MATH 7210 Homework 1

Andrea Bourque

September 2021

1 Problem 2(b,c)

b) Show that a finite cancellation semigroup is a group.

Proof. Let $S = \{x_1, ..., x_n\}$ be a cancellation semigroup. Consider the set $x_1S = \{x_1x_j, j = 1, ..., n\}$. Since $x_1x_j = x_1x_i$ implies $x_i = x_j$, each x_1x_j is a distinct element in S; there are n of them, so $x_1S = S$. In fact, $x_iS = S$ for each i, a fact used later. In particular, there is some k such that $x_1x_k = x_1$. Then $x_1x_kx_1 = x_1x_1$ by multiplication on the right by x_1, and then cancellation on the left gives $x_kx_1 = x_1$. Now, consider x_ix_k for some i. This must be in S, so it is equal to some x_j. Right-multiplying by x_1 gives $x_ix_kx_1 = x_jx_1$, but on the left hand side, using $x_kx_1 = x_1$, we have x_ix_1. Then right-cancellation gives $x_i = x_j$. Thus $x_ix_k = x_i$ for all i. Similarly, $x_kx_i = x_i$ for all i, which follows by left-multiplying x_1, simplifying the left hand side, and then using left-cancellation. Thus, x_k is an identity element.

Using $x_iS = S$ again, we see that there is some j such that $x_ix_j = x_k$. Right-multiplying by x_i gives $x_ix_jx_i = x_kx_i$, where the right hand side is also equal to x_ix_k. Left-cancellation gives $x_jx_i = x_k$. Thus each element $x_i \in S$ has an inverse. Thus, S is a group. □

c) Give an example of an infinite cancellation semigroup which is not a group.

Proof. Consider the non-zero integers $\mathbb{Z}^*$, with the operation of standard integer multiplication. Since $\mathbb{Z}$ has no zero-divisors, $ab = ac$ implies $b = c$ for $a \neq 0$. (In particular, in the ring $\mathbb{Z}$, $a(b - c) = 0$ so $a = 0$ or $b - c = 0$). Thus $\mathbb{Z}^*$ is an infinite cancellation semigroup. However, it is not a group, since there are no inverses; there is no integer a for which $2a = 1$. □

2 Problem 4

Let G be a group.

a) If G is a group of even order, then the number of elements of order 2 is odd.

Proof. Notice that $g = g^{-1}$ implies $g^2 = e$, which means g is either identity or has order 2. Then the elements of order > 2 come in pairs (x, x^{-1}), so there are an even number of them. Since $|G|$ is even, there are an even number of elements that are their own inverses. One of these is the identity, so there are an odd number of order 2 elements. □

b) Show TFAE:

i) G is abelian.

ii) $\iota : G \to G$ given by $\iota(a) = a^{-1}$ is a group homomorphism.

iii) $h : G \to G$ given by $h(a) = a^2$ is a group homomorphism.

Proof. i)→ ii) $\iota(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$, with the last equality coming from G being abelian. Then $a^{-1}b^{-1} = \iota(a)\iota(b)$, so ι is a group homomorphism.

ii)→ i) $\iota(a^{-1}b^{-1}) = \iota(a^{-1})\iota(b^{-1})$ implies $ba = ab$ by using the definition of ι. Thus G is abelian since a, b are arbitrary.

i)→ iii) $h(ab) = (ab)^2 = abab = aabb$, with the last inequality coming from G being abelian. Then $aabb = a^2b^2 = h(a)h(b)$, so h is a group homomorphism.

iii)→ i) $h(ab) = h(a)h(b)$ gives $abab = aabb$ by using the definition of h. By left-multiplying by a^{-1} and right-multiplying by b^{-1}, we get $ba = ab$. Since a, b are arbitrary, G is abelian. □

3 Problem 5

Let G be a finite group and let $a, b \in G$ such that $ab = ba$.

a) Show $|ab|$ divides $|a||b|$.

Proof. Since $ab = ba$, $(ab)^n = ab...ab = a^n b^n$ for all n. In particular, $(ab)^{|a||b|} = a^{|a||b|} b^{|a||b|} = e^{|b|} e^{|a|} = e$. But in general, if $x^n = e$, then $|x|$ divides n. Therefore, $|ab|$ divides $|a||b|$. □

b) If $\langle a \rangle \cap \langle b \rangle = \{e\}$, show that $|ab| = lcm\{|a|, |b|\}$.

Proof. Note that $(ab)^{|ab|} = e = a^{|ab|} b^{|ab|}$ implies $a^{|ab|} = b^{-|ab|}$. But $\langle a \rangle \cap \langle b \rangle = \{e\}$ implies that the only element that is both a power of a and b is e. Thus $a^{|ab|} = b^{-|ab|} = e$. Thus $|a|$ and $|b|$ divide $|ab|$. Since $|ab|$ is minimal, $|ab| = lcm\{|a|, |b|\}$. □

c) If $|a|, |b|$ are coprime, show that $|ab| = |a||b|$.

Proof. Suppose $a^p = b^q \neq e$. Then since $|a^p|$ divides $|a|$ and $|b^q|$ divides $|b|$, $|a|$ and b share a factor. Thus, if $|a|, |b|$ are coprime, $\langle a \rangle \cap \langle b \rangle = \{e\}$. The lcm of coprime numbers is their product, so we are done by part b. □

d) Exhibit a counterexample where these results fail if $ab \neq ba$.

Proof. Consider the group S_4 of permutations on three elements. Consider the elements $a = (34), b = (124)$. Then $|a| = 2, |b| = 3$. $ab = (1234)$, while $ba = (1243)$. $|ab| = 4$, which does not divide $2 * 3 = 6$, so a fails. $\langle a \rangle = \{(34), e\}$, and $\langle b \rangle = \{(124), (142), e\}$, so $\langle a \rangle \cap \langle b \rangle = \{e\}$, but 4 is not the lcm of 2 and 3, so b fails. Finally, 2 and 3 are coprime, but $4 \neq 2 * 3$, so c fails as well. □

4 Problem 6

Let $K = \{\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) | x > 0, y \in \mathbb{R}\}$ and $H = \{\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) | x > 0\}$.

a) Show that K, H are subgroups of $GL_2(\mathbb{R})$.

Proof. Clearly $K, H \subset GL_2(\mathbb{R})$ since $\det\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) = x \neq 0$ by the hypothesis that $x > 0$. Furthermore, both contain the identity $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ since $1 > 0$.

Now, $\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} w & z \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} wx & xz+y \\ 0 & 1 \end{smallmatrix}\right) \in K$ since $wx > 0$ for $w, x > 0$. By solving $wx = 1, xz + y = 0$ we get $w = \frac{1}{x}, z = \frac{-y}{x}$, which are well-defined since $x \neq 0$, and the resulting matrix is in K since $x > 0$ implies $w = \frac{1}{x} > 0$. Thus K is closed under multiplication and inverses, so K is a subgroup.

Now,

$$\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} w & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} wx & 0 \\ 0 & 1 \end{smallmatrix}\right) \in H$$

since $w, x > 0$ implies $wx > 0$. The inverse is given when $w = \frac{1}{x}$, which is well-defined and positive since $x > 0$. Thus H is also closed under multiplication and inverses, so it is a subgroup. □

b) Is H normal in K?

Proof. First we note that H is a subgroup of K, which is clear since H is obviously a subset of K by definition, and since both are subgroups of $GL_2(\mathbb{R})$. Now let $k = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right), h = \left(\begin{smallmatrix} z & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $khk^{-1} = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} z & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} xz & y \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} z & y-yz \\ 0 & 1 \end{smallmatrix}\right)$, which is, in general, not an element of H (say $y \neq 0$, $z \neq 1$). Thus H is not normal in K. □

c) Identify K with the right half plane of $\mathbb{R}^2$ by $\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) \mapsto (x, y)$. Draw the partitions of K into left and right cosets of H.

Proof. For $k = \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$, the coset kH consists of $\left(\begin{smallmatrix} xz & y \\ 0 & 1 \end{smallmatrix}\right)$ for all $z > 0$. These are just the open rays $(0, \infty) \times \{y\}$. The right coset Hk consists of $\left(\begin{smallmatrix} z & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} zx & zy \\ 0 & 1 \end{smallmatrix}\right)$ for all $z > 0$. These are the open rays starting at the origin and passing through the point (x, y). For figures, see the next page. □

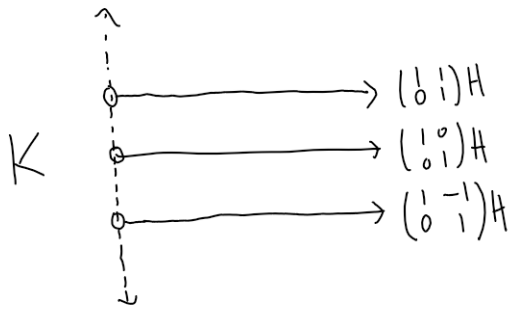

Figure 1: Left cosets

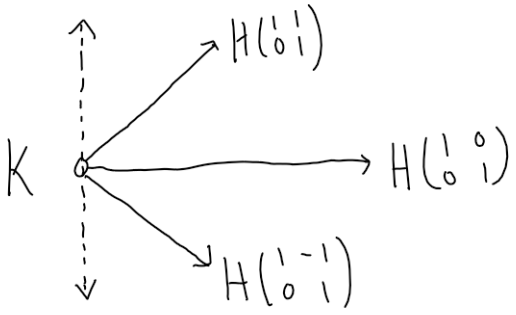

Figure 2: Right cosets

5 Problem 2.1.13

Let H be a subgroup of $(\mathbb{Q}, +)$ such that $1/x \in H$ for all nonzero $x \in H$. Prove $H = 0$ or $H = \mathbb{Q}$.

Proof. $H = 0$ satisfies the hypothesis vacuously. Thus assume $H \neq 0$. Let $a = \frac{p}{q} \in H$ be nonzero, where p, q are coprime and $q > 0$. Then $a + ... + a$, q times is equal to p, so $p \in H$. Since $p, -p \in H$, let $r = |p| \in H$. Since $r \neq 0$, $\frac{1}{r} \in H$. Thus $\frac{1}{r} + ... + \frac{1}{r}$, r times, which is 1, is in H. It follows then that all integers are in H, since $1 + ... + 1 \in H$ and $-1 + ... + -1 \in H$. Then $\frac{1}{n} \in H$ for all nonzero integers n. Then $\frac{1}{n} + ... + \frac{1}{n}$, m times gives an arbitrary rational number $\frac{m}{n} \in H$, so $H = \mathbb{Q}$ as desired. □