

MATH 113 HOMEWORK 2 SOLUTIONS

1. BASIC PROBLEMS

Divisibility.

Problem 1.1. Let a and b be integers and let n be a natural number. Let $d = \gcd(a, n)$. Show that the equation

$$ax \equiv b \pmod{n}$$

has a solution if and only if $d|b$.

Solution: Suppose that $ax \equiv b \pmod{n}$ has a solution. Then there is some integer c such that $n|(ac - b)$. Hence there is another integer e such that $en = ac - b$. Thus $b = ac - en$. Since $d|a$ and $d|n$, we have $d|(ac - en)$, i.e. $d|b$.

Suppose on the other hand that $d|b$. Then there exists an integer c such that $cd = b$. By the GCD theorem, there exist integers p and q such that $d = pa + qn$. Hence we have $b = cd = cpa + cq n$, which we can rewrite as $cpa - b = (-cq)n$. Hence $n|(cpa - b)$, so cp is a solution to $ax \equiv b \pmod{n}$.

Problem 1.2. Do Judson, Ch. 2 Additional Exercises 1-4 (you can skip the programming exercise 1(e)). These are the exercises on UPC symbols and ISBN codes.

Exercise 1: This is a computation; come ask at office hours if you're stumped. Part (d) is wrong; the error detection scheme does not detect the example transposition error.

Exercise 2: Let $w_1, \dots, w_k \in \mathbb{Z}$ be fixed. We want to show that the error-detection scheme

$$(d_1, \dots, d_k) \cdot (w_1, \dots, w_k) \equiv 0 \pmod{n}$$

detects all single-digit errors if and only if $\gcd(w_i, n) = 1$ for all i . So, suppose that (d_1, \dots, d_k) is a correct sequence for this scheme, i.e. suppose that for each i , we have $0 \leq d_i < n$, and suppose further that

$$(d_1, \dots, d_k) \cdot (w_1, \dots, w_k) \equiv 0 \pmod{n}.$$

Suppose that an error is introduced, changing the ℓ th digit d_ℓ to a different digit $d'_\ell \neq d_\ell$, with $0 \leq d'_\ell < n$ also. We will show that our error-detection scheme detects all such errors in the ℓ th position if

and only if $\gcd(w_\ell, n) = 1$.

Subtract the quantity

$$(d_1, \dots, d_k) \cdot (w_1, \dots, w_k) \equiv 0 \pmod{n}$$

from

$$(d_1, \dots, d_{\ell-1}, d'_\ell, d_{\ell+1}, \dots, d_k) \cdot (w_1, \dots, w_k).$$

We get that

$$(d_1, \dots, d_{\ell-1}, d'_\ell, d_{\ell+1}, \dots, d_k) \cdot (w_1, \dots, w_k) = (d'_\ell - d_\ell)w_\ell \pmod{n}.$$

The error is detected if and only if the right-hand quantity is not 0 mod n , i.e. if and only if

$$(d'_\ell - d_\ell)w_\ell \not\equiv 0 \pmod{n}.$$

So *all* such errors are detected if and only if the equation

$$x \cdot w_\ell \equiv 0 \pmod{n}$$

has only the trivial solution $x = [0]$. I claim that this is true if and only if $\gcd(w_\ell, n) = 1$.

To see this, suppose first that $\gcd(w_\ell, n) = 1$. Then w_ℓ has a multiplicative inverse mod n , say $c \in \mathbb{Z}$ such that $c \cdot w_\ell \equiv 1 \pmod{n}$. Then from

$$x \cdot w_\ell \equiv 0 \pmod{n}$$

we deduce that

$$x \equiv x \cdot w_\ell \cdot c \equiv 0 \pmod{n},$$

so $[x] = 0$ is the only solution. On the other hand, suppose that $\gcd(w_\ell, n) \neq 0$. Then the order of w_ℓ as an element of $\mathbb{Z}/n\mathbb{Z}$ is n/d , which is less than n , so $[x] = [n/d]$ is a nontrivial solution to the equation

$$x \cdot w_\ell \equiv 0 \pmod{n}.$$

Exercise 3: The proof is essentially identical to that of Exercise 2.

The difference is that we subtract

$$(d_1, \dots, d_i, \dots, d_j, \dots, d_k) \cdot (w_1, \dots, w_k) \equiv 0 \pmod{n}$$

from

$$(d_1, \dots, d_j, \dots, d_i, \dots, d_k) \cdot (w_1, \dots, w_k)$$

to get

$$(d_i - d_j)w_i + (d_j - d_i)w_j,$$

which we can rewrite as $(d_i - d_j)(w_i - w_j)$. So we get that

$$(d_1, \dots, d_j, \dots, d_i, \dots, d_k) \cdot (w_1, \dots, w_k) \equiv (d_i - d_j)(w_i - w_j) \pmod{n}$$

Hence if we swap two digits d_i and d_j which are not already equal, then all such errors are detected if and only if the equations

$$x(w_i - w_j) \equiv 0 \pmod{n}$$

have only the trivial solution $x = [0]$. This is the same as asking that $\gcd(w_i - w_j, n) = 1$, as we saw above.

Exercise 4: (b) The method detects all single-digit and transposition errors, since each w_i and each difference $w_i - w_j$ is relatively prime to 11.

(c) The digit d_10 is totally determined by the first nine digits, which can be chosen freely from 0 through 9. So there are 10^9 (1 billion) possible ISBN codes.

(e) We are given some German ISBN code $3450d_5 \cdots d_{10}$, such that

$$(3, 4, 5, 0, d_5, \dots, d_{10}) \cdot (10, 9, \dots, 1) \equiv 0 \pmod{11}.$$

We want to find digits a, b, c such that

$$(1, a, b, c, d_5, \dots, d_{10}) \cdot (10, 9, \dots, 1) \equiv 0 \pmod{11}.$$

Subtract the first equation from the second. We get that

$$(-2) \cdot 10 + (a - 4) \cdot 9 + (b - 5) \cdot 8 + c \cdot 7 \equiv 0 \pmod{11},$$

so

$$9a + 8b + 7c \equiv 20 + 36 + 40 \equiv 8 \pmod{11}.$$

Hence $a = 0, b = 1, c = 0$ is one solution (there are many!).

Groups and Subgroups.

Problem 1.3. Let (G, \circ) and (H, \star) be two groups. Define the *direct product* $(G, \circ) \times (H, \star)$ to be the set $G \times H$ with the operation $(g_1, h_1)(g_2, h_2) = (g_1 \circ g_2, h_1 \star h_2)$. Show that this operation makes $G \times H$ into a group. We often write $G \times H$ for $(G, \circ) \times (H, \star)$ when the operations \circ and \star are understood.

Solution: All of this is a matter of boiling down the properties for $G \times H$ to the properties for G and H . As an example, to show that $G \times H$ has inverses, I claim that $(g, h)^{-1} = (g^{-1}, h^{-1})$. Indeed, we have

$$(g, h)(g^{-1}, h^{-1}) = (g \circ g^{-1}, h \star h^{-1}) = (e_G, e_H),$$

which is the identity element for $G \times H$ (as you must check). Likewise for $(g^{-1}, h^{-1})(g, h)$. The proofs for the identity and associativity are done in exactly the same way.

Problem 1.4. Do Judson, Ch. 2 Exercises 10, 16, 17, 32, 39, and 52.

Exercise 10: This is a definition-check and a computation. Ask at office hours if you didn't get this one.

Exercise 16: A simple example: let $G = S_3$, $g = (12)$, $h = (23)$, and $n = 2$. Then $gh = (123)$ and so $(gh)^2 = (132)$. On the other hand, $g^2 = 1$ and $h^2 = 1$, so $g^2h^2 = 1 \neq (132)$.

Exercise 17: Here are four different examples: $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and Q_8 (the quaternions). The first three are abelian, so clearly none is equal to Q_8 . $\mathbb{Z}/8\mathbb{Z}$ is cyclic, whereas a quick computation shows that the other groups are not. So it remains to see that $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ cannot be the same as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To see this, note that in the latter group, all elements have order 1 or 2, whereas the element $(1, 0) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 4. It turns out that there is only one more example: the group of symmetries of the square is the last group of order 8 (although we need to say what it means for two groups to be “the same.” We will in Chapter 8.)

Exercise 32: Consider first the cyclic subgroups generated by the various elements in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$; these are:

- (1) The trivial subgroup, $\{(0, 0)\}$,
- (2) $\langle(1, 0)\rangle = \langle(2, 0)\rangle = \{(0, 0), (1, 0), (2, 0)\}$,
- (3) $\langle(1, 1)\rangle = \langle(2, 2)\rangle = \{(0, 0), (1, 1), (2, 2)\}$,
- (4) $\langle(1, 2)\rangle = \langle(2, 1)\rangle = \{(0, 0), (1, 2), (2, 1)\}$,
- (5) $\langle(0, 1)\rangle = \langle(0, 2)\rangle = \{(0, 0), (0, 1), (0, 2)\}$.

I claim that these, together with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ itself, are all of the subgroups of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. To see this, suppose that we have a subgroup H which is *not* cyclic. Then H contains two elements (a, b) and (c, d) , neither of which is a multiple of the other. Then either $a \neq 0$ or $c \neq 0$, so assume WLOG that $a \neq 0$. Then a has an inverse mod 3; writing this as a^{-1} , we have that $(c, d) - ca^{-1}(a, b)$ has 0 as its first coordinate, but is nonzero (since (c, d) is not a multiple of (a, b)); this element is either $(0, 1)$ or $(0, 2)$, so in either case, some multiple of this element is $(0, 1)$, and hence H contains $(0, 1)$. The same argument applied to the second coordinate shows that H also contains $(1, 0)$. Hence for every element $(e, f) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, we have H contains $(e, f) = e(1, 0) + f(0, 1)$, hence $H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. (This week we will see how to avoid all of this work using Lagrange’s Theorem).

Exercise 39: Clearly G is non-empty. Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be two elements of G . Then

$$(a + b\sqrt{2})(c + d\sqrt{2})^{-1} = (a + b\sqrt{2})\frac{c - d\sqrt{2}}{c^2 + 2d^2} = \frac{ac - 2bd}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2}\sqrt{2} \in G.$$

Hence G is a subgroup of \mathbb{R}^* .

Exercise 52: The statement is utterly false. Let G be *any* nonabelian group and let $g \in G$ be any non-identity element (such an element must exist since the trivial group is abelian). Then the cyclic subgroup of G generated by g is a nontrivial abelian subgroup of G .

Problem 1.5. Define an equivalence relation \sim on \mathbb{Q} by $a \sim b$ if $a - b \in \mathbb{Z}$. We write \mathbb{Q}/\mathbb{Z} for \mathbb{Q}/\sim . Show that:

- (1) The relation \sim is in fact an equivalence relation.
- (2) If $a, b \in \mathbb{Q}$ and $0 \leq a < b < 1$, then $[a] \neq [b]$. Conclude that \mathbb{Q}/\mathbb{Z} is infinite.
- (3) The operation $+$ on \mathbb{Q}/\mathbb{Z} defined by $[a] + [b] = [a + b]$ is well-defined.
- (4) $(\mathbb{Q}/\mathbb{Z}, +)$ is an abelian group.
- (5) Every element of \mathbb{Q}/\mathbb{Z} has finite order. More specifically, if $a/b \in \mathbb{Q}$ is a proper fraction in lowest terms, calculate the order of $[a/b]$ in \mathbb{Q}/\mathbb{Z} .
- (6) The operation \cdot on \mathbb{Q}/\mathbb{Z} defined by $[a] \cdot [b] = [a \cdot b]$ is *not* well-defined.

Solution: (1) Reflexivity and Symmetry are straightforward. Suppose $a \sim b$ and $b \sim c$. Then $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$, so

$$a - c = (a - b) + (b - c) \in \mathbb{Z},$$

hence $a \sim c$, so \sim is transitive.

(2) Recall that $[a] = [b]$ if and only if $a \sim b$. Suppose $0 \leq a < b < 1$. Then we have $0 < b - a < 1$, so $b - a \notin \mathbb{Z}$, and hence $a \not\sim b$, so $[a] \neq [b]$. Hence \mathbb{Q}/\mathbb{Z} has a distinct equivalence class for each rational number a with $0 \leq a < 1$; since there are infinitely many such numbers, \mathbb{Q}/\mathbb{Z} is infinite. (For those who know/care, this set is *countably* infinite; the map $[0, 1) \cap \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$ sending a to $[a]$ is a bijection).

(3) Suppose that $[a] = [a']$ and $[b] = [b']$. Then $a - a' \in \mathbb{Z}$ and $b - b' \in \mathbb{Z}$. Hence

$$(a + b) - (a' + b') = (a - a') + (b - b') \in \mathbb{Z},$$

so $[a + b] = [a' + b']$, hence $+$ is well-defined.

(4) Associativity follows immediately from associativity of addition on \mathbb{Q} ; for $a, b, c \in \mathbb{Q}$ we have

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]).$$

Similarly one checks that $[0]$ is the identity element of \mathbb{Q}/\mathbb{Z} and that $-[a] = [-a]$ (recall we use $-$ to denote inverses when the operation in question is $+$).

(5) Note that indeed every element in \mathbb{Q}/\mathbb{Z} can be written as $[a/b]$ where a/b is a proper fraction, i.e. $0 \leq a < b$; if a/b is any element of \mathbb{Q} , use the division algorithm to write $a = bq + r$ where $0 \leq r < b$. Then $a/b = q + r/b$, so $a/b - r/b \in \mathbb{Z}$, i.e. $[a/b] = [r/b]$; replacing a/b by r/b does the job. Likewise we can assume a/b is in lowest terms, i.e. $\gcd(a, b) = 1$; indeed, just divide a and b by $\gcd(a, b)$ to

obtain such an expression.

So, now, assume that a/b is a proper fraction in lowest terms with $a \neq 0$. I claim that $o([a/b]) = b$. To prove this, note first that by definition of \sim , for any $q \in \mathbb{Q}$, we have $[q] = [0]$ if and only if $q \in \mathbb{Z}$. So $o([a/b])$ is the smallest positive integer n such that $n \cdot (a/b) \in \mathbb{Z}$. This is equivalent to saying that $b|na$. Since $\gcd(a, b) = 1$, this holds true if and only if $b|n$; since the smallest positive n such that $b|n$ is b , we have $o([a/b]) = b$.

(6) If this operation were well-defined, we would have, for example, that $[1/4] = [1/2] \cdot [1/2] = [3/2] \cdot [1/2] = [3/4]$ which is false since $3/4 - 1/4 = 1/2 \notin \mathbb{Z}$.

Problem 1.6. Let G be a group with identity e and suppose that $a^2 = e$ for all $a \in G$. Show that G is abelian.

Solution: Let $a, b \in G$ be arbitrary. By assumption, $e = a^2 = a \cdot a$, so $a = a^{-1}$. Likewise, $b = b^{-1}$. Then we have

$$e = (ab)^2 = abab = aba^{-1}b^{-1}.$$

Multiplying on the right by ba yields $ba = aba^{-1}b^{-1}ba = ab$. Hence G is a abelian.

Note: When I took my first abstract algebra course, this was the first really good problem on the first homework assignment; it stumped me for a while. Maybe you got it right away, but I had a lot of fun thinking about it.

Cyclic Groups and Subgroups.

Problem 1.7. Do Judson, Ch.3 Exercises 4, 5, 6, 9.

Note: All are computations following directly from what we've done in class. If you want to see these worked through, come to office hours and ask.

Problem 1.8. Let a and b be integers. Show that $H = \{na+mb \mid n, m \in \mathbb{Z}\}$ is a subgroup of \mathbb{Z} . This is called the *subgroup generated by a and b* . Since \mathbb{Z} is cyclic, H must also be cyclic. Find the generator of H in terms of a and b (with proof!).

Solution: We check that H is a subgroup using the “two-part criterion.” We have that H is nonempty since $0 = 0a + 0b \in H$. Suppose that $x, y \in H$ are arbitrary. Then $x = na + mb$ and $y = pa + qb$ for some $n, m, p, q \in \mathbb{Z}$. We have $x - y = (n - p)a + (m - q)b \in H$; hence H is a subgroup of \mathbb{Z} .

Suppose that one of a or b is 0. WLOG we can assume $a = 0$. Then $H = \{n \cdot 0 + mb \mid n, m \in \mathbb{Z}\} = b\mathbb{Z}$, so H is cyclic with

generator b . Suppose on the other hand that neither a nor b is 0. Let $d = \gcd(a, b)$. I claim that $H = d\mathbb{Z}$. Indeed, we have that $d \in H$ since, by the GCD theorem, $d = na + mb$ for some $n, m \in \mathbb{Z}$; hence $d\mathbb{Z} = \langle d \rangle \subseteq H$. And since $d|a$ and $d|b$, we have that $d|(pa + qb)$ for all $p, q \in \mathbb{Z}$, so $H \subseteq d\mathbb{Z}$. Thus $H = d\mathbb{Z}$, as desired.

Problem 1.9. Prove or disprove: the group $(\mathbb{Q}, +)$ is cyclic.

Solution: The group $(\mathbb{Q}, +)$ is *not* cyclic. We prove this by contradiction: suppose that \mathbb{Q} were cyclic with generator $a/b \in \mathbb{Q}$; we clearly can assume $a \neq 0$ since \mathbb{Q} is not the trivial group. Then every element of \mathbb{Q} is of the form $n \cdot \frac{a}{b}$ for some $n \in \mathbb{Z}$. In particular, we have $\frac{a}{2b} = n \cdot \frac{a}{b}$ for some $n \in \mathbb{Z}$. Cross-multiplying, we have $ab = 2nab$. Dividing by the nonzero number ab , we have $2n = 1$; this is a contradiction since $n \in \mathbb{Z}$. Hence no such generator a/b exists, so $(\mathbb{Q}, +)$ is not cyclic.

2. CREATIVE PROBLEMS

Problem 2.1. Do Judson Ch.3 Exercise 13.

Solution: This one is hard. Calculation yields that $U(n)$ is cyclic for $n = 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19$, and not cyclic for $n = 8, 12, 15, 16, 20$. Here are a few example conjectures (each of which is true):

- (1) The group $U(4n)$ is *not* cyclic for $n \geq 2$.
- (2) The group $U(n)$ is cyclic for n prime.
- (3) The group $U(n)$ is cyclic for $n = 2p$ where p is a prime.
- (4) If n is an odd number such that $U(n)$ is cyclic, then $U(2n)$ is cyclic also.
- (5) If p and q are odd primes, then $U(pq)$ is *not* cyclic.

Among these, we can prove (1): we will do this by showing that the group $U(4n)$ has two different elements of order 2, and hence cannot be cyclic. Consider the element $[2n - 1] \in \mathbb{Z}/4n\mathbb{Z}$. I claim that this element is a unit, i.e. that $\gcd(2n - 1, 4n) = 1$. We have that $2 = 1 \cdot 4n + (-2) \cdot (2n - 1)$, and so

$$\begin{aligned} 1 &= (-1) \cdot (2n - 1) + n \cdot 2 \\ &= (-1) \cdot (2n - 1) + n \cdot (4n) + (-2n) \cdot (2n - 1), \end{aligned}$$

and hence 1 is an integer linear combination of $2n - 1$ and $4n$, so $\gcd(2n - 1, 4n) = 1$. Now, we have that

$$[2n - 1]^2 = [4n^2 - 4n + 1] = [1],$$

so $[2n - 1]$ is an element of order 2 in $U(4n)$, provided that $[2n - 1] \neq 1$. But $[2n - 1] = [1]$ if and only if $2n - 1 = 1$, which happens only if $n = 1$.

So, this is one element with order 2. The second one is $[4n - 1]$; we have $[4n - 1] \in \mathbb{Z}/4n\mathbb{Z}$ since $1 = 1 \cdot 4n + (-1) \cdot (4n - 1)$. And

$$[4n - 1]^2 = [-1]^2 = [1].$$

So $U(4n)$ has two different elements of order 2, provided that $[4n - 1] \neq [1]$ and $[4n - 1] \neq [2n - 1]$. Neither can occur for $n \geq 2$.

The other conjectures (2)-(5) are beyond our current abilities. We will be able to prove (4) and (5) once we learn the Chinese remainder theorem. We won't be able to prove (2) until we discuss fields and the structure theorem for finitely generated abelian groups, but then (3) will follow immediately from (2) and (4) (plus checking the special case $p = 2$).

Problem 2.2. Let (G, \circ) be an abelian group. We say a subgroup H of G is *generated by two elements* if there exist elements $g, h \in H$ such that every element of H can be written in the form $g^n h^m$ for some integers n and m . Investigate the subgroups of $(\mathbb{Q}, +)$ which are generated by two elements. Compute a few examples and make some conjectures. Try to prove your conjectures.

Solution: I was hoping you would discover from playing around that all of your examples were cyclic. In fact this is true; any subgroup of \mathbb{Q} generated by two elements is cyclic. Here's a proof: suppose H is the subgroup of \mathbb{Q} generated by a/b and c/d . We can assume that $a \neq 0$ and $c \neq 0$, otherwise clearly H is cyclic. We have:

$$\begin{aligned} H &= \left\{ n \frac{a}{b} + m \frac{c}{d} \mid n, m \in \mathbb{Z} \right\} \\ &= \left\{ \frac{1}{bd} (nad + mbc) \mid n, m \in \mathbb{Z} \right\} \\ &= \left\{ \frac{k}{bd} \cdot \gcd(ad, bc) \mid k \in \mathbb{Z} \right\} \\ &= \left\{ k \cdot \frac{\gcd(ad, bc)}{bd} \mid k \in \mathbb{Z} \right\} \\ &= \left\langle \frac{\gcd(ad, bc)}{bd} \right\rangle \end{aligned}$$

The vital step here was one we have already seen in other problems: the set of numbers of the form $nad + mbc$ with $n, m \in \mathbb{Z}$ is the same as the set of multiples of $\gcd(ad, bc)$.

There are many interesting questions you could ask from here. For example, when do a/b and c/d generate the same subgroup as a'/b' and c'/d' ? Of course, the answer is "when $\gcd(ad, bc)/bd = \gcd(a'd', b'c')/b'd'$," but maybe this can be phrased in a nicer way. Another nice question might be: how does the group $H \cap \mathbb{Z}$ relate to the groups $\langle a/b \rangle \cap \mathbb{Z}$ and $\langle c/d \rangle \cap \mathbb{Z}$? I'll leave this to you to investigate.

3. CHALLENGE PROBLEM

Problem 3.1. Show that $(\mathbb{Q}/\mathbb{Z}, +)$ has a subgroup H with the following two properties:

- (1) H is infinite.
- (2) Every proper subgroup of H is finite.

Solution: Let $H = \{[m/2^n] \mid n \in \mathbb{Z}_{\geq 0}, m \in \mathbb{Z}\}$. I claim that H is a subgroup with the desired properties. I leave it to you to check that H is a subgroup. H is clearly infinite: the subset $\{[1/2^n] \mid n \in \mathbb{Z}_{\geq 0}\}$ is a nice infinite subset of H . It remains to see that every proper subgroup is finite. I will prove the contrapositive of this statement, i.e. I will show that if K is an infinite subgroup of H , then $K = H$.

So, assume that K is an infinite subgroup of H . Then I claim that K must contain elements of the form $[m/2^n]$ for arbitrarily large n , with m relatively prime to n . Indeed, suppose not. Then there is some $n \in \mathbb{N}$ such that all elements of K can be written as $[m/2^\ell]$ with $\ell \leq n$. Multiplying the numerator and denominator of this expression by $2^{n-\ell}$, we see that every element in K must be of the form $[m/2^n]$ for some $m \in \mathbb{Z}$. But there are finitely many such classes, namely the classes given by $m = 0, 1, \dots, 2^n - 1$. Hence K is finite, contradicting our assumption.

Thus K must contain elements of the form $[m/2^n]$ for arbitrarily large n , with m odd. Now, let $[m/2^n] \in H$ be arbitrary. We will show that this element is also in K . We know by the above that we can find a $k \in \mathbb{N}$, $k \geq n$, such that K contains an element of the form $a/2^k$ with $\gcd(a, 2^k) = 1$. Write $1 = pa + q2^k$ for some $p, q \in \mathbb{Z}$. Then we have

$$\begin{aligned} \left[\frac{m}{2^n} \right] &= \left[\frac{2^{k-n}}{2^k} \right] \\ &= \left[\frac{2^{k-n}(pa + q2^k)}{2^k} \right] \\ &= \left[p2^{k-n} \cdot \frac{a}{2^k} + q \right] \\ &= p2^{k-n} \cdot \left[\frac{a}{2^k} \right] \in K, \end{aligned}$$

as desired.