MATH 4041 HW 5

David Chen, dc3451

October 11, 2020

Problem 1

We can induct on n for nonnegative n: we have that for $n = 0$, $f(g^0) = f(e_1)$, where e_1 is the identity element of G_1. Further, since we have that for every $g \in G_1$, $f(g) = f(e_1 g) = f(e_1)f(g)$, we have that $f(e_1)$ must be the identity of G_2, as we know that identities are unique in groups. Then, $f(g^0) = f(e_1) = (f(g))^0$.

Now, if $f(g^n) = (f(g))^n$, then

$$f(g^{n+1}) = f(g^n g) = f(g^n)f(g) = (f(g))^n f(g) = (f(g))^{n+1}$$

So we have that $f(g^n) = (f(g))^n$ holds for $n \geq 0$. Now for $n < 0$, we have by the result for $n > 0$ that $f(g^n) = f((g^{-1})^{-n}) = (f(g^{-1}))^{-n}$. Further, since we have that $f(e_1) = f(g^{-1}g) = f(g^{-1})f(g)$, and since the identity element in G_2 is exactly $f(e_1)$, as shown earlier, by the definition of inverses, $f(g^{-1}) = f(g)^{-1}$. Then, we have that $f(g^n) = (f(g^{-1}))^{-n} = ((f(g))^{-1})^{-n} = (f(g))^n$.

Thus, if g has finite order in G_1, then there is some $n \in \mathbb{Z}$ such that $g^n = e_1$. Then $f(e_1) = f(g^n) = (f(g))^n$, and since $f(e_1)$ is the identity in G_2, we have that $f(g)$ has also order at most n, and thus has finite order. The same result holds, since f admits another isomorphism $f^{-1} : G_2 \to G_1$, so if $f(g)$ has finite order, then there is some $m \in \mathbb{Z}$ such that $(f(g))^m = f(e_1)$, so $f^{-1}((f(g))^m) = f^{-1}(f(e_1)) = e_1$. Then, $f^{-1}((f(g))^m) = f^{-1}(f(g^m)) = g^m$, so $g^m = e_1$ so we have that g has finite order of at most m.

From above, we also can see that the order of $f(g)$ is at most n, the order of g, and the order of g is at most m, the order of $f(g)$. Thus, $n \leq m$ and $m \leq n \implies n = m$.

Problem 2

Write 1 as the identity element in G.

The least common multiple of d_1 and d_2 is the least $n \in \mathbb{N}$ such that $n = d_1 k_1$ and $n = d_2 k_2$ for integers k_1, k_2. Then, we have that $(gh)^n = g^n h^n = g^{d_1 k_1} h^{d_2 k_2} = (g^{d_1})^{k_1} (h^{d_2})^{k_2} = 1^{k_1} 1^{k_2} = 1$

(commutativity is used in the first equality), so gh has order at most n. Since we know that the least common multiple of d_1 and d_2 for finite d_1, d_2 is at most $d_1 d_2$, gh must have finite order when g, h have finite order.

This is not always true: consider in $\mathbb{Z}_2$ that $[1]$ has order 2, but $[1] + [1] = [0]$ has order 1, whereas the least common multiple of 2 and $2 > 1$.

If g has finite order and h has finite order, then gh cannot have finite order. To see this, note that $h^n = 1 \implies (h^{-1})^n = (h^n)^{-1} = 1^{-1} = 1$ (the first equality follows from $h^n h^{-n} = (hh^{-1})^n = 1 \implies (h^{-1})^n = h^{-n} = (h^n)^{-1}$), so h^{-1} is of order n as well. Then, if gh has finite order, we have that $g = (gh)h^{-1}$ as the product of two elements of finite order must have finite order, so $\Rightarrow\Leftarrow$ and gh cannot have finite order.

If g, h both have infinite order, gh may have finite order: consider that -1 and 1 both have infinite order in $\mathbb{Z}$ under addition, but $-1 + 1 = 0$ has order 1 in $\mathbb{Z}$.

Problem 3

We need to show that $H = \{g \in G \mid g^n = 1\}$ contains the identity, inverses, and is closed. The identity satisfies that $1^n = 1$, so $1 \in H$. Then, we have that $g^n = 1 \implies (g^{-1})^n = (g^n)^{-1} = 1^{-1} = 1$ (first equality was shown in one of the proofs for a question in problem 2) so every element in H has an inverse in H. Lastly, if $g^n = 1, h^n = 1$, we have that since G is abelian $1 = g^n h^n = (gh)^n$, so $gh \in H$ as well.

Problem 4

Again, we need to check that $H = \{g \in G \mid \exists N \in \mathbb{N} \text{ s.t. } g^N = 1\}$ contains the identity, inverses, and is closed. First, we have that $1^1 = 1$, so $1 \in H$. Again, if $g^N = 1$, we have from the last problem that $(g^{-1})^N = 1$ and so $g^{-1} \in H$. Lastly, we have from problem 2 that since $g, h \in H$ have finite order, gh must also have finite order at most the lcm of the orders of g and h, and thus $gh \in H$.

Problem 5

i

We have that $A_\theta A_\theta = A_{2\theta}$ from earlier homework, so $(A_\theta)^n = A_{n\theta}$. Then, we have that $(A_{2\pi/n})^n = A_{2\pi} = I$. If $0 < m < n$, then we have that $(A_{2\pi/n})^m = A_{2m\pi/n}$, where $0 < m/n < 1$. However, as shown in earlier homework, $A_\theta = I$ if and only if $\theta = 2\pi k$ for some integer k. Since there is no such integer m/n where $0 < m/n < 1$, we have that $(A_{2\pi/n})^m \neq I$, so we have that n is the least positive integer such that $(A_{2\pi/n})^n = I$, so $A_{2\pi/n}$ has order n.

The elements of finite order are exactly A_θ where $\theta = 2\pi r$ for some $r \in \mathbb{Q}$. To see that this is sufficient, we have that if $r = p/q$, then $(A_{2\pi r})^q = A_{2p\pi} = I$, so $A_{2\pi r}$ has order at most q. Further, if $\theta \neq 2\pi r$ for any $r \in \mathbb{Q}$, we have that $\theta = 2\pi x$ for some irrational $x \in \mathbb{R}$. Then, we have that if there is some $n \in \mathbb{N}$ such that $(A_{2\pi x})^n = I$, then $2\pi nx = 2\pi k$ for some $k \in \mathbb{Z}$, so $x = n/k \implies x \in \mathbb{Q}$, so $\Rightarrow\Leftarrow$ and A_θ must be of the form $\theta = 2\pi r$ for $r \in \mathbb{Q}$.

In the second homework, we showed that $B_\theta B_\theta = I$, so $(B_\theta)^2 = I$ and thus B_θ always has order 2 (note that the only element in a group with order 1 is the identity, and $B_\theta \neq I$ for any θ, as we would need that $\cos(\theta) = -\cos(\theta) = 1$, which is clearly impossible).

ii

We have from the second homework that $B_{\theta_1} B_{\theta_2} = A_{\theta_1 - \theta_2}$. Then, from earlier, we know that this has finite order if and only if $\theta_1 - \theta_2 = 2\pi r$ for some $r \in \mathbb{Q}$.

Problem 6

i

Every element of $\langle(3, -5)\rangle$ is given by $n(3, -5)$ for some n. Then, since the operation is defined componentwise, we have that $n(3, -5) = (n3, n(-5)) = (3n, -5n)$, so we have that

$$\langle(3, -5)\rangle = \{(3n, -5n) \mid n \in \mathbb{Z}\} = \{\dots, (-6, 10), (-3, 5), (0, 0), (3, -5), (6, -10) \dots\}$$

ii

To show that it is a proper subgroup, we only need to show that there is some element in $\mathbb{Z} \times \mathbb{Z}$ that is not contained in $\langle(a, b)\rangle$ for any given (a, b) (in particular, we already showed that this would be a subgroup in class).

If $(a, b) = (0, 0)$, then $\langle(a, b)\rangle = \{(0, 0)\}$, as we have that $n(0, 0) = (0n, 0n) = (0, 0)$ for any n. This is clearly a proper subgroup of $\mathbb{Z} \times \mathbb{Z}$.

If $(a, b) \neq (0, 0)$, then we can show that $(-b, a) \notin (a, b)$. Suppose that $n(a, b) = (-b, a)$ for some $n \in \mathbb{Z}$. Then, we have that since $0(a, b) = (0, 0)$, we have that $n \neq 0$ as well. Since we have that for any n, $n(a, b) = (na, nb)$, if we have $n(a, b) = (-b, a)$, then $na = -b$ and $nb = a$. Then, $na(a) = -b(nb) \implies na^2 = -nb^2 \implies a^2 = -b^2$ (we can cancel the n since we already know $n \neq 0$). However, $b \in \mathbb{Z} \implies b^2 \geq 0 \implies a^2 = -b^2 \leq 0$, but $a \in \mathbb{Z} \implies a^2 \geq 0$. Thus, the only option is that $a^2 = -b^2 = 0 \implies a = b = 0$, but is contrary to the initial assumption that $(a, b) \neq (0, 0)$. $\Rightarrow\Leftarrow$, so $\langle(a, b)\rangle$ does not contain $(-b, a)$, and is thus a proper subgroup of $\mathbb{Z} \times \mathbb{Z}$.

Problem 7

Note that repeated addition in $\mathbb{Q}$ is just multiplication by an integer, so $\sum_{i=1}^{n} r = nr$ in the sense of multiplication in $\mathbb{Q}$, so being able to cancel something like $r/2 = nr$ to $1/2 = n$ is not just a coincidence of notation.

Suppose that $r/2 \in \langle r \rangle$, such that $r/2 = nr$ for some $n \in \mathbb{Z}$. Then, $1/2 = n$, which clearly is not an integer, so $r/2$ cannot be generated by r.

Problem 8

Write 1 as the identity of G.

We need to show it contains the identity, inverses, and is closed. First, since H_1, H_2 are subgroups, $1 \in H_1$ and $1 \in H_2$, so $1 \in H_1 \cap H_2$. Next, $g \in H_1 \cap H_2 \implies g \in H_1$ and $g \in H_2$, and since H_1, H_2 are subgroups, each much contain inverses for their elements, so $g \in H_1 \implies g^{-1} \in H_1$ and $g \in H_2 \implies g^{-1} \in H_2$, so $g^{-1} \in H_1 \cap H_2$. Lastly, if $g, h \in H_1 \cap H_2$, we have that since subgroups are closed, $g, h \in H_1 \implies gh \in H_1$ and $g, h \in H_2 \implies gh \in H_2$, so $gh \in H_1 \cap H_2$.

Problem 9

We have that H is a subgroup, so it contains the identity, inverses, and is closed. We want to show the same things for $f(H)$. Earlier in the homework (problem 1) we showed that if f is an isomorphism and e_1 is the identity of G_1, then $f(e_1)$ is the identity of G_2, so $e_1 \in H \implies f(e_1) \in f(H)$, so $f(H)$ contains the identity of G_2, which will be written e_2.

Since $e_2 = f(e_1) = f(gg^{-1}) = f(g)f(g^{-1})$, we have that $(f(g))^{-1} = f(g^{-1})$. Thus, given any $f(g) \in f(H)$, we have that since H is a subgroup $g^{-1} \in H \implies (f(g))^{-1} = f(g^{-1}) \in f(H)$. Lastly, given any two $f(g), f(h) \in f(H)$, we have that $f(g)f(h) = f(gh)$. However, $g, h \in H \implies gh \in H$ since H as a subgroup is closed, so $f(g)f(h) = f(gh) \in f(H)$.