective.

Second, we show that α is injective; in other words, if $f\colon \mathbb{Z} \to G$ and $f'\colon \mathbb{Z} \to G$ are two homomorphisms with $f(1) = f'(1)$, then $f = f'$.

We prove by induction on $n \geq 0$ that $f(n) = f'(n)$. Let g be the element $g = f(1) = f'(1)$. Our base cases are $n = 0$, since $f(0) = 1 = f'(0)$ for any homomorphisms, and $n = 1$ which is our assumption. Therefore assume by induction that $f(n) = f'(n)$. For the inductive step,

$$f(n+1) = f(n) \cdot f(1) = f(n) \cdot g = f'(n) \cdot g = f'(n) \cdot f'(1) = f'(n+1)$$

which completes the inductive step.

For any $m \geq 0$ we conclude that

$$f(-m) = f(m)^{-1} \neq f'(m)^{-1} = f'(-m)$$

so we also have $f(n) = f'(n)$ for all $n < 0$.

This proves that $f = f'$ and thus concludes the proof that α is injective.

Question 2

Let S be the set $S = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Note that in this question we will not really be considering S as a group, mostly just as a set. We'll say that a bijection $g\colon S \to S$ is adjacency-preserving if for all $s \in S$, either $g(s+1) = g(s) + 1$ or $g(s+1) = g(s) - 1$.

(a) How many adjacency-preserving bijections on S are there?

You do not have to list them all out (although you might want to give them names for the later parts) but you do need to justify why your answer is correct.

There are 8 adjacency-preserving bijections. They are f_0, f_1, f_2, f_3 and g_0, g_1, g_2, g_3 where $f_i(s) = i + s$ and $g_i(s) = i - s$. The point is that once $g(0)$ is chosen in one of $|S| = 4$ ways, there are two ways $g(0) \pm 1$ to choose $g(1)$, and then the other values $g(2), g(3)$ are determined by the adjacency-preserving property. [Note from TC: a bit more detail here was probably necessary for students, but not a ton more.] Thus, there are 8 total possibilities.

Let G be the set of adjacency-preserving bijections on S. You should convince yourself that G is a group under composition, but you do not have to prove it.

(b) Does G have a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}$? Prove or disprove.

The subgroup $H = \{f_0, f_1, f_2, f_3\}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ via the map $\varphi(f_i) = i$. Note that H is a subgroup because it's nonempty, closed under composition $f_i \circ f_j = f_{i+j}$, and closed under inverses $f_i^{-1} = f_{-i}$. The map is an isomorphism because it's a bijection and $\varphi(f_i) + \varphi(f_j) = i + j = \varphi(f_i \circ f_j)$.

(c) How many subgroups H of G containing 4 elements are there? (i.e. $|H| = 4$) Justify your answer.

We know that every element $h \in H$ has order dividing $|H| = 4$, so all elements have order 1 (for the identity), order 2, or order 4. There are only two elements of order 4 (f_1 and f_3), and any subgroup which contains one of them must be the subgroup $\{f_0, f_1, f_2, f_3\}$ described above.

Therefore any other subgroup of order 4 consists of the identity together with three elements of order 2. There are five elements of order 2, namely f_2, g_0, g_1, g_2, g_3. The key computation is that $g_i \circ g_j = f_{i-j}$ for any i and j. So for H to not contain f_1 or f_3, it must contain no pair $\{g_i, g_j\}$ for which $i - j$ is odd. For H to contain three out of five of f_2, g_0, g_1, g_2, g_3, it must therefore be either $H' = \{f_0, f_2, g_0, g_2\}$ or $H'' = \{f_0, f_2, g_1, g_3\}$. To check that H' and H'' are subgroups, the key computation is $f_2 \circ g_i = g_i \circ f_2 = g_{i+2}$ (in addition to the computation $g_i \circ g_j = f_{i-j}$ above).

There are three subgroups of order 4 in total.

(d) How many elements of G have order 1? order 2? order 3? order 4? order 5? and so on.

The identity is f_0, which is the unique element of order 1. The five elements f_2, g_0, g_1, g_2, g_3 all have order 2. The two elements f_1, f_3 have order 4. There are no elements of higher order.

(e) (open-ended, optional) Suppose that instead of $S = \mathbb{Z}/4\mathbb{Z}$ we had taken $S' = \mathbb{Z}/100\mathbb{Z}$, and built the group G' of adjacency-preserving bijections on S' . If you wanted to describe the structure of G' to a friend, can you come up with a better way than listing out all its elements and saying which ones multiply to what?

For the same reason as in (a), G' will contain 200 total bijections $f_i, g_i, 0 \leq i \leq 99$, where $f_i(s) = i + s$ and $g_i(s) = i - s$. In other words, $G' \cong D_{200}$, the dihedral group of order 200, which is the group of rotations and reflections of the 100-gon. [See Section 1.2 of the book.] The f_i correspond to rotations and the g_i to reflections.

Question 3

Let $Z_{12} = \langle x \rangle$ and $Z_9 = \langle y \rangle$. (i.e. $x^{12} = 1$ and $y^9 = 1$; see §2.3 for more on Z_n.)

For which integers $a \in \mathbb{Z}$ does there exist an homomorphism $f\colon Z_{12} \to Z_9$ with $f(x) = y^a$?

Since f is a homomorphism, it must be the case that $1 = f(1) = f(x^{12}) = f(x)^{12}$, so $f(x)$ must have order dividing 12. Since y has order 9, y^a has order dividing 12 if and only if a is divisible by 3, so f can only exist if a is divisible by 3. Conversely, if a is divisible by 3, define $f\colon Z_{12} \to Z_9$ by $f(x^b) = y^{ab}$. We must check that this is well-defined and a homomorphism. Note that $x^b = x^c$ in Z_{12} iff $b \equiv c \bmod 12$, i.e. if $c = b + 12\ell$ for some ℓ. To check that f is well-defined, we must check that $f(x^b) = y^{ab}$ is equal to $y^{ac} = f(x^c)$ in Z_9. Since a is divisible by 3, write $a = 3k$. Then we have

$$y^{ac} = y^{3kc} = y^{3k(b+12\ell)} = y^{3kb+36k\ell} = y^{3kb}y^{36k\ell} = y^{3kb}(y^9)^{4k\ell} = y^{3kb} \cdot 1 = y^{ab}$$

so f is a well-defined function.

To check that f is a homomorphism is actually easier: we just check that

$$f(x^i \cdot x^j) = f(x^{i+j}) = y^{a(i+j)} = y^{ai+aj} = y^{ai} \cdot y^{aj} = f(x^i) \cdot f(x^j).$$

For which integers $a \in \mathbb{Z}$ does there exist more than one such homomorphism?

There are no such a. A homomorphism out of a cyclic group is always uniquely determined by the image of any generator, so the condition $f(x) = y^a$ guarantees that there is always at most one such homomorphism.